COMPUTING SOLUTIONS OF LINEAR MAHLER EQUATIONS

FRÉDÉRIC CHYZAK, THOMAS DREYFUS, PHILIPPE DUMAS,
AND MARC MEZZAROBBA

Abstract. Mahler equations relate evaluations of the same function f at iterated bth powers of the variable. They arise in particular in the study of automatic sequences and in the complexity analysis of divide-and-conquer algorithms. Recently, the problem of solving Mahler equations in closed form has occurred in connection with number-theoretic questions. A difficulty in the manipulation of Mahler equations is the exponential blow-up of degrees when applying a Mahler operator to a polynomial. In this work, we present algorithms for solving linear Mahler equations for series, polynomials, and rational functions, and get polynomial-time complexity under a mild assumption. Incidentally, we develop an algorithm for computing the gcrd of a family of linear Mahler operators.

1. Introduction

1.1. **Context.** Our interest in the present work is in computing various classes of solutions to *linear Mahler equations* of the form

$$\ell_r(x)y(x^{b^r}) + \cdots + \ell_1(x)y(x^b) + \ell_0(x)y(x) = 0, \tag{EQN}$$

where $\ell_0, \dots, \ell_r$ are given polynomials, $r > 0$ is the order of the equation, and $b \geq 2$ is a fixed integer.

Mahler equations were first studied by Mahler himself in a nonlinear context [15]. His aim was to develop a general method to prove the transcendence of values of certain functions. Roughly speaking, the algebraic relations over $\bar{\mathbb{Q}}$ between certain of these values come from algebraic relations over $\bar{\mathbb{Q}}(x)$ between the functions themselves. This direction was continued by several authors. We refer to Pellarin's introduction [17] for a historical and tutorial presentation, and to the references therein; see also Nishioka [16] for a textbook.

Mahler equations are closely linked with automata theory: the generating series of any b-automatic sequence is a Mahler function, that is, a solution of a linear Mahler equation; see [8, 9]. Mahler functions also appear in many areas at the interface of mathematics and computer science, including combinatorics of partitions, enumeration of words, and the analysis of divide-and-conquer algorithms.

Very recently, functional relations between Mahler functions have been further studied with a bias to effective tests and procedures [4, 10, 18]. Such studies motivate the need for algorithms that solve Mahler equations in various classes of functions. For instance, testing transcendence by the criterion of Bell and

Date: February 1, 2017.

2010 *Mathematics Subject Classification.* Primary: 39A06; Secondary: 33F10, 68W30.

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 648132. MM was supported in part by ANR grant ANR-14-CE25-0018-01 (FastRelax).

Coons [4] requires to compute a truncation of a Mahler series to suitable order, and the hypertranscendence criterion by Dreyfus, Hardouin, and Roques [10] relies on determining if certain Mahler equations possess ramified rational solutions.

1.2. **Related work.** Mahler equations are a special case of difference equations, in the sense of functional equations relating iterates of a ring endomorphism σ applied to the unknown function.

Algorithms dealing with difference equations have been widely studied. In particular, the computation of rational solutions of linear difference equations with coefficients polynomial in the independent variable x is an important basic brick coming up repeatedly in other algorithms. Algorithms in the cases of the usual shift $\sigma(x) = x + 1$ and its q-analogue $\sigma(x) = qx$ have been given by Abramov [2, 3] for equations with polynomial coefficients: in both cases, the strategy is to compute a denominator bound before changing unknown functions and computing the numerator as a polynomial solution of an auxiliary difference equation. Bronstein [6] provides a similar study for difference equations over more general coefficient domains; his denominator bound is however available under a restriction (*unimonomial extensions*) that do not allow for the Mahler operator $\sigma(x) = x^b$.

Mahler equations can also be viewed as difference equations in terms of the usual shift $\sigma(t) = t + 1$ after performing the change of variables $t = \log_b \log_b x$. This reduction from Mahler to difference equation, however, does not preserve polynomial coefficients, which means that neither Abramov's nor Bronstein's algorithm can be used in this setting.

There has been comparatively little interest in algorithmic aspects specific to Mahler equations. To the best of our knowledge, the only systematic study is by Dumas in his PhD thesis [11]. In particular, he describes procedures for computing various types of solutions of linear Mahler equations [11, Chapter 3]. However, beside a few gaps of effectiveness, that work does not take computational complexity issues into account. To a large extent, the results of the present work can be viewed as refinements of it, with a focus on efficiency and complexity analysis. More recently, Bell and Coons [4] give degree bounds that readily translate into algorithms for polynomial and rational solutions based on undetermined coefficients. With regard to series solutions, van der Hoeven [20, §4.5.3] suggests an algorithm that applies, under hypotheses, to certain equations of the form (EQN) as well as to certain nonlinear generalizations, and computes the first n terms of a power series solution in $\tilde{\mathrm{O}}(n)$ arithmetic operations. At least in the linear case and in analogy to the case of difference equations, this leaves the open question of an algorithm in complexity $\mathrm{O}(n)$.

1.3. **Setting.** Our goal in this article is to present algorithms that compute complete sets of polynomial solutions, rational function solutions, truncated power series solutions, and truncated Puiseux series solutions of (EQN). More precisely, let $\mathbb{K}$ be a (computable) subfield of $\mathbb{C}$, and suppose $\ell_0, \dots, \ell_r \in \mathbb{K}[x]$. Denote by $\mathbb{K}((x^{1/*}))$ the field $\bigcup_{n=1}^{+\infty} \mathbb{K}((x^{1/n}))$ of formal Puiseux series with coefficients in $\mathbb{K}$. Let M denote the *Mahler operator of radix* b, that is the automorphism of $\mathbb{K}((x^{1/*}))$ that substitutes x^b for x and reduces to the identity map on $\mathbb{K}$. Writing x again for the operator of multiplication of a series by x, M and x follow the commutation rule $Mx = x^b M$. Equation (EQN) then rewrites as $Ly = 0$ where

$$L = \ell_r M^r + \cdots + \ell_0 \tag{OPR}$$

Kind of solutions	Algorithm	Complexity
$\mathbb{K}[[x]]$, to order $\lfloor \nu \rfloor + 1$	Alg. 4	$O(rdv_0^2 + r^2\,M(v_0))$
$\mathbb{K}[[x]]$, to order n, when $r = O(d)$	Alg. 3	$O(rd^3 + nrd)$
$\mathbb{K}[x]$	Alg. 6	$\tilde{O}(b^{-r}d^2 + M(d))$
$\mathbb{K}((x^{1/N}))$	Alg. 7	$\tilde{O}(r^2Nd(d+n))$
$\mathbb{K}((x^{1/*}))$	Alg. 7	$\tilde{O}(r^2b^rd(d+n))$
$\mathbb{K}(x)$, when $b = 2$	Alg. 9	$\tilde{O}(d^3)$
$\mathbb{K}(x)$, when $b \geq 3$	Alg. 9	$\tilde{O}(b^{-r}d^2)$

TABLE 1. Complexity of the solving algorithms presented in the paper, assuming $\ell_0 \neq 0$.

in the algebra generated by M and x. We are interested in the algebraic complexity of computing the kernel of L in each of $\mathbb{K}[x]$, $\mathbb{K}(x)$, $\mathbb{K}[[x]]$, and $\mathbb{K}((x^{1/*}))$.

We always assume that ℓ_r is nonzero. Except where otherwise noted, we also assume $\ell_0 \neq 0$. From a decidability viewpoint, the latter assumption is no loss of generality thanks to the following result [11, Cor. 6, p. 36].

Proposition 1.1. *Given a linear Mahler equation of the form* (EQN)*, one can compute an equation of the same form, with $\ell_0 \neq 0$, that has exactly the same same formal Laurent series solutions—and therefore, the same polynomial solutions and the same rational-function solutions.*

Note however that this result does not say anything about the cost of reducing to the case $\ell_0 \neq 0$. We give a complexity bound for this step in §4. As it turns out, this bound often dominates our complexity estimates for the actual solving algorithms. Let us therefore stress that all other complexity results are stated under the assumption that ℓ_0 is nonzero.

For $0 \leq k \leq r$, we denote by $v_k \in \mathbb{N} \cup \{+\infty\}$ and $d_k \in \mathbb{N} \cup \{-\infty\}$ the valuation and degree of the coefficient ℓ_k. Let $d \geq \max_{0\leq k\leq r} d_k$. Polynomials are implicitly represented in dense form, so that polynomials of degree d in $\mathbb{K}[x]$ have size $d+1$. All complexity estimates are given in terms of arithmetical operations in $\mathbb{K}$, which we denote "ops". The complexity of multiplying two polynomials of degree at most n is denoted by $M(n)$; we make the standard assumptions that $M(n) = O(n^2)$ and that $n \mapsto M(n)/n$ is nondecreasing.

Given two integers or polynomials a and b, we denote their gcd by $a \wedge b$ and their lcm by $a \vee b$; we use $\bigwedge$ and $\bigvee$ for $n$ary forms.

The following identities are used repeatedly in the text. We gather and repeat them here for easier reference:

$$\ell_r(x)y(x^{b^r}) + \cdots + \ell_1(x)y(x^b) + \ell_0(x)y(x) = 0, \tag{EQN}$$

$$L = \ell_r M^r + \cdots + \ell_0, \tag{OPR}$$

$$\nu = \max_{k\geq 1} \frac{v_0 - v_k}{b^k - 1}, \qquad \mu = v_0 + \nu. \tag{MU-NU}$$

1.4. **General strategy and outline.** The article is organized as follows. In §2, we develop algorithms to compute truncated series solutions of equations of the form (EQN). We start with an example that illustrates the structure of the solution space and some of the main ideas behind our algorithms (§2.1). Then, we introduce a notion of Newton polygons, and use it to prove that the possible valuations (resp.

degrees) of the solutions of (EQN) in $\mathbb{K}((x^{1/*}))$ (resp. $\mathbb{K}[x]$) belong to a finite set that we make explicit (§2.2). We compute a suitable number of initial coefficients by solving a linear system (§2.4), then prove that the following ones can be obtained iteratively in linear time, and apply these results to give a procedure that computes a complete set of truncated series solutions (§2.5). Finally, we extend the same ideas to the case of solutions in $\mathbb{K}[x]$ (§2.6) and in $\mathbb{K}((x^{1/*}))$ (§2.7).

The next section, §3, deals with solutions in $\mathbb{K}(x)$. The general idea is to first obtain a denominator bound, that is a polynomial q such that $Lu = 0$ with $u \in \mathbb{K}(x)$ implies $qu \in \mathbb{K}[x]$ (§3.1). Based on elementary properties of the action of M on elements of $\mathbb{K}[x]$ (§3.2), we give several algorithms for computing such bounds (§3.3–§3.4). This reduces the problem to computing a set of polynomial solutions with certain degree constraints, which can be solved efficiently using the primitives developed in §2. This leads to an algorithm for solving linear Mahler equations in $\mathbb{K}(x)$ (§3.5).

Finally, in §4, we generalize our study to the situation where the coefficient ℓ_0 in (EQN) is zero. This makes us develop an unexpected algorithm for computing the gcrd of a family of operators, which we analyze and compare to the more traditional approach via Sylvester matrices and subresultants.

1.5. **Acknowledgment.** The authors are indebted to Alin Bostan for helpful discussions and for pointing us to the work of Grigor'ev [12].

2. Polynomial and series solutions

2.1. **A worked example.** The aim of this section is to illustrate our solving strategy in $\mathbb{K}[[x]]$ and $\mathbb{K}((x^{1/*}))$ on an example that we treat straightforwardly.

In radix $b = 3$, consider the equation $Ly = 0$ where

$$\begin{aligned} L = {} & x^3(1 - x^3 + x^6)(1 - x^7 - x^{10})\, M^2 \\ & - (1 - x^{28} - x^{31} - x^{37} - x^{40})\, M + x^6(1 + x)(1 - x^{21} - x^{30}). \end{aligned} \tag{2.1}$$

Assume that $y \in \mathbb{K}((x^{1/*}))$ is a solution whose valuation is a rational number v. The valuations of $\ell_k M^k y$, for $k = 0, 1, 2$, are respectively equal to $6 + v, 3v, 3 + 9v$. If one of these rational numbers was less than the other two, then the valuation of the sum $\sum_{k=0}^{2} \ell_k M^k y$ would be this smaller number, and Ly could not be zero. Consequently, at least two of the three rational numbers $6 + v, 3v, 3 + 9v$ have to be equal to their minimum. After solving, we find $v \in \{-1/2, 3\}$.

First consider the case $v = 3$, and write $y = \sum_{n \geq 3} y_n x^n$. For m from 10 to 15, extracting the coefficients of x^m from both sides of $0 = \ell_0 y + \ell_1 My + \ell_2 M^2 y$, we find that $y_3, \dots, y_9$ satisfy

$$\begin{aligned} 0 &= y_3 + y_4, \\ 0 &= \quad y_4 + y_5, \\ 0 &= -y_4 + y_5 + y_6, \\ 0 &= \quad\quad y_6 + y_7, \\ 0 &= \quad\quad\quad y_7 + y_8, \\ 0 &= -y_5 \quad\quad + y_8 + y_9. \end{aligned} \tag{2.2}$$

More generally, extracting the coefficient of x^m yields the relation

$$\begin{aligned}(2.3)\quad &\big(y_{m-6}+y_{m-7}-y_{m-27}-y_{m-28}-y_{m-36}-y_{m-37}\big)\\ &\quad-\big(y_{\frac{m}{3}}-y_{\frac{m-28}{3}}-y_{\frac{m-31}{3}}-y_{\frac{m-37}{3}}-y_{\frac{m-40}{3}}\big)\\ &\qquad+\big(y_{\frac{m-3}{9}}-y_{\frac{m-6}{9}}+y_{\frac{m-9}{9}}-y_{\frac{m-10}{9}}-y_{\frac{m-19}{9}}\big)=0,\end{aligned}$$

where y_s is understood to be zero if the rational number s is not a nonnegative integer. This equation takes different forms, depending on the residue of m modulo 9: for example, for $m=20$ and $m=42$, it reduces to, respectively,

$$y_{14}+y_{13}=0, \qquad y_{36}+y_{35}-y_{15}-2y_{14}-y_6-y_5-y_4=0.$$

Despite these variations, for any $m\geq 10$ the index $n=m-6$ is the largest integer index occurring in (2.3). It follows that for successive $m\geq 10$, we can iteratively obtain y_n from (2.3) in terms of already known coefficients of the series. Conversely, any sequence $(y_n)_{n\geq 3}$ that satisfies (2.3) gives a solution $y=\sum_{n\geq 3} y_n x^n$ of (EQN).

As a consequence, the power series solution is entirely determined by the choice of y_3 and the space of solutions of (EQN) in $\mathbb{K}[[x]]$ has dimension one. A basis consists of the single series

$$(2.4)\qquad x^3-x^4+x^5-2x^6+2x^7-2x^8+3x^9-3x^{10}+3x^{11}-5x^{12}+\cdots.$$

The other possible valuation, $v=-1/2$, is not a natural number. To revert to the simpler situation of the previous case, we perform the change of variables $x=t^2$ followed by the change of unknowns $y(t)=\tilde{y}(t)/t$. The equation becomes $\tilde{L}\tilde{y}=0$ with

$$\begin{aligned}(2.5)\quad \tilde{L}=&(1-t^6+t^{12})(1-t^{14}-t^{20})\,M^2\\ &-(1-t^{56}-t^{62}-t^{74}-t^{80})\,M+t^{14}(1+t^2)(1-t^{42}-t^{60}).\end{aligned}$$

To understand this calculation, remember that M was defined on $\mathbb{K}((x^{1/*}))$, so that $M(t)=M(x^{1/2})=x^{3/2}=t^3$.

We now expect $\tilde{L}$ to have solutions $\tilde{y}=\sum_{n\geq 0}\tilde{y}_n t^n$ of valuation 0 and 7 with respect to t, and the solutions of $\tilde{L}$ with valuation 0 to correspond to the solutions of L with valuation $-1/2$. Extracting the coefficients of x^m for m from 0 to 24 from both sides of $\tilde{L}\tilde{y}=0$ and skipping tautologies, we find that $\tilde{y}_0,\dots,\tilde{y}_{10}$ satisfy

$$\begin{aligned}
0 &= -\tilde{y}_1,\\
0 &= -\tilde{y}_0 - \tilde{y}_2,\\
0 &= \tilde{y}_1 - \tilde{y}_3,\\
0 &= \tilde{y}_0 - \tilde{y}_4,\\
0 &= -\tilde{y}_5,\\
0 &= \tilde{y}_0 + \tilde{y}_2,\\
0 &= \tilde{y}_1 + \tilde{y}_3,\\
0 &= 2\tilde{y}_2 + \tilde{y}_4 - \tilde{y}_6,\\
0 &= \tilde{y}_3 + \tilde{y}_5,\\
0 &= \tilde{y}_4 + \tilde{y}_6,\\
0 &= \tilde{y}_1 + \tilde{y}_5,\\
0 &= \tilde{y}_6 + \tilde{y}_8,\\
0 &= -\tilde{y}_1 + \tilde{y}_7 + \tilde{y}_9,\\
0 &= -\tilde{y}_2 + \tilde{y}_{10}.
\end{aligned}$$

Reasoning as above, we derive that, given $\tilde{y}_0$ while enforcing $\tilde{y}_7 = 0$, there is exactly one power series solution to $\tilde{L}$. More specifically when $\tilde{y}_0 = 1$ and $\tilde{y}_7 = 0$, we find the series

$$1 - t^2 + t^4 - t^6 + t^8 - t^{10} + t^{12} + \cdots .$$

Hence, there is a 2-dimensional solution space in $\mathbb{K}((x^{1/*}))$ for the original equation (EQN), with a basis consisting of the power series (2.4) and the additional Puiseux series

$$x^{-1/2} - x^{1/2} + x^{3/2} - x^{5/2} + x^{7/2} - x^{9/2} + x^{11/2} + \cdots .$$

2.2. **Valuations and degrees.** Let us assume that $y \in \mathbb{K}((x^{1/*}))$ is a solution of (EQN), whose valuation is a rational number v. The valuation of the term $\ell_k M^k y$ is then $v_k + b^k v$. Among those expressions, at least two must be minimal to permit the left-hand side of (EQN) to be 0: therefore, there exist distinct indices k_1, k_2 between 0 and r such that

$$v_{k_1} + b^{k_1} v = v_{k_2} + b^{k_2} v = \min_{0 \le k \le r} v_k + b^k v. \tag{2.6}$$

This necessary condition for $Ly = 0$ can be interpreted using a *Newton polygon* analogous to that of algebraic equations [21, Sec. IV.3.2-3]: to each monomial $x^j M^k$ in L, we associate the point (b^k, j) in the first quadrant of the Cartesian plane endowed with coordinates U and V (see Fig. 1). We call the collection of these points the *Newton diagram* of L, and the lower (resp. upper) boundary of its convex hull the *lower* (resp. *upper*) *Newton polygon* of L. That two integers k_1, k_2 satisfy (2.6) exactly means that (b^{k_1}, v_{k_1}) and (b^{k_2}, v_{k_2}) belong to an edge E of slope $-v$ of the corresponding lower Newton polygon.

Given an edge E as above, an arithmetic necessary condition holds in addition to the geometric one just mentioned: the coefficients of the monomials of L associated to points of E must add up to zero. We call an edge with this property *admissible*.

Example 2.1. The lower Newton polygon of the operator (2.1) appears in dashed lines in Figure 1. It contains two admissible edges, corresponding to the valuations 3 and $-1/2$.

We get the following criterion, already stated in [11, p. 51] with a slightly different proof.

Lemma 2.2. *Let L be defined as in (OPR). The valuation v of any formal Puiseux series solution of (EQN) is the opposite of the slope of an admissible edge of the lower Newton polygon of L. It satisfies*

$$-\frac{v_r}{b^{r-1}(b-1)} \le v = -\frac{v_{k_1} - v_{k_2}}{b^{k_1} - b^{k_2}} \le \frac{v_0}{b-1},$$

where (b^{k_1}, v_{k_1}) and (b^{k_2}, v_{k_2}) are the endpoints of the implied edge.

Proof. The fact that v is the opposite of a slope together with its explicit form follow from (2.6) and the discussion above. There remains to prove the upper and lower bounds. The leftmost edge of the lower Newton polygon of L provides the largest valuation and its slope $(v_k - v_0)/(b^k - 1)$ for some $k \ge 1$ is bounded below by $-v_0/(b-1)$. In the same way, the rightmost edge provides the smallest valuation and its slope, of the form $(v_r - v_k)/(b^r - b^k)$ for some $k < r$, is bounded above by $v_r/(b^r - b^{r-1})$. □

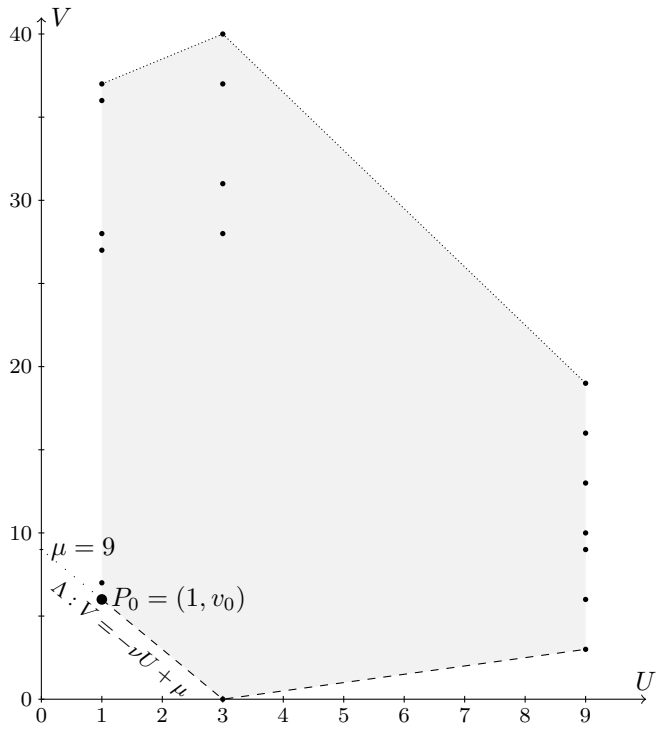

FIGURE 1. The Newton diagram of the equation treated in §2.1 for radix $b = 3$, with corresponding lower Newton polygon (dashed line) and upper Newton polygon (dotted line).

Proposition 2.3. *The dimension of the space of solutions of the homogeneous equation $Ly = 0$ in $\mathbb{K}((x^{1/*}))$ is bounded by the order r of L.*

Proof. The space of solutions admits a basis consisting of Puiseux series with pairwise distinct valuations. The number of possible valuations is bounded by the edge count of the lower Newton polygon of L, which is at most r. □

Remark 2.4. As we will see, the dimension of the solutions in $\mathbb{K}((x^{1/*}))$ can be strictly less than r. It is natural to ask how to construct a "full" system of r linearly independent formal solutions in some larger extension of $\mathbb{K}(x)$. We will not pursue this question here and point to Roques's work for an answer; see [18, Lemma 20 and Thm 35] and [19, Theorem 1]. See also Remark 2.18 below.

In analogy with the previous discussion on valuations of solutions, if a Puiseux series solution of (EQN) involves monomials with maximal exponent δ, then the expression $d_k + b^k\delta$ must reach its maximum at least twice as k ranges from 0 to r. As we see by the same reasoning as above (or by changing x to $1/x$, which exchanges the lower and upper Newton polygons), $-\delta$ is then one of the slopes of the upper Newton polygon of L. The largest possible value corresponds to the rightmost edge.

Lemma 2.5. *The maximum exponent δ of a monomial in a finite Puiseux series solution, and in particular the degree of a polynomial solution, is the opposite of the*

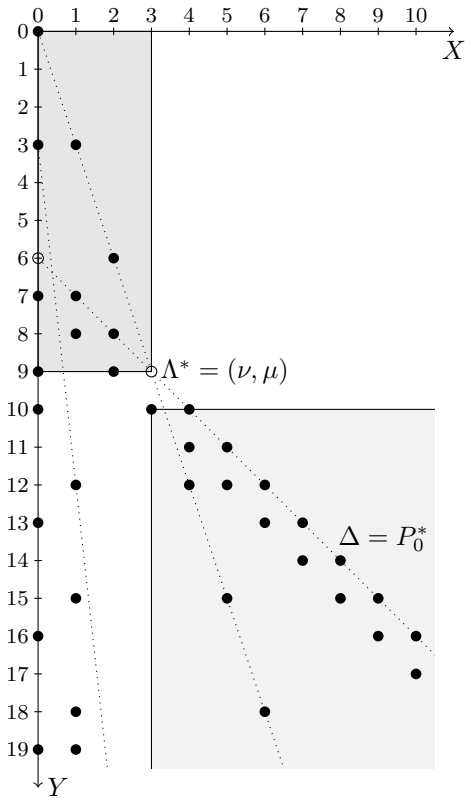

FIGURE 2. The infinite matrix R corresponding to the example treated in §2.1: solid circles denote nonzero entries, hollow circles denote recombinations to zero.

slope of an admissible edge of the upper Newton polygon. It satisfies

$$\delta = -\frac{d_{k_1} - d_{k_2}}{b^{k_1} - b^{k_2}} \leq \frac{d}{b^{r-1}(b-1)},$$

for some $k_1 \neq k_2$.

The admissibility of an edge of the upper Newton polygon is defined in analogy with admissibility in the lower Newton polygon.

2.3. **The nonhomogeneous case.** One of the proofs of results about Puiseux series solutions in §2.7 makes use of extended Newton diagrams that take into account the right-hand side of nonhomogeneous equations.

For L as in (OPR) and a Puiseux series $\ell_{-\infty}$ of valuation $v_{-\infty} \in \mathbb{Q} \cup \{+\infty\}$, consider the nonhomogeneous equation

$$\ell_r(x)y(x^{b^r}) + \cdots + \ell_1(x)y(x^b) + \ell_0(x)y(x) = \ell_{-\infty}(x). \tag{2.7}$$

Given a Puiseux series solution $y \in \mathbb{K}((x^{1/*}))$ of this equation, with valuation $v \in \mathbb{Q}$, we define the Newton diagram of $(L, \ell_{-\infty})$ as the Newton diagram of L, augmented with all points $(0, \alpha)$ for which x^α appears with nonzero coefficient in $\ell_{-\infty}$. The notion of lower Newton polygon extends correspondingly.

As in §2.2, these definitions are motivated by analyzing the minimum of the valuations $v_k + b^k v$ of the terms of the left-hand side of (2.7): either this minimum is equal to $v_{-\infty}$, or it is less than $v_{-\infty}$ and must be reached as least twice on the left-hand side. In both cases, making the convention that $b^{-\infty} = 0$, there exist distinct indices k_1, k_2, now in $\{-\infty, 0, 1, \dots, r\}$, such that the analogue

$$v_{k_1} + b^{k_1} v = v_{k_2} + b^{k_2} v = \min_{k \in \{-\infty,0,1,\dots,r\}} v_k + b^k v$$

of (2.6) holds. Again, this exactly means that (b^{k_1}, v_{k_1}) and (b^{k_2}, v_{k_2}) belong to an edge E of slope $-v$ of the lower Newton polygon, now of $(L, \ell_{-\infty})$.

Depending on $v_{-\infty}$ and $\hat{v} = \min_{0 \le k \le r}(v_k + b^k v)$, the lower Newton polygon of $(L, \ell_{-\infty})$ can: be equal to that of L, if $\ell_{-\infty} = 0$; add an edge to its left, if $v_{-\infty} > \hat{v}$; prolong its leftmost edge, if $v_{-\infty} = \hat{v}$; or replace some of its leftmost edges, if $v_{-\infty} < \hat{v}$. We defined the admissibility of an edge E of the lower Newton polygon of L in terms of the coefficients of those monomials $x^{v_k} M^k$ in L associated to points on E. We extend the definition to edges of the lower Newton polygon of $(L, \ell_{-\infty})$ by the convention that, if a point has to be considered for $k = -\infty$, the corresponding coefficient is the opposite of the coefficient of $x^{v_{-\infty}}$ in $\ell_{-\infty}$. Admissibility is again a necessary condition for v to be a possible valuation of a solution of (2.7).

2.4. **Approximate series solutions.** We now concentrate on the search for power series solutions $y(x) = y_0 + y_1 x + \cdots \in \mathbb{K}[[x]]$ of (EQN). Extracting the coefficient of x^m in both sides of it yields a linear equation for the coefficients y_n. This linear equation can be viewed as a row, denoted R_m, of an infinite matrix $R = R(L)$.

The matrix R consists of overlapping strips with different slopes. We view its row and column indices, starting at 0, as continuous variables Y and X with the Y-axis oriented downwards. Each nonzero term $\ell_k(x) M^k$ then corresponds to matrix entries in the strip $b^k X + v_k \le Y \le b^k X + d_k$. By definition of v_k and d_k, the entries lying on the lines $Y = b^k X + d_k$ and $Y = b^k X + v_k$ that delimit the strip are nonzero, except maybe at intersection points of such lines (obtained for different k). Because of our assumption that ℓ_0 is nonzero, the smallest slope is 1, obtained for $k = 0$.

For large Y, the line $Y = X + v_0$ becomes the topmost one, and each row R_m determines a new coefficient y_n uniquely, for $n = m - v_0$. Thus, the power series solutions are characterized by a finite subsystem of R. In order to state this fact more precisely in Proposition 2.6 below, define

(MU-NU) $$\nu = \max_{k \ge 1} \frac{v_0 - v_k}{b^k - 1}, \qquad \mu = v_0 + \nu.$$

In terms of the Newton diagram, ν and μ are, respectively, the opposite of the slope and the V-intercept of the leftmost edge of the lower Newton polygon. Note that, as we can deduce from the proof of Lemma 2.2, there is no nonzero power series solution when $\nu < 0$, which happens if and only if v_0 is a strict minimum of all the v_k over $0 \le k \le r$.

Proposition 2.6. *Assume that $\nu \ge 0$. A vector $(y_0, \dots, y_{\lfloor \nu \rfloor})$ is a vector of initial coefficients of a formal power series solution*

(2.8) $$y = y_0 + \cdots + y_{\lfloor \nu \rfloor} x^{\lfloor \nu \rfloor} + y_{\lfloor \nu \rfloor + 1} x^{\lfloor \nu \rfloor + 1} + \cdots$$

of (EQN) *if and only if it satisfies the linear system given by the upper left* $(\lfloor\mu\rfloor+1)\times(\lfloor\nu\rfloor+1)$ *submatrix of* R*. The power series solution* (2.8) *extending* $(y_0,\dots,y_{\lfloor\nu\rfloor})$ *is then unique.*

Proof. A series $y = y_0 + y_1 x + \cdots$ is a solution if and only if its coefficients satisfy the system $(R_m)_{m\geq 0}$. Whenever

$$v_0 + n < v_1 + b^1 n, \quad \dots, \quad v_0 + n < v_r + b^r n, \tag{2.9}$$

the row R_{v_0+n} of R is the first one with a nonzero entry of index n. It then determines y_n in terms of $y_0,\dots,y_{n-1}$. Condition (2.9) is equivalent to $n > \nu$, hence, for any given $(y_n)_{0\leq n\leq\nu}$, there is a unique choice of $(y_n)_{n>\nu}$ satisfying all the equations R_m for $m > v_0 + \nu = \mu$. As, when (2.9) holds for a given n, the entries of index n of R_m with $m < v_0 + n$ are zero, the remaining equations $(R_m)_{0\leq m\leq\mu}$ only involve the unknowns $(y_n)_{0\leq n\leq\nu}$. □

We note in passing the following corollary, which is the essential argument in the proof of [18, Theorem 22].

Corollary 2.7. *In case the leftmost edge of the lower Newton polygon of* L *lies on the axis of abscissas and is admissible, Equation* (EQN) *admits a power series solution of valuation 0.*

Proof. We then have $\nu = \mu = 0$, so the only condition to check is that the first entry of R_0 is zero. This is equivalent to the edge being admissible. □

The geometric interpretation of the quantities μ and ν defined by (MU-NU) is a special case of a general correspondence between the structure of the matrix R and the Newton diagram of L via the point-line duality of plane projective geometry. The correspondence stems from the fact that a monomial $x^j M^k$ of L is associated both to a point (b^k, j) in the Newton diagram and, by considering its action on powers of x, to the entries of R lying on the line $Y = b^k X + j$. More generally, under projective duality, each point (U, V) in the plane of the Newton diagram corresponds to a line $Y = UX + V$ in the plane of the matrix R, while, conversely, the dual of a point (X, Y) is the line $V = -XU + Y$. A line through two points (U_1, V_1) and (U_2, V_2) corresponds to the intersection of their duals.

In particular, the point $P_0 = (1, v_0)$ corresponds to the right boundary $\Delta : Y = X + v_0$ of the strip of entries of slope 1 in the matrix R (see Figures 1 and 2). In the (U, V)-plane, the line containing the leftmost edge of the lower Newton polygon passes through that point $P_0 = \Delta^*$. This line is $\Lambda : V = -\nu U + \mu$ and corresponds to the bottommost intersection $\Lambda^* = (\nu, \mu)$ of Δ with the right boundary of another strip. Below this intersection, the entries of R lying on Δ are the topmost nonzero entries of their respective columns, and, at the same time, the rightmost nonzero entries of their respective rows: as already observed, each row R_m then determines a new y_n.

Example 2.8. For the operator L of §2.1, the right boundaries of the strips associated to the three terms of L have equations $Y = X+6$, $Y = 3X$, and $Y = 9X+3$ respectively (dotted lines in Fig. 2). The first two of them meet at $\Lambda^* = (3, 9)$ (Fig. 2, hollow circle at the bottom right corner of the gray rectangle), and the line $\Delta : Y = X + 6$ becomes the rightmost line for $Y > 9$. For $m \geq 10$, the row R_m reflects the relation (2.3). In particular, the existence of a power series solution is entirely determined by the small linear system that uses the rows R_0 to R_9 and

Input: The linear Mahler equation (EQN). A transformation ϕ of the form (2.10). Integers w, h. A set $E = \{m_0, m_1, \dots\}$ of row indices, with $m_0 < m_1 < \cdots < h$.
Output: The submatrix $R_E = (R_{m,n})_{\substack{m\in E\\ 0\le n<w}}$ of the infinite matrix $R(\phi(L))$.

(1) Initialize a row-sparse $|E| \times w$ matrix R_E.
(2) For $i = 0, 1, \dots, |E| - 1$ and $k = 0, 1, \dots, r$:
  (a) Set $B = m_i + \gamma - \alpha b^k$.
  (b) Compute $j_0' = \beta^{-1} B \bmod b^k$ (with $0 \le j_0' < b^k$).
  (c) For $j' = j_0', j_0' + b^k, j_0' + 2b^k, \dots$ while $j' \le d_k$ and $\beta j' \le B$:
    (i) If $\beta j' > B - b^k w$, then add $\ell_{k,j'}$ to $A[i, b^{-k}(B - \beta j')]$.
(3) Return R_E.

Algorithm 1. Matrix R.

the unknowns y_0 to y_3 (gray rectangle on Figure 2). Solving the system yields $y_0 = y_1 = y_2 = 0$ and y_3 arbitrary. We then recover the results of §2.1: the space of solutions of (EQN) in $\mathbb{K}[[x]]$ has dimension one and a basis consists of the single series (2.4). The V-intercept of the leftmost edge of the lower Newton polygon is $\mu = 9$, and the corresponding slope is $-\nu = -3$. In this case, it is both the column dimension of the small system and the valuation of the solution. Observe how the bottom right sector depicted in light gray corresponds to the system starting with equations (2.2): as the top left rectangle imposes $y_0 = y_1 = y_2 = 0$, the dots on the left of the sector in light gray play no role in the equations.

As we will see, in the situation of Proposition 2.6, the coefficients $y_{\lfloor\nu\rfloor+1}$ to $y_{\lfloor\nu\rfloor+n}$ of y can be computed from $y_0, \dots, y_{\lfloor\nu\rfloor}$ in $\mathrm{O}(n)$ ops for fixed L. This motivates to call the truncation to order $\mathrm{O}(x^{\lfloor\nu\rfloor+1})$ of a series solution an *approximate series solution* of (EQN).

2.5. **Power series solutions.** Our goal at this point is to describe an algorithm that computes the formal power series solutions of (EQN), truncated to any specified order. We first explain how to compute the entries of the matrix R. It is convenient, for expository reasons, to frame this computation as an individual step that returns a sparse representation of a submatrix of R corresponding to a subset of the rows. Indeed, in our complexity model dense matrices could not lead to good bounds. We therefore define a matrix representation to be *row-sparse* if iterating over the nonzero entries of any given row does not require any zero test in $\mathbb{K}$. Then, the algorithm essentially amounts to an explicit expression for the coefficients of recurrences similar (2.3), which can as well be computed on the fly.

In view of the computation of ramified solutions (§2.7), Algorithms 1 and 2 accept as input a $\mathbb{K}$-linear transformation ϕ to be applied to the operator L. In general, ϕ will take the form

$$\phi(x^j M^k) = x^{\alpha b^k + \beta j - \gamma} M^k, \qquad \alpha, \gamma \in \mathbb{Z}, \quad \beta \in \mathbb{N}_{>0}, \quad \beta \wedge b = 1, \tag{2.10}$$

with α, β, γ chosen such that $\phi(L)$ has plain (as opposed to Laurent) polynomial coefficients. The reader only interested in polynomial, rational, and power series solutions of L may safely assume $\phi = \mathrm{id}$, i.e., $\alpha = \gamma = 0, \beta = 1$.

Lemma 2.9. *Algorithm 1 computes the submatrix R_E obtained by taking the first w entries of the rows of $R(\phi(L))$ with index $m \in E$ in $\mathrm{O}\big((r+d)|E|\big)$ ops. Each row of R_E has at most $r + 2d$ nonzero entries.*

Proof. Write $\tilde{L} = \sum_{k=0}^{r} \tilde{\ell}_k(x) M^k = \phi(L)$. Recall that the row R_m is obtained by extracting the coefficient of x^m in the equality $\tilde{L}y = 0$, where $y = \sum_{n \geq 0} y_n x^n$. More precisely, $R_{m,n}$ is the coefficient of $y_n x^m$ in the series

$$\tilde{L}y = \sum_{k=0}^{r} \sum_{j=0}^{d} \tilde{\ell}_{k,j} x^j \sum_{n=0}^{\infty} y_n x^{b^k n} = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} \Big(\sum_{j + b^k n = m} \tilde{\ell}_{k,j} \Big) y_n x^m.$$

The definition of ϕ translates into $\tilde{\ell}_{k,j} = 0$ when $j \not\equiv \alpha b^k - \gamma \pmod{\beta}$, and otherwise $\tilde{\ell}_{k,j} = \ell_{k,j'}$ for $j = \alpha b^k + \beta j' - \gamma$. Therefore, $R_{m,n}$ is equal to the sum of $\ell_{k,j'}$ for (k, j') satisfying $\alpha b^k + \beta j' - \gamma = m - n b^k$. For fixed m and k, the coefficient $\ell_{k,j'}$ only contributes when $\beta j' \equiv m + \gamma \pmod{b^k}$. Its contribution is then to $R_{m,n}$ with $n = b^{-k}(B - \beta j')$ where $B = m + \gamma - \alpha b^k$, and we are only interested in $0 \leq n < w$, i.e., $B - b^k w < \beta j' \leq B$. Using the assumption that β is coprime with b, the condition on $\beta j' \pmod{b^k}$ rewrites as $j' \equiv j'_0 \pmod{b^k}$, where j'_0 is the integer computed at step 2b. Therefore, the loop 2c correctly computes the contribution of $\tilde{\ell}_k$ to the entries of index less than w of the row R_{m_i}, and hence the algorithm works as stated.

The only operations in $\mathbb{K}$ performed by the algorithm are one addition and possibly one comparison (to update the sparse structure) at each loop pass over step 2(c)i. The total number of iterations of the innermost loop for a given i is at most

$$\sum_{k=0}^{r} \left\lceil \frac{d_k}{b^k} \right\rceil \leq r + \frac{b}{b-1} d \leq r + 2d$$

and bounds the number of nonzero entries in the row of index m_i. The complexity in ops follows by summing over i. □

According to Proposition 2.6, the number of linearly independent power series solutions and their valuations are determined by a small upper upper left submatrix of R. As a direct attempt at solving the corresponding linear system would have too high a complexity (see Remark 2.11), our approach is to first find a set of candidate solutions, spanning a low-dimensional vector space that contains the approximate series solutions, and to refine the solving in a second step. Geometrically, the idea to obtain a candidate solution $g = g_0 + g_1 x + \cdots$ is to follow the "profile" of R (more precisely, the right boundary of the overlapping strips described in the previous section), using a single equation R_m to try and compute each coefficient g_n from $g_0, \ldots, g_{n-1}$. (That is, for each n, we resolutely skip all but one equations susceptible to determine g_n.) By duality, this corresponds to keeping a varying line of increasing integer slope in contact with the lower Newton polygon, and having it "pivot" around it. In this process, the only case that potentially leaves a degree of freedom in the choice of g_n is when column n contains a "corner" of the profile, corresponding to an edge of the Newton polygon. As a consequence, it is enough to construct at most r independent candidates solutions. The second step then

Input: A linear Mahler operator L of order r. A transformation ϕ of the form (2.10). Integers $h, w \in \mathbb{N}$. A set $E = \{m_0, \dots, m_{w-1}\}$ with $m_0 < \cdots < m_{w-1} < h$, such that the submatrix $(R_{m_i,j})_{0\le i,j<w}$ of $R(\phi(L))$ is lower, resp. upper, triangular, with at most r zeros on the diagonal.

Output: A vector $(f_1, \dots, f_\sigma)$ of polynomials of degree less than w.

(1) Construct the row-sparse submatrix $S_E = (R_{m_i,j})_{0\le i,j<w}$ by Algorithm 1.
(2) Compute a basis of $\ker S_E$ as a matrix $G = (G_{i,j}) \in \mathbb{K}^{w\times\rho}$ by forward, resp. backward, substitution, using the row-sparse structure.
(3) For $1 \le j \le \rho$, set $g_j = G_{0,j} + G_{1,j}x + \cdots + G_{w-1,j}x^{w-1} \in \mathbb{K}[x]$ and compute the coefficients of $Lg_j(x) \bmod x^h = \sum_{0\le i<h} s'_{i,j}x^i$, then form the matrix $S' = (s'_{i,j}) \in \mathbb{K}^{h\times\rho}$.
(4) Compute a basis of $\ker S'$ as a matrix $K \in \mathbb{K}^{\rho\times\sigma}$ by the algorithm of Ibarra, Moran and Hui [14].
(5) Compute $F = (F_{i,j}) = GK \in \mathbb{K}^{w\times\sigma}$.
(6) Return $(f_1, \dots, f_\sigma)$ where $f_j = F_{0,j} + \cdots + F_{w-1,j}x^{w-1}$.

Algorithm 2. Solutions over prescribed monomial support.

consists in recombining the candidates in such a way that the equations R_m that were skipped in the first phase be satisfied.

This strategy is made more precise in Algorithm 2, which will then be specialized to power series solutions (and later to other types of solutions) by a suitable choice of E, h and w. By construction, Algorithm 2 outputs polynomials of degree less than w that are solutions of a subsystem of the linear system induced by L. These polynomials need not *a priori* prolong into actual solutions.

Lemma 2.10. *Algorithm 2 runs in* $\mathrm{O}(rwd + r^2w + r^2\,\mathrm{M}(h))$ *ops, and returns a basis of the kernel of the linear map induced by* $\phi(L)$ *from* $\mathbb{K}[x]_{<w}$ *to* $\mathbb{K}[x]/(x^h)$.

Proof. When S_E is lower, respectively upper, triangular it is possible at step 2 to compute G by forward, respectively backward, substitution, in such a way that $S_EG = 0$. By interpreting the $h \times w$ upper left submatrix S of R as the matrix of a restriction of L to suitable monomial bases, it follows from the definition of S' that $S' = SG$. Step 4 computes K such that $S'K = 0$.

The columns of F, computed as GK at step 5, span the kernel of S: Indeed, assume $Sf = 0$, so that by selecting rows $S_Ef = 0$, and f can be written as $G\gamma$ for some γ. Then, $S'\gamma = SG\gamma = Sf = 0$. But this means that $\gamma = K\eta$ for some η, so that $f = GK\eta = F\eta$. Conversely, we have $SF = SGK = S'K = 0$, so that any vector of the form $F\eta$ belongs to $\ker S$.

Additionally, since the columns of G, respectively those of K, are linearly independent, $GK\eta = 0$ implies $K\eta = 0$, which implies $\eta = 0$. The columns of $F = GK$ hence form a basis of $\ker S$.

By Lemma 2.9, step 1 takes $\mathrm{O}(w(r + d))$ ops. The number of nonzero entries in each row of S_E is bounded by $r + 2d$ by Lemma 2.9, hence the cost of computing ρ linearly independent solutions by substitution at step 2 is $\mathrm{O}(\rho w(r + d))$. As no

Input: A linear Mahler operator L of order r. A transformation ϕ of the form (2.10). A polynomial $\hat{y} = y_0 + \cdots + y_{\lfloor\tilde{\nu}\rfloor} x^{\lfloor\tilde{\nu}\rfloor}$ such that $\phi(L)\,\hat{y} = \mathrm{O}(x^{\lfloor\tilde{\mu}\rfloor+1})$, for $\tilde{\nu}$ and $\tilde{\mu}$ defined by (2.11). An integer n.
Output: A polynomial $y_0 + \cdots + y_{\lfloor\tilde{\nu}\rfloor+n} x^{\lfloor\tilde{\nu}\rfloor+n}$.

(1) Use Algorithm 1 with $E = \{\lfloor\tilde{\mu}\rfloor + 1, \ldots, \lfloor\tilde{\mu}\rfloor + n\}$, $h = \lfloor\tilde{\mu}\rfloor + n + 1$, and $w = \lfloor\tilde{\nu}\rfloor + n + 1$ to construct a submatrix R_E of R.
(2) Solve $R_E\,(y_0, \ldots, y_{\lfloor\tilde{\nu}\rfloor+n})^{\mathrm{T}} = 0$ for $y_{\lfloor\tilde{\nu}\rfloor+1}, \ldots, y_{\lfloor\tilde{\nu}\rfloor+n}$, by forward substitution, starting with the coefficients $y_0, \ldots y_{\lfloor\tilde{\nu}\rfloor}$ given on input.
(3) Return $y_0 + \cdots + y_{\lfloor\tilde{\nu}\rfloor+n} x^{\lfloor\tilde{\nu}\rfloor+n}$.

ALGORITHM 3. Prolonging an approximate series solution to any order.

more than r of the diagonal entries of S_E are zero, ρ is at most r. The computation of each column of S' at step 3 amounts to adding $r+1$ products of the ℓ_k by the $M^k S_i$, truncated to order h, for a total of $\mathrm{O}(r^2\,\mathrm{M}(h))$ ops. As $\rho \le r$, computing the kernel of S' at step 4 via an LSP decomposition (a generalization of the LUP decomposition) requires $\mathrm{O}(hr^{\omega-1}) = o(r^2\,\mathrm{M}(h))$ ops [14]. Finally, the recombination at step 5 takes $\mathrm{O}(wr^{\omega-1}) = o(r^2 w)$ ops as $\sigma \le \rho \le r$. □

Remark 2.11. Note that a direct attempt to solve S, when, say, $\phi = \mathrm{id}$ and $w = \mathrm{O}(d)$, would result in a complexity $\mathrm{O}(d^\omega)$ (e.g., using the LSP decomposition), as opposed to $\mathrm{O}(d^2)$ when using Algorithm 2 and disregarding the dependency in r.

Let $\tilde{v}_k$ be the valuation of the coefficient $\tilde{\ell}_k$ of $\phi(L) = \sum_k \tilde{\ell}_k(x) M^k$. In analogy with (MU-NU), define

$$\tilde{\nu} = \max_{k\ge1} \frac{\tilde{v}_0 - \tilde{v}_k}{b^k - 1}, \qquad \tilde{\mu} = \tilde{v}_0 + \tilde{\nu}. \tag{2.11}$$

We now specialize the generic solver to the computation of approximate series solutions (in the sense of the previous subsection) of $\phi(L)$. The case $\phi = \mathrm{id}$ is formalized as Algorithm 4 on page 15.

Proposition 2.12. *Assume $\tilde{\nu} \ge 0$. Algorithm 2, called with*

$$h = \lfloor\tilde{\mu}\rfloor + 1, \quad w = \lfloor\tilde{\nu}\rfloor + 1, \quad E = \big(\min_k(\tilde{v}_k + nb^k)\big)_{0\le n<w},$$

runs in $\mathrm{O}(rd\tilde{v}_0 + r^2\,\mathrm{M}(\tilde{v}_0))$ ops and returns a basis of approximate series solutions of the equation $\phi(L)\,y = 0$.

Proof. First of all, when $m = m_i \in E$, none of the terms $\tilde{\ell}_k M^k$ of $\phi(L)$ contributes to the entries of S located above $S_{m,n}$. The matrix S_E is thus lower triangular. In addition, $R_{m,n}$ is zero (if and) only if $-n$ is an (admissible) slope of the lower Newton polygon, so that no more than r of the diagonal entries of S_E are zero. Both preconditions of Algorithm 2 are therefore satisfied. By Proposition 2.6 and Lemma 2.10, it follows from the choice of h and w that the f_j form a basis of approximate series solutions. Using the inequalities $h \le bv_0/(b-1) + 1 = \mathrm{O}(\tilde{v}_0)$ and $w \le v_0/(b-1) + 1 = \mathrm{O}(\tilde{v}_0)$ in the formula of Lemma 2.10, the total complexity is as announced. □

Input: A linear Mahler operator L of order r.
Output: A basis $(f_1, \dots, f_\sigma)$ of approximate series solutions of L.

Let μ, ν be as defined by (MU-NU). If $\nu < 0$, return $()$. Otherwise, call Algorithm 2 with $\phi = \mathrm{id}$,

$$h = \lfloor \mu \rfloor + 1, \quad w = \lfloor \nu \rfloor + 1, \quad E = \big(\min_k (v_k + nb^k)\big)_{0 \le n < w},$$

and return the result.

ALGORITHM 4. Approximate series solutions.

Given an approximate series solution, the next terms of the corresponding series solutions can be computed efficiently one by one using simple recurrence formulae.

Proposition 2.13. *Given an approximate series solution $\hat{y} = y_0 + \cdots + y_{\lfloor \tilde{\nu} \rfloor} x^{\lfloor \tilde{\nu} \rfloor}$ of (EQN), Algorithm 3 computes the truncation to the order $\mathrm{O}(x^{\lfloor \tilde{\nu} \rfloor + n})$ of the unique solution y of (EQN) of the form $y = \hat{y} + \mathrm{O}(x^{\lfloor \tilde{\nu} \rfloor + 1})$ in $\mathrm{O}((r+d)\,n)$ ops.*

Proof. By Proposition 2.6, the system to be solved at step 2 is compatible. According to the description of R provided above, the submatrix $(R_{m,n})_{m > \lfloor \tilde{\mu} \rfloor, n > \lfloor \tilde{\nu} \rfloor}$ is lower triangular, with nonzero diagonal coefficients, so that the system can be solved by forward substitution. As explained in §2.4, the output is a truncation of a solution of $\phi(L)$. By Lemma 2.9, the cost in ops of step 1 is $\mathrm{O}((r+d)\,n)$, and each row of S contains at most $r + 2d$ nonzero entries. Therefore, step 2 costs $\mathrm{O}((r+d)\,n)$ ops. □

2.6. **Polynomial solutions.** Our goal in this subsection is Algorithm 6, which computes a basis of all polynomial solutions. Lemma 2.5 provides us with an upper bound $d/(b^r - b^{r-1}) + 1 = \mathrm{O}(d/b^r)$ for the degree of any polynomial solution. Before we take this into account, we provide an algorithm to compute polynomial solutions with degree bounded by $w \ge 0$, which runs in a complexity that is sensitive to w.

In the same way as in Proposition 2.12, to obtain candidate polynomial solutions $f = f_0 + \cdots + f_{w-1} x^{w-1}$, we set $f_n = 0$ for $n \ge w$ and then compute f_n for decreasing n by "following" the "left profile" of the matrix R (or, dually, the upper Newton polygon). The corresponding specialization of Algorithm 2 is formalized as Algorithm 5.

Proposition 2.14. *Assume $\nu \ge 0$. Algorithm 2, called with $\phi = \mathrm{id}$ and*

$$h = d + (w-1)b^r + 1, \qquad E = \big(\max_k (d_k + nb^k)\big)_{0 \le n \le w}, \tag{2.12}$$

returns a basis of the space of polynomial solutions of (EQN) of degree less than w. For $w = \mathrm{O}(d/b^r)$, the algorithm runs in $\tilde{\mathrm{O}}(wd + \mathrm{M}(d))$ ops.

Proof. The proof is similar to that of Proposition 2.12: the extracted submatrix of R is now upper triangular; the zeros on its diagonal correspond to the admissible nonpositive integer slopes of the upper Newton polygon; the number of such zeros is not more than r. Both preconditions of Algorithm 2 are therefore satisfied and Lemma 2.10 applies. Additionally, the choice of h in terms of w is such that $\deg(Ly) < h$ whenever $\deg y < w$ for a polynomial y. So, the basis returned is that of the kernel of the map induced by L from $\mathbb{K}[x]_{<w}$ to $\mathbb{K}[x]$, as announced.

Input: A linear Mahler operator L of order r. An integer $w \in \mathbb{N}$.
Output: A basis $(f_1, \dots, f_\sigma)$ of the polynomial solutions of L of degree less than w.

Let μ, ν be as defined by (MU-NU). If $\nu < 0$, return (). Otherwise, call Algorithm 2 with $\phi = \mathrm{id}$,

$$h = \max_k d_k + (w-1)b^r + 1, \quad w, \quad E = \big(\max_k(d_k + nb^k)\big)_{0 \le n < w},$$

and return the result.

ALGORITHM 5. Polynomial solutions of bounded degree.

Input: A linear Mahler operator L of order r.
Output: A basis $(f_1, \dots, f_\sigma)$ of all polynomial solutions of L.

Call Algorithm 5 with $w = \left\lfloor \frac{\max_k d_k}{b^{r-1}(b-1)} \right\rfloor + 1$ and return the result.

ALGORITHM 6. Basis of polynomial solutions.

For the complexity result, the hypothesis on w implies $h = \mathrm{O}(d)$ and $r = \mathrm{O}(\log_b d)$, so that the conclusion of Lemma 2.10 specializes to $\tilde{\mathrm{O}}(wd + \mathrm{M}(d))$ ops. □

Remark 2.15. The loose bound on w, namely $w = \mathrm{O}(d/b^r)$, permits in particular to obtain a result when d is not the maximal degree of the ℓ_k, but only bounds them up to a multiplicative constant. In this case, the complexity announced by Proposition 2.14 specializes to the same complexity as in Corollary 2.16. This will be used for the numerators of rational-function solutions in §3.5.

By Lemma 2.5, the degree of any polynomial solution is bounded above by $\delta_0 = d/(b^r - b^{r-1}) + 1$. Specializing Proposition 2.14 to $w = \lfloor \delta_0 \rfloor$, we obtain a bound for the complexity of computing the whole space of polynomial solutions.

Corollary 2.16. *Assuming $\nu \ge 0$, Algorithm 2, called with $\phi = \mathrm{id}$,*

$$h = 3d + 1, \qquad w = \left\lfloor \frac{d}{b^{r-1}(b-1)} \right\rfloor + 1, \qquad E = \big(\max_k(d_k + nb^k)\big)_{0 \le n \le w},$$

computes a basis of the polynomial solutions of (EQN) in $\tilde{\mathrm{O}}(d^2/b^r + \mathrm{M}(d))$ ops.

Proof. Observe that the choice for w induces that h, as defined in Algorithm 6, satisfies $h \le 3d + 1$. The result follows from this fact and $w = \mathrm{O}(d/b^r)$. □

2.7. **Puiseux series solutions.** We now discuss the computation of solutions of (EQN) in $\mathbb{K}((x^{1/*}))$. Even though Proposition 1.1 does not apply, we still assume that the coefficient ℓ_0 of L is nonzero. There is no loss of generality in doing so: if $L = L_1 M^w$ for some $w \in \mathbb{N}$, then the Puiseux series solutions of L are exactly the $y(x^{b^{-w}})$ where y ranges over the Puiseux series solutions of L_1. Additionally, the order of L_1 is bounded by that of L, so that the complexity estimates depending on it will still hold (and equations of order zero that result from the transformation when $r = w$ have no nontrivial solutions).

The computation of solutions $y \in \mathbb{K}((x^{1/N}))$ with a given ramification index N is similar to that of power series solutions. In order to compute a full basis of solutions in $\mathbb{K}((x^{1/*}))$, however, we need a bound on the ramification index necessary to express them all. Lemma 2.17, communicated to us by Dreyfus and Roques, and Proposition 2.19 below provide constraints on the possible ramification indices.

Lemma 2.17. *If $y \in \mathbb{K}((x^{1/*}))$ is a Puiseux series such that $Ly \in \mathbb{K}((x^{1/q'}))$ where q' is coprime with b, then $y \in \mathbb{K}((x^{1/q}))$ for some q coprime with b.*

Proof. Let q_0 be the smallest positive integer such that $y \in \mathbb{K}((x^{1/q_0}))$. Set $g = q_0 \wedge b$ and $q'' = q_0/g$, so that $My \in \mathbb{K}((x^{b/q_0})) \subset \mathbb{K}((x^{1/q''}))$. The expression

$$y = \ell_0^{-1} \left(Ly - (\ell_1 + \cdots + \ell_r M^{r-1}) My \right)$$

shows that $y \in \mathbb{K}((x^{1/q_1}))$ where $q_1 = q'q''$. By minimality of q_0, we have $q_1 = kq_0$ for some $k \in \mathbb{N}$, which simplifies to $q' = kg$. Since q' was assumed to be coprime with b, this implies $g = 1$. □

Remark 2.18. Some non-Puiseux formal series solutions of Mahler equations with $\ell_0 \neq 0$ do involve ramifications of order divisible by b: perhaps the simplest example, akin to [7, p. 64] (see also [1]), is $y = x^{1/b} + x^{1/b^2} + x^{1/b^3} + \cdots$, which satisfies $(M - x^{b-1})(M - 1)\, y = 0$.

The following proposition formalizes, as a consequence of Lemma 2.17 and the properties of Newton polygons discussed in §2.2, that no ramification is needed beyond those present in the candidate leading terms given by the Newton polygon. Call $\mathcal{N}$ the lower Newton polygon of L, and let Q denote the set of denominators q of slopes (written in lowest terms) of admissible edges of $\mathcal{N}$ such that $q \wedge b = 1$.

Proposition 2.19. *Any Puiseux-series solution y of $Ly = 0$ belongs to $\mathcal{V} = \sum_{q \in Q} \mathbb{K}((x^{1/q}))$. In particular, the space of solutions of L in $\mathbb{K}((x^{1/*}))$ is contained in $\mathbb{K}((x^{1/N}))$, where $N \leq b^r - 1$ denotes the lcm of the elements of Q.*

Proof. Let $y \in \mathbb{K}((x^{1/*}))$ satisfy $Ly = 0$, and suppose by contradiction that y contains a nonzero term of exponent p_1/q_1 where $p_1 \wedge q_1 = 1$ and q_1 does not divide any element of Q. Choose p_1/q_1 minimal with these properties. Write $y = y_0 + y_1$ where y_0 consists of the terms of y with exponent strictly less than p_1/q_1, so that $y_0 \in \mathcal{V}$ and y_1 has valuation p_1/q_1. Then $g = Ly_0$ belongs to $\mathcal{V}$, so that there exists $q' \in \mathbb{N}$ for which $q' \wedge b = 1$ and $g \in \mathbb{K}((x^{1/q'}))$. Since $Ly_1 = -g$, Lemma 2.17 implies that $y_1 \in \mathbb{K}((x^{1/q}))$ for some q coprime with b. In particular, q_1 is coprime with b.

Since p_1/q_1 is the valuation of a solution of the equation $Lz = -g$, its opposite $s = -p_1/q_1$ is the slope of an admissible edge $\mathcal{E}$ of the lower Newton polygon $\mathcal{N}_g$ of $(L, -g)$ (see §2.3). On the other hand, because of the definition of Q and the properties $q_1 \wedge b = 1$ and $q_1 \notin Q$, the edge $\mathcal{E}$ cannot be an edge of $\mathcal{N}$. Therefore, by the description in §2.3, g must be nonzero and the edge $\mathcal{E}$ must be the leftmost edge of $\mathcal{N}_g$. The valuation of $g \in \mathcal{V}$ is thus a rational number p_0/q_0 (not necessarily in lowest terms) with $q_0 \in Q$, so that in particular $q_0 \wedge b = 1$. As s is the slope of $\mathcal{E}$ in $\mathcal{N}_g$, it is of the form $(q_0 v_k - p_0)/(q_0 b^k)$ for some $k \in \{0, \ldots, r\}$. Then, q_1 divides $q_0 b^k$. As it is coprime with b, this implies that q_1 divides $q_0 \in Q$, a contradiction. We have proved that y belongs to $\mathcal{V}$.

Next, it is clear that $\mathcal{V}$ is contained in $\mathbb{K}((x^{1/N}))$. Finally, letting (b^{k_i}, v_i) denote the vertices of $\mathcal{N}$ (sorted from left to right as i increases), the lcm N satisfies $N \leq \prod_i (b^{k_{i+1} - k_i} - 1) < b^r$, as claimed. □

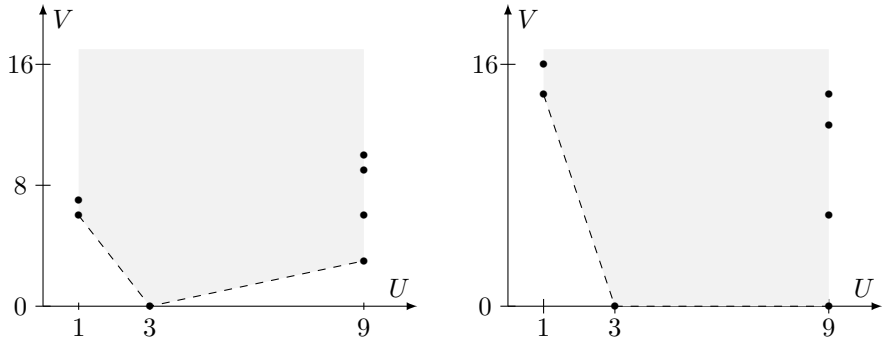

FIGURE 3. The transformation in Example 2.22 puts the edge with slope 1/2 of the lower Newton polygon of L (left) onto the U-axis (Newton polygon of $\tilde{L}$, right).

Remark 2.20. The bound $N < b^r$ is tight, as shown by the example of $M^r - x$, which admits the solution $x^{1/(b^r-1)}$.

In order to obtain an algorithm that computes a basis of the space of Puiseux series solutions, there remains to generalize the results of §2.4–2.5 to the case of solutions lying in $\mathbb{K}((x^{1/N}))$ where N is given. Motivated by the structure of the space $\mathcal{V}$ described in Proposition 2.19, we do not require here that N be equal to the lcm of all elements of Q: setting it to the lcm of any subset of these elements also makes sense. For the most part, the algorithms searching for power series solutions apply *mutatis mutandis* when the indices m and n are allowed to take negative and noninteger rational values. Nevertheless, some care is needed in the complexity analysis, so we explicitly describe a way to reduce the computation of ramified solutions of L to that of power series solutions of an operator $\tilde{L}$.

Denote $x = t^\beta$, and consider the change of unknown functions $y(x) = t^\alpha z(t)$, for $\alpha \in \mathbb{Z}$ and $\beta \in \mathbb{N}_{>0}$ to be determined. Observe that $Mt = t^b$. If $y(x)$ is a solution of $Ly = 0$, then $z(t)$ is annihilated by

$$\tilde{L} = t^{-\gamma} L\, t^\alpha = t^{-\gamma} \sum_{k=0}^{r} t^{\alpha b^k} \ell_k(t^\beta) M^k = \sum_{k=0}^{r} \tilde{\ell}_k(t) M^k$$

where $\gamma \in \mathbb{Z}$ can be adjusted so that the $\tilde{\ell}_k$ belong to $\mathbb{K}[t]$. We then have $\tilde{L} = \phi(L)$ where ϕ is the $\mathbb{K}$-linear map, already introduced in §2.5, that sends $x^j M^k$ to

$$\phi(x^j M^k) = t^{-\gamma} t^{\beta j} M^k t^\alpha = t^{-\gamma+\beta j+\alpha b^k} M^k. \tag{2.13}$$

Viewing monomials $x^j M^k$ as points in the plane of the Newton diagram, the map ϕ induces an affine shearing

$$[\phi] : \begin{pmatrix} b^k \\ j \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ \alpha & \beta \end{pmatrix} \begin{pmatrix} b^k \\ j \end{pmatrix} + \begin{pmatrix} 0 \\ -\gamma \end{pmatrix}. \tag{2.14}$$

As in §2.5, denote by $\tilde{v}_k$ and $\tilde{d}_k$ the valuations and degrees of the coefficients of $\tilde{L}$, and by $\tilde{\mu}$ and $\tilde{\nu}$ the quantities defined by (MU-NU) with v_k replaced by $\tilde{v}_k$.

Lemma 2.21. *Fix an edge S_0 of the lower Newton polygon of L, of slope $-p/q$ for (not necessarily coprime) $p \in \mathbb{Z}$ and $q \in \mathbb{N}$. Let c be the V-intercept of the line supporting S_0. Set $\alpha = p$, $\beta = q$, and $\gamma = qc$ in (2.13). Then:*

(a) *the operator* $\tilde{L} = \phi(L)$ *has polynomial coefficients;*
(b) *its Newton diagram is the image of that of* $\tilde{L}$ *by* $[\phi]$*, with the edge* S_0 *being mapped to a segment of the U-axis;*
(c) *in terms of those of* L*, the parameters associated to* $\tilde{L}$ *satisfy*

$$\tilde{d}_k = -qc + pb^k + qd_k \geq \tilde{v}_k = -qc + pb^k + qv_k \geq 0,$$
$$\tilde{\nu} = q\nu - p \geq 0, \qquad \tilde{\mu} = q(\mu - c) \geq 0.$$

Proof. Observe that qc is equal to the common value on S_0 of $pU + qV$. Since the endpoints of S_0 have integer coordinates, this value is an integer, and hence the coefficients of $\tilde{L}$ are Laurent polynomials. The transformation $[\phi]$ of the Newton plane maps segments of slope s to segments of slope $(\alpha + \beta s)/(1 + 0 \cdot s) = p + qs$, and in particular maps S_0 to a horizontal segment. By the choice of c, that segment lies on the U-axis. Since $q > 0$, images by $[\phi]$ of points above S_0 lie above $[\phi](S_0)$. As monomials of L correspond to points lying on or above S_0, their images by ϕ are monomials of nonnegative degree. This proves assertion (a). It follows that $\tilde{L}$ has a Newton diagram in the sense of our definition, and it is then clear this Newton diagram is as stated by (b). The expressions of $\tilde{v}_k$ and $\tilde{d}_k$ in (c) are a consequence of (2.13), using again the positivity of β. Those of $\tilde{\nu}$ and $\tilde{\mu}$ follow. We already observed that $\tilde{v}_k \geq 0$. Finally, $-\tilde{\nu}$ and $\tilde{\mu}$ are, respectively, the slope and V-intercept of the leftmost edge of the lower Newton polygon $\tilde{\mathcal{N}}$ of $\tilde{L}$. Since $\tilde{\mathcal{N}}$ has a horizontal edge, $\tilde{\nu}$ and $\tilde{\mu}$ are nonnegative. □

Example 2.22. Consider again the Mahler operator L in (2.1) treated for $b = 3$ in §2.1. We already observed that the slopes of the Newton polygon of L are -3 and $1/2$ and that they are admissible, and, in §2.1, we performed the transformation (2.13) for the parameters $\alpha = -1$, $\beta = 2$, and $\gamma = -3$, to obtain the operator $\tilde{L}$ in (2.5). The slopes of the Newton polygon of $\tilde{L}$ are -7 and 0 and are both admissible.

Theorem 2.23. *Algorithm 7 runs in*

$$\mathrm{O}(r^2\,\mathrm{M}(Nd) + rN(d^2 + (r+d)\,n)) = \tilde{\mathrm{O}}(r^2 Nd\,(d+n))\ \textit{ops}$$

(assuming a softly linear-time polynomial multiplication) and computes the truncation to order $\mathrm{O}(x^{n+1})$ *of a basis of solutions of* (EQN) *in* $\mathbb{K}((x^{1/N}))$.

Proof. The discussion at the beginning of this section shows that $z(x) \in \mathbb{K}((x^{1/*}))$ is a solution of the operator $\tilde{L}$ computed at step 2 if and only if $y(x) = x^{-s} z(x^{1/N})$ is a solution of L. By Lemma 2.2 and the choice of s, solutions of L in $\mathbb{K}((x^{1/N}))$ have valuation at least $-s$, and hence correspond to solutions of $\tilde{L}$ lying in $\mathbb{K}[[x]]$. Since the mapping $z \mapsto y$ is linear and invertible, a basis of solutions of $\tilde{L}$ in $\mathbb{K}[[x]]$ provides a basis of solutions of L in $\mathbb{K}((x^{1/N}))$.

Let S_0 be the edge of the Newton polygon of L considered at step 1, so that the notation of the algorithm agrees with that of Lemma 2.21. Lemma 2.21(c) then provides expressions various parameters associated to $\tilde{L}$ in terms of s, c, and quantities that can be read off L. Since $\tilde{\nu}$ is nonnegative, Proposition 2.12 applies and shows that step 3 computes a basis $(f_1, \ldots, f_\sigma)$ of the space of approximate solutions of $\tilde{L}$ in $\mathbb{K}[[x]]$ in $\mathrm{O}(rd\tilde{v}_0 + r^2\,\mathrm{M}(\tilde{v}_0))$ ops. Denote by $(z_1, \ldots, z_\sigma)$ the basis of power series solutions of $\tilde{L}$ such that each z_i extends f_i. Then, according to Proposition 2.13, the series $\hat{z}_i$ computed at step 4 satisfy $z_i = \hat{z}_i + \mathrm{O}(x^{N(s+n)+1})$,

Input: A linear Mahler operator L as in (OPR). A ramification index $N \in \mathbb{N}_{>0}$. A truncation order $n \in \mathbb{N}$.
Output: A vector $(\hat{y}_1, \dots, \hat{y}_\sigma)$ of truncated Puiseux series.

(1) Compute the slope s and V-intercept c of the rightmost admissible edge of the lower Newton polygon of L with slope in $N^{-1}\mathbb{Z}$.
(2) Define ϕ and $\tilde{L} = \phi(L)$ according to (2.13), with $\alpha = -Ns$, $\beta = N$, and $\gamma = Nc$.
(3) Call Algorithm 2 on L and ϕ, with
$$h = \lfloor \tilde{\mu} \rfloor + 1, \quad w = \lfloor \tilde{\nu} \rfloor + 1, \quad E = \big(\min_k(\tilde{v}_k + nb^k)\big)_{0 \le n < w},$$
where $\tilde{\mu}$, $\tilde{\nu}$ and $\tilde{v}_k$ are given by Lemma 2.21(c), to compute a vector $(f_1, \dots, f_\sigma)$ of approximate power series solutions of $\tilde{L}z = 0$.
(4) For $i = 1, \dots, \sigma$, call Algorithm 3 to compute $\tilde{n} = \max(0, N(s+n) - \lfloor \tilde{\nu} \rfloor)$ additional terms of f_i, thus extending it to a truncated power series solution $\hat{z}_i = z_0 + \cdots + z_{N(s+n)}x^{N(s+n)}$ of $\tilde{L}$.
(5) Return $(\hat{y}_1, \dots, \hat{y}_\sigma)$ where $\hat{y}_i = z_0 x^{-s} + z_1 x^{-s+1/N} + \cdots + z_{N(s+n)} x^n$.

ALGORITHM 7. Solving a Mahler equation in $\mathbb{K}((x^{1/N}))$.

and their computation takes $\mathrm{O}(\sigma(r+d)\tilde{n})$ ops. Finally, the truncated Puiseux series returned by the algorithm satisfy $\hat{y}_i = x^{-s}\hat{z}_i(x^{1/N})$, hence are truncations of elements of a basis of solutions of $\tilde{L}$ in $\mathbb{K}((x^{1/N}))$.

Steps other than 3 and 4 do not perform any operation in $\mathbb{K}$, so that the cost in ops of the algorithm is concentrated in those two steps. Let (b^{k_1}, v_{k_1}) and (b^{k_2}, v_{k_2}) with $k_1 < k_2$ be the endpoints of S_0, so that

$$qc = pb^{k_1} + qv_{k_1} = pb^{k_2} + qv_{k_2}. \tag{2.15}$$

Lemma 2.21(c) gives $\tilde{v}_0 = qv_0 + p - qc$. If $p \ge 0$, then (2.15) implies $qc \ge p$ and hence $\tilde{v}_0 \le qv_0 \le Nd$. If, now, $p < 0$, first observe that since $b^{k_2} \ge 2b^{k_1}$, we have $-pb^{k_1} \le -p(b^{k_2} - b^{k_1}) = q(v_{k_2} - v_{k_1})$. It follows that $-qc = -pb^{k_1} - qv_{k_1} \le qv_{k_2}$, whence $\tilde{v}_0 \le q(v_0 + v_{k_2}) \le 2Nd$. In both cases, we have proved that $\tilde{v}_0 = \mathrm{O}(Nd)$. The complexity estimate for step 3 thus rewrites as $\mathrm{O}(rNd^2 + r^2\,\mathrm{M}(Nd))$ ops. As $s \le d$ (because all slopes of the Newton polygon are bounded by d in absolute value) and $\sigma \le r$, that of step 4 becomes $\mathrm{O}(rN(r+d)(d+n))$ ops. The total running time is therefore $\mathrm{O}(r^2\,\mathrm{M}(Nd) + rN(d^2 + (r+d)\,n))$ ops. □

Recall that Q denotes the set of denominators q of slopes, written in lowest terms, of admissible edges of $\mathcal{N}$ such that $q \wedge b = 1$.

Corollary 2.24. *Algorithm 7 with N set to the lcm of elements in Q, returns the truncation to order $\mathrm{O}(x^{n+1})$ of a basis of solutions of (EQN) in $\mathbb{K}((x^{1/*}))$ in $\tilde{\mathrm{O}}(r^2 b^r d(d+n))$ ops, assuming $\mathrm{M}(k) = \tilde{\mathrm{O}}(k)$.*

Proof. This follows by combining Proposition 2.19 with Theorem 2.23. □

Example 2.25. With $b = 3$, let us consider the order $r = 11$ Mahler operator

$$\begin{aligned} L = {} & x^{568} - (x^{1218} + x^{1705})M + x^{3655}M^2 - (x^{162} - x^{10962})M^3 \\ & + (1 + x^{487} - x^{4104} - x^{4536} - x^{32887})M^4 - (x - x^{11826} - x^{12313} - x^{13122} - x^{13609})M^5 \\ & - (1 + x^{35479} + x^{39367})M^6 + (x + x^{95634} - x^{106434} - x^{118098})M^7 \\ & - (x^{286416} + x^{286903} - x^{319303} - x^{354295})M^8 + x^{859249}M^9 \\ & + x^{2577744}M^{10} - x^{7733233}M^{11}. \end{aligned}$$

Its associated parameters are $w = 0$, $v_0 = 568$, and a Newton polygon made from five segments, all admissible, with slopes $-203/13$, -3, 0, $1/1458$, and $221/5$. Except for $1458 = 2 \cdot 3^6$, the denominators are coprime with $b = 3$ and their lcm is $N = 65$. The rightmost slope is $s = 221/5$ and we perform the change of variables of Algorithm 7 with $\alpha = -2873$, $\beta = 65$, hence $\gamma = -6283186$ and this provides us with the new operator

$$\begin{aligned} \tilde{L} = {} & t^{6317233} - (t^{6353737} + t^{6385392})M + t^{6494904}M^2 - (t^{6216145} - t^{6918145})M^3 \\ & + (t^{6050473} + t^{6082128} - t^{6317233} - t^{6345313} - t^{8188128})M^4 \\ & - (t^{5585112} - t^{6353737} - t^{6385392} - t^{6437977} - t^{6469632})M^5 \\ & - (t^{4188769} - t^{6494904} - t^{6747624})M^6 + (1 + t^{6216145} - t^{6918145} - t^{7676305})M^7 \\ & - (t^{6050473} + t^{6082128} - t^{8188128} - t^{10462608})M^8 + t^{5585112}M^9 + t^{4188769}M^{10} - M^{11}. \end{aligned}$$

We want to find a basis of Puiseux solutions for L with a precision $\mathrm{O}(x^n)$ where $n = 10^6$. According to Algorithm 7, this leads us to compute a basis of formal series solutions for $\tilde{L}$ with a precision $\mathrm{O}(x^{\tilde{n}})$ where $\tilde{n} = 65002873$. We first apply Algorithm 4 with $\tilde{\nu} = 3888$, $\tilde{\mu} = 6321121$. The computation shows that the space of solutions has dimension 2. We extend the solutions to the requested precision by Algorithm 3 and we obtain a basis of formal series solutions

$$\begin{aligned} \tilde{f}_1(t) = {} & 1 + t^{28080} + t^{657072} + t^{2274480} + t^{2302560} + t^{17639856} + t^{53222832} \\ & + t^{53250912} + t^{62068032} + \mathrm{O}\left(t^{65002873}\right), \end{aligned}$$

$$\begin{aligned} \tilde{f}_2(t) = {} & t^{3888} + t^{314928} + t^{343008} + t^{9160128} + t^{25509168} + t^{25537248} \\ & + t^{27783648} + t^{27811728} + \mathrm{O}\left(t^{65002873}\right). \end{aligned}$$

Reversing the change of variable, we find the basis

$$\begin{aligned} f_1(x) = {} & x^{-\frac{221}{5}} + x^{\frac{1939}{5}} + x^{\frac{50323}{5}} + x^{\frac{174739}{5}} + x^{\frac{176899}{5}} + x^{\frac{1356691}{5}} + x^{\frac{4093843}{5}} \\ & + x^{\frac{4096003}{5}} + x^{\frac{4774243}{5}} + \mathrm{O}\left(x^{1000000}\right), \end{aligned}$$

$$\begin{aligned} f_2(x) = {} & x^{\frac{203}{13}} + x^{\frac{62411}{13}} + x^{\frac{68027}{13}} + x^{\frac{1831451}{13}} + x^{\frac{5101259}{13}} + x^{\frac{5106875}{13}} \\ & + x^{\frac{5556155}{13}} + x^{\frac{5561771}{13}} + \mathrm{O}\left(x^{1000000}\right). \end{aligned}$$

These truncated series satisfy $Lf_1 = \mathrm{O}(x^e)$, $Lf_2 = \mathrm{O}(x^e)$ with $e = v_0 + n = 1000568$.

3. Rational solutions

We now turn to the computation of rational function solutions of Mahler equations of the form (EQN). Our algorithm follows a classical pattern: it first computes a *denominator bound*, that is, a polynomial that the denominator of any (irreducible) rational solution must divide. Then it makes a change of unknown functions and computes the possible numerators using the algorithm of §2.6. As is usual with other functional equations, the denominator bound is obtained by analyzing the action of the operator L on zeros and poles of the functions it is applied to.

3.1. **Denominator bounds: setting.** We will call a rational function $p/(x^{\bar v}q)$ *in lowest terms* if it satisfies the following conditions: $\bar v \geq 0$; $p, q \in \mathbb{K}[x]$ are coprime polynomials; $q(0) \neq 0$; and $p(0)$ can be zero only if $\bar v = 0$.

Consider a rational solution $p/(x^{\bar v}q)$ of (EQN), written in lowest terms. We already know from Lemma 2.2 that $\bar v \leq v_r/(b^r - b^{r-1})$, so we are left with the problem of finding a multiple of q.

Write $Ta = \bigvee_{i=0}^{r-1} M^i a$. We will freely use the fact that $T(ab) \mid (Ta)\,(Tb)$ for all a and b. For any j between 0 and r, multiplying the equation

$$\ell_r(x)M^r y + \cdots + \ell_1(x)\,My + \ell_0(x)y = 0,$$

by $(M^r x^{\bar v})\,(M^j q) \bigvee_{i\neq j} M^i q$ and reducing modulo $M^j q$ yields

$$M^j q \mid x^{(b^r-b^j)\bar v}\ell_j\,(M^j p) \bigvee_{i\neq j} M^i q. \tag{3.1}$$

As q is coprime with p and $q(0) \neq 0$, Equation (3.1) with $j = r$ implies

$$M^r q \mid \ell_r\, Tq. \tag{3.2}$$

This relation is our starting point for computing a polynomial $q^\star$, depending only on ℓ_r, such that $q \mid q^\star$.

The algorithm for this task, presented in §3.3, operates with polynomials over $\mathbb{K}$, but it may be helpful in order to get an intuition to first consider the case $\mathbb{K} = \mathbb{C}$. Assume for simplicity that q is squarefree. Equation (3.2) then says that, if α is a zero of q, each of its b^rth roots is either a b^kth root with $k < r$ of some zero of q or a zero of ℓ_r. Thus, when α is not a root of unity, its b^rth roots are either zeros of ℓ_r or roots of lower order of some *other* zero of q, whose b^rth roots then satisfy the same property. (Compare Lemma 3.4 below.) As q has finitely many zeros, this cannot continue indefinitely, so, in this case, we will eventually find a zero α whose b^rth roots are zeros of ℓ_r. A difficulty arises when α is a root of unity, but then at most one of its bth roots can be part of a cycle of the map $\zeta \mapsto \zeta^b$ (cf. Lemma 3.6), and a closer examination shows that the $b - 1$ other roots behave essentially like non-roots of unity.

3.2. **Properties of the Mahler and Gräffe operators.** Going back to the general case, and before making the reasoning sketched above more precise, let us state a few properties of the action of M on polynomials. Besides M, we consider the *Gräffe operator* defined by

$$G : \mathbb{K}[x] \to \mathbb{K}[x], \quad p \mapsto \operatorname{Res}_y(y^b - x, p(y)).$$

In other words, Gp is the product $p(x^{1/b})p(\zeta x^{1/b}) \cdots p(\zeta^{b-1}x^{1/b})$ for any primitive bth root of unity ζ. While M maps a polynomial p to a polynomial whose complex

zeros are the bth roots of the zeros of p, the zeros of Gp are the bth powers of the zeros of p.

As a direct consequence of the definitions, M and G act on degrees by:

$$\deg Mp = b \deg p, \qquad \deg Gp = \deg p.$$

Some other elementary properties that will be useful in the sequel are as follows.

Lemma 3.1. *For any nonzero $i \in \mathbb{N}$, the following relations between M and G hold for all $p, q \in \mathbb{K}[x]$:*

(a) $G^i M^i p = p^{b^i}$,
(b) $p \mid M^i G^i p$,
(c) $p \mid q \iff M^i p \mid M^i q$.

Proof. The case $i > 1$ reduces to the case $i = 1$ by changing the radix, since M^i (resp. G^i) is nothing but the Mahler (resp. Gräffe) operator of radix b^i; so we set $i = 1$. The assertions (a) and (b) are direct consequences of the definition of G as a resultant. The direct implication in (c) is clear. For the converse, write the Euclidean division $q = up + v$. If $Mq = sMp$ for some $s \in \mathbb{K}[x]$, then $(Mu)(Mp) + (Mv) = sMp$, whence $Mv = 0$ since $\deg Mv < \deg Mp$. □

Lemma 3.2. *If $p \in \mathbb{K}[x]$ is monic irreducible and $i \in \mathbb{N}$, then $G^i p = q^e$ for some monic irreducible $q \in \mathbb{K}[x]$ and $e \in \mathbb{N}$. Furthermore, $G^i p = p$ if and only if p divides $M^i p$. If this holds for $i > 0$, $G^j p$ is monic irreducible for any $j \in \mathbb{N}$.*

Proof. To prove the first point, consider the factorization $G^i p = c q_1^{e_1} \cdots q_s^{e_s}$ of $G^i p$ for monic irreducible and pairwise coprime q_j and a nonzero $c \in \mathbb{K}$. Because of Lemma 3.1(c), the polynomials $M^i q_1^{e_1}, \dots, M^i q_s^{e_s}$ are pairwise coprime. We have

$$M^i G^i p = c\,(M^i q_1^{e_1}) \cdots (M^i q_s^{e_s}),$$

and, by Lemma 3.1(b), $p \mid M^i q_j^{e_j}$ for some j. It follows that $G^i p \mid G^i M^i q_j^{e_j} = q_j^{e_j b^i}$ by Lemma 3.1(a), proving the first point.

Now if $p \mid M^i p$, then $G^i p \mid p^{b^i}$, and necessarily there is $e \in \mathbb{N}$ such that $G^i p = p^e$. In fact, $e = 1$ and $G^i p = p$ as $G^i p$ and p have the same degree and p is irreducible. Conversely, if $G^i p = p$, then p divides $M^i p$ by Lemma 3.1(b).

Assume $G^i p = p$ for some $i > 0$. Let $j \in \mathbb{N}$ and $m \in \mathbb{N}$ such that $mi \geq j$. Then $p = G^{mi} p = G^{mi-j}(G^j p)$ is monic irreducible, so that $G^j p$ is monic irreducible too. □

Lemma 3.3. *Let $f \in \mathbb{K}[x]$ be a nonconstant polynomial with $f(0) \neq 0$. If f and its derivative f' are coprime, so are Mf and $(Mf)'$.*

Proof. Assume $f \wedge f' = 1$. Applying M to a Bézout relation shows that $Mf \wedge M(f') = 1$. Now, $(Mf)' = bx^{b-1} M(f')$, so a common factor s of Mf and $(Mf)'$ must divide x. As x cannot divide Mf because $x \nmid f$, the only possibility is that s be a constant. □

The following lemma generalizes the fact that the iterated bth roots of a complex number $\alpha \neq 0$ are all distinct, except in some cases where α is a root of unity.

Lemma 3.4. *Let $p \in \mathbb{K}[x]$ be monic and irreducible. For general $\mathbb{K}$, $M^i p$ and $M^j p$ are coprime for all $i > j \geq 0$ if none of the $G^i p$ for $i \geq 1$ is equal to p. When $\mathbb{K} = \mathbb{Q}$, the same conclusion holds if Gp is not equal to p.*

Proof. We proceed by contraposition, assuming the negation of the common conclusion: for monic irreducible p, assume $M^i p \wedge M^j p \neq 1$ for some $i > j \geq 0$. Set $k = i - j \geq 1$. Lemma 3.1(c) implies that $M^k p$ and p are not coprime. Then p divides $M^k p$ and Lemma 3.2 implies that $G^k p = p$. This proves the result for general $\mathbb{K}$. For $\mathbb{K} = \mathbb{Q}$, a further consequence is that the map $\alpha \mapsto \alpha^{b^k}$ is a permutation of the roots of p in $\bar{\mathbb{Q}}$. Hence, all roots of p satisfy $\alpha^B = \alpha$ for some power $B = b^e$ of b, with $e > 0$. This means that p divides $x^B - x$. If $p = x$, $Gp = p$; otherwise, p is a cyclotomic polynomial Φ_a with $a \mid b^e - 1$, so $a \wedge b = 1$. Applying the formula in [11, Prop. 4 p. 14] yields $M\Phi_a = \prod_{b' \mid b} \Phi_{ab'}$, so that p divides Mp. Lemma 3.2 now implies $Gp = p$ again, completing the proof. □

Remark 3.5. Over a general subfield $\mathbb{K} \subset \mathbb{C}$, the cyclotomic polynomial Φ_a factors as $\Phi_a = \Psi_1 \cdots \Psi_s$ and G acts as a cyclic permutation of the Ψ_i. See also [11, Chap. 1] for a detailed description of the case $a \wedge b \neq 1$.

Lemma 3.4 states a result for polynomials p that are not part of a cycle of the map G. As a matter of fact, a related graph whose structure plays a crucial role in what follows is that of the map $\sqrt{G}$ that maps a monic irreducible p to the unique monic irreducible q such that Gp is some power of q: we call this map the *radical* of G, as it ignores the exponent generally introduced by G. An immediate degree argument shows that the cycles of G are exactly the cycles of $\sqrt{G}$, and consist of monic irreducible polynomials only.

To find a kind of generalization of Lemma 3.4 that applies to polynomials on cycles of $\sqrt{G}$, we can always reduce to its hypothesis $G^i p \neq p$ for nonzero i, by "stepping back one step" in the graph of $\sqrt{G}$, leaving the cycle.

Lemma 3.6. *Let $f \in \mathbb{K}[x]$ be a nonconstant polynomial with $f(0) \neq 0$. There exists a monic irreducible factor $q \in \mathbb{K}[x]$ of Mf such that $G^k q \neq q$ for all nonzero $k \in \mathbb{N}$.*

Proof. Choose a monic irreducible factor p of f and write $Mp = q_1 \cdots q_s$ for monic irreducible q_i. By contradiction, assume that for each i, there is some nonzero k_i for which $G^{k_i} q_i = q_i$. It follows that for $k = k_1 \cdots k_s$ and all i, $G^k q_i = q_i$. Lemma 3.1(a) implies $p^b = (Gq_1) \cdots (Gq_s)$, and because of Lemma 3.2, for all i, Gq_i is irreducible. Hence, there exist nonzero $e_i \in \mathbb{N}$ such that $Gq_i = p^{e_i}$, with $b = e_1 + \cdots + e_s$. Therefore, for each i, $q_i = G^{k-1} p^{e_i}$, so that, as q_i is irreducible, $e_i = 1$, and thus all q_i are equal to some same monic irreducible $\tilde{q}$. It follows that $Mp = \tilde{q}^b$. As p is irreducible, Lemma 3.3 applies to show that $Mp \wedge (Mp)' = 1$, which is impossible. The result follows by setting $q = q_i$ for a suitable i. □

Example 3.7. To suggest the graph structures induced by the Mahler and Gräffe operators, we depict on Figure 4 the graph of the radical $\sqrt{G}$. Applying M to some vertex p in the graph results in the product of all antecedents under the map. For example, $M(x - 2^6) = (x - 2)(x + 2)(x^2 - 2x + 4)(x^2 + 2x + 4)$, and $M\Phi_a = \Phi_a \Phi_{2a} \Phi_{3a} \Phi_{6a}$. In the second example, Φ_a appears to the right as a consequence of it being mapped to itself by G.

The depicted case, $b = 6$, is typical for $\mathbb{Q}[x]$. In particular, all cycles have length 1 as a consequence of the second part of Lemma 3.4.

3.3. **Denominator bounds: algorithm.** Armed with the previous lemmas, we can now prove the key result that leads to our main denominator bound. Still,

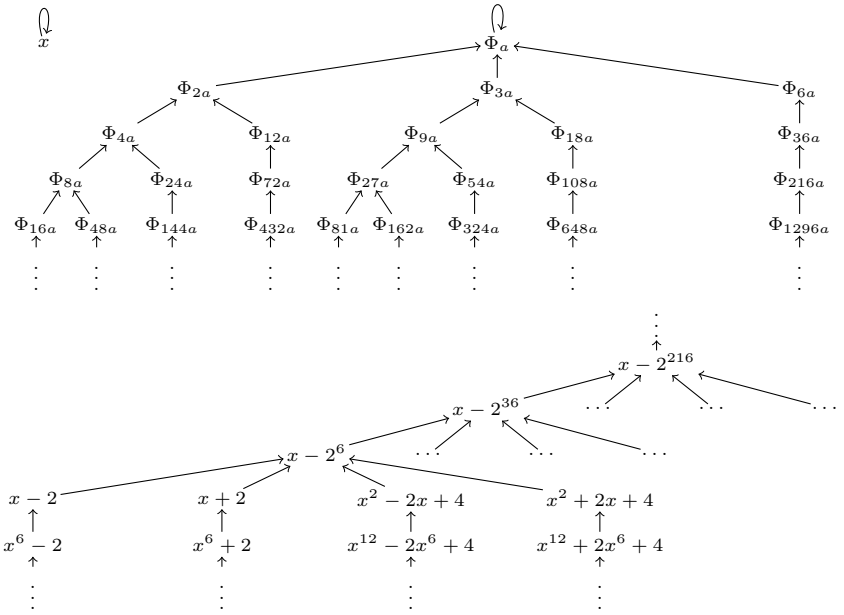

FIGURE 4. Graph of the radical $\sqrt{G}$ of the Gräffe operator for $b = 6$ in $\mathbb{Q}[x]$. Here, a is a positive integer, coprime to b. In general, the graph of $\sqrt{G}$ consists of a loop rooted at x (top left), bi-infinite trees (bottom), and cycles between cyclotomic polynomials with infinite trees rooted at them (top right).

to avoid repetitions in the proof of Proposition 3.10 below, we first state two intermediate lemmas.

The following lemma can be expressed more intuitively as follows: for any $\tilde{f}$ that is not on a cycle of $\sqrt{G}$, any g that appears on the tree rooted at $\tilde{f}$ of antecedents under $\sqrt{G}$ is also not on a cycle.

Lemma 3.8. *Let $\tilde{f} \in \mathbb{K}[x]$ be monic irreducible and satisfy $G^i\tilde{f} \neq \tilde{f}$ for all $i > 0$. Further, let $g \in \mathbb{K}[x]$ be monic irreducible and divide $M^j\tilde{f}$ for some $j \geq 0$. Then $G^i g \neq g$ for all $i > 0$.*

Proof. Suppose $G^i g = g$ for some $i \geq 1$. By Lemma 3.2, $G^j g$ is monic irreducible, and since $G^j g \mid G^j M^j \tilde{f} = \tilde{f}^{b^j}$, it must be $\tilde{f}$. Thus, $G^i\tilde{f} = G^{i+j}g = G^j g = \tilde{f}$, in contradiction with the definition of $\tilde{f}$. □

Lemma 3.9. *Let $s \geq r - 1$ and $m \geq 1$ be integers, and let $f \in \mathbb{K}[x]$ be monic irreducible, $q \in \mathbb{K}[x]$ be nonconstant, and $\ell \in \mathbb{K}[x]$ be nonzero, and such that $x \nmid q$, $M^s f^m \mid M^r q \mid \ell Tq$, and $M^{s-i} f \wedge q = 1$ whenever $0 \leq i < r$. Then $M^s f^m$ divides ℓ.*

Proof. Let $h^k \mid M^s f^m$ for a monic irreducible $h \in \mathbb{K}[x]$ and $k > 0$, so that $h^k \mid \ell Tq$. We prove by contradiction that h is coprime with Tq: suppose there exists some i satisfying $0 \leq i < r$ such that h divides $M^i q$. Then, $G^i h$ divides both $G^i M^i q$ and $G^i M^s f$, which, upon applying Lemma 3.1(a), are equal to powers of q and $M^{s-i} f$, respectively. This contradicts the coprimality of q and $M^{s-i} f$. We conclude that $h^k \mid \ell$, and the conclusion follows upon considering all $h^k \mid M^s f^m$. □

The following proposition will be used implicitly as a termination test in Algorithm 8: as long as there exists a nonpolynomial rational solution p/q, the nonconstant polynomial u proved to exist contains (potential) factors of q and can be used to change unknowns in a way that lessens the degree of ℓ_r. An interpretation of the structure of the proof is as follows:

- If some factor of q appears out of all cycles of $\sqrt{G}$, there exists such a factor u with no other factor of q in the tree rooted at u, and this u satisfies $M^r u \mid \ell$.
- Otherwise, each factor f of q is on a cycle and leads to some antecedent $\tilde{f}$ under $\sqrt{G}$ that is on no cycle, for which f divides $G\tilde{f}$. Considering all possible f and taking multiplicities into account, we construct a polynomial u such that $M^{r-1}u \mid \ell$ and $q \mid Gu$.

Proposition 3.10. *Let $\ell \in \mathbb{K}[x]$ be a nonzero polynomial and $q \in \mathbb{K}[x]$ be a nonconstant polynomial such that $x \nmid q$ and $M^r q \mid \ell\, Tq$. Then there exists a nonconstant $u \in \mathbb{K}[x]$ such that:*

- *either $M^r u \mid \ell$,*
- *or $M^{r-1}u \mid \ell$ and $q \mid Gu$.*

Proof. We consider two cases, the first one being when there exists a monic irreducible f dividing q such that $G^i f \neq f$ for all $i > 0$. In this case, we first prove that we can also assume without loss of generality that $M^j f \wedge q = 1$ for all $j > 0$. Assume the contrary: that the gcd is nontrivial for at least one $j > 0$. By Lemma 3.4, the $M^j f$ for $j \in \mathbb{N}$ are pairwise coprime, and since q has finitely many factors, $M^j f \wedge q \neq 1$ for at most finitely many j. Set j to the maximal possible value and g to a monic irreducible factor of $M^j f \wedge q$. Lemma 3.8 applied to g and $\tilde{f} = f$ implies that $G^i g \neq g$ for all $i > 0$, and g can replace f with the added property on the $M^j g$. At this point, Lemma 3.9 applies with $s = r$ and $m = 1$, proving that $M^r f$ divides ℓ. The proposition is proved in this case by choosing $u = f$.

In the second case, let $q = c\prod_k f_k^{m_k}$ be the irreducible factorization of q, for a nonzero constant c and two-by-two distinct monic irreducible f_k, and with, for each k, some $i_k > 0$ satisfying $G^{i_k} f_k = f_k$. Fix any k. Lemma 3.6 provides a monic irreducible factor $\tilde{f}_k \in \mathbb{K}[x]$ of Mf_k such that $G^i \tilde{f}_k \neq \tilde{f}_k$ for all $i > 0$. If $M^i \tilde{f}_k \wedge q$ was nontrivial for some $i \in \mathbb{N}$, this gcd would contain some monic irreducible factor g, necessarily equal to some $f_{k'}$, and Lemma 3.8 would contradict the existence of $i_{k'}$. So the polynomials $M^j \tilde{f}_k$ are coprime with q for all $j \in \mathbb{N}$. Upon setting $s = r - 1$, $m = m_k$, and $g = \tilde{f}_k$, $M^s g^m = M^{r-1}\tilde{f}_k^{m_k} \mid M^r f_k^{m_k} \mid M^r q$, and $M^{s-i} g = M^{r-1-i}\tilde{f}_k$ is coprime with q for all i satisfying $0 \leq i < r$, so that Lemma 3.9 proves that $M^{r-1}\tilde{f}_k^{m_k} = M^s g^m$ divides ℓ. Additionally, $Gg = G\tilde{f}_k \mid GMf_k = f_k^b$, so that Gg is a power of f_k, hence $f_k \mid Gg = G\tilde{f}_k$, and next $f_k^{m_k} \mid G\tilde{f}_k^{m_k}$. Gathering the results over all k, the $\tilde{f}_k$ are pairwise coprime because the f_k are; it follows that all $M^{r-1}\tilde{f}_k^{m_k}$ divide ℓ and are pairwise coprime, so that, finally, the product $u = \prod_k \tilde{f}_k^{m_k}$ satisfies $M^{r-1}u \mid \ell$ and $q \mid Gu$. □

Remark 3.11. In the first case of the proof, which builds u satisfying $M^r u \mid \ell$, it is of interest to compare the construction with that in the case of usual recurrences [2]. The obtained u is extremal, in the sense that no other factor of q can be found in the tree rooted at it, that is to say by iterating $\sqrt{G}$ backward from it; this is used to compute u from the leading coefficient ℓ of the Mahler operator. In the case of usual recurrences, the shift operator S (with respect to the variable n)

Input: A linear Mahler equation of the form (EQN).
Output: A polynomial $q^\star \in \mathbb{K}[x]$.

(1) Set $\ell := \ell_r$, then repeat for $k = 1, 2, \ldots$:
  (a) write $\ell = \sum_{i=0}^{b^r-1} x^i M^r f_i$ with $f_i \in \mathbb{K}[x]$;
  (b) set $u_k := \bigwedge_{i=0}^{b^r-1} f_i$;
  (c) set $\ell := (\ell / M^r u_k) \bigvee_{i=0}^{r-1} M^i u_k$
  until $\deg u_k = 0$, at which point set $t = k - 1$.
(2) Set $\tilde{u} := \bigwedge_{i=0}^{b^{r-1}-1} f_i$ where $\ell = \sum_{i=0}^{b^{r-1}-1} x^i M^{r-1} f_i$.
(3) Return $u_1 \cdots u_t \, (G\tilde{u})$.

ALGORITHM 8. Obtain a denominator bound from ℓ_r.

and its inverse S^{-1} play roles similar to M and $\sqrt{G}$, respectively. In Abramov's algorithm for denominator bounds, poles are searched for by considering poles that are extremal in a class $\alpha + \mathbb{Z}$: in particular, a pole $\beta \in \alpha + \mathbb{Z}$ with minimal real part corresponds to a monic irreducible factor $u = n - \beta$ such that $S^r u$ divides the leading coefficient ℓ of the recurrence operator.

Corollary 3.12. *When $d < b^{r-1}$, Eq. (EQN) has no nonconstant rational solution.*

Proof. With the notation above, Lemma 2.2 implies $\bar{v} = 0$. If a nonconstant q could satisfy Eq. (3.2), Proposition 3.10 would apply, inducing the contradiction $b^{r-1} \leq \deg \ell_r \leq d$. So q is constant, and Lemma 2.5 applies and proves p is constant. □

Proposition 3.10 forms the basis of Algorithm 8, which repeatedly searches for factors of the form $M^r u$ to "be removed" from ℓ_r (while "adding back" other factors of strictly smaller degree) and accumulates the corresponding u into the denominator bound. The update of ℓ at step 1c of each loop iteration can be viewed as a change of unknown functions of the form $y = \tilde{y}/u_k$ in (EQN). The search for factors of the form $M^r u$, respectively $M^{r-1}\tilde{u}$, uses the following property (for radix b^r, resp. b^{r-1}).

Lemma 3.13. *Let $f_0, \ldots, f_{b-1}, u \in \mathbb{K}[x]$. The polynomial $\ell = Mf_0 + x\,Mf_1 + \cdots + x^{b-1}\,Mf_{b-1}$ is divisible by Mu if and only if $f_0, \ldots, f_{b-1}$ are all divisible by u.*

Proof. The "if" part is clear. Conversely, fix $i < b$, and assume that $Mu \mid \ell$. Let ω be a primitive bth root of unity. Then, $Mu = (Mu)(\omega^j x) \mid \ell(\omega^j x)$ for all j, hence Mu divides

$$\sum_{j=0}^{b-1} \omega^{-ij} \ell(\omega^j x) = b\, x^i Mf_i.$$

As $Mu \in \mathbb{K}[x^b]$ and $i < b$, this implies $Mu \mid Mf_i$, and $u \mid f_i$ by Lemma 3.1(c). □

Example 3.14. In this example, we let $b = 3$ and use Algorithm 8 to analyze the potential poles in rational-function solutions of an operator

$$L = \big(p_1(x) \cdots p_6(x)\big)\, M^2 + \cdots,$$

where the p_i are polynomials to be found in Figure 5 and the coefficients of M^1 and M^0 will be disclosed below. In the figure and this example, polynomials of

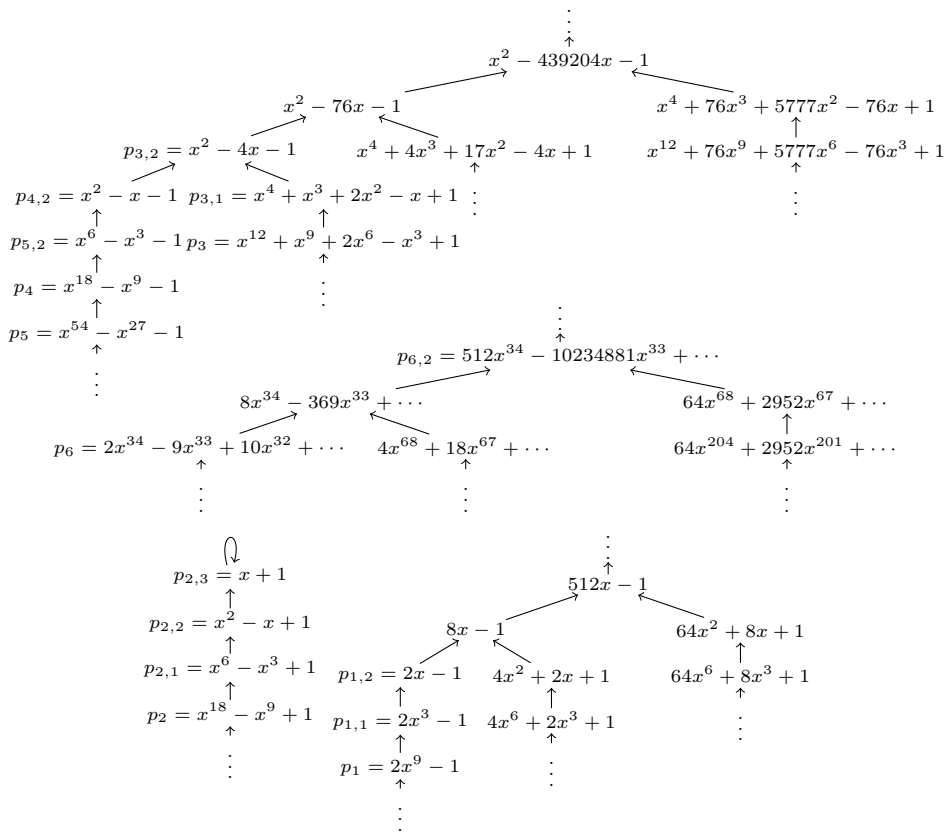

FIGURE 5. Portion of the graph of the radical $\sqrt{G}$ of the Gräffe operator used for the resolution in Example 3.14.

large size are truncated to their first few monomials, and in most cases, we write them in factored form, although polynomials are manipulated in expanded form in the actual algorithm.

Following Algorithm 8, we set $\ell = p_1 \cdots p_6$. Step 1 is motivated by the first case in Proposition 3.10: it strives to solve (3.2) by finding a factor u of q such that $M^2 u \mid \ell$. For each i, the only monic irreducible candidate factor of u that can "cover" p_i upon application of M^2 is the polynomial $p_{i,2}$ in the figure. However, $M^2 p_{i,2}$ consists of *all* factors on the level of p_i with same ancestor $p_{i,2}$. So, for example, $M_2 p_{1,2} = p_1$ and $p_{1,2}$ can be part of u, whereas $M_2 p_{6,2}$ is a strict multiple of p_6 so that $p_{6,2}$ cannot be made part of u. As a matter of fact, for $k = 1$ in the loop, the algorithm finds $u_1 = p_{1,2} p_{2,2} p_{4,2} p_{5,2}$ at step 1b, after rewriting ℓ in the form

$$\ell = -M^2\big((2x-1)(x^2-x+1)(x^2-x-1)(x^6-x^3-1)(9x^5-133x^4+\cdots)\big)+\cdots+ x^8 M^2\big(2(2x-1)(x^2-x+1)(x^2-x-1)(x^6-x^3-1)(5x^4-74x^3+\cdots)\big)$$

at step 1a. Step 1c resets ℓ to a polynomial that factors into

$$p_{1,1}\, p_{1,2}\, p_{2,1}\, p_{2,2}\, p_3\, p_4\, p_{5,2}\, p_{4,2}\, p_6.$$

Following the same approach for $k = 2$, a new phenomenon occurs because of the loops in the graph: the candidate factor $p_{2,3}$ that would "cover" $p_{2,1}$ appears in its own tree on the same level as $p_{2,1}$, and thus has to be rejected. It follows that the algorithm finds $u_2 = p_{3,2}p_{4,2}$ at step 1b, after rewriting ℓ in the form

$$\ell = -M^2\big((x^2-4x-1)(x^2-x-1)(248x^5-5615x^4+\cdots)\big)+\cdots+ \\ x^8M^2\big((x^2-4x-1)(x^2-x-1)(532x^4-6211x^3+\cdots)\big)$$

at step 1a. Step 1c resets ℓ to a polynomial that factors into

$$p_{1,1}\,p_{1,2}\,p_{2,1}\,p_{2,2}\,p_{3,1}\,p_{5,2}\,p_{4,2}\,p_{3,2}\,p_6.$$

Following the same approach for $k = 3$ leads to $u_3 = 1$: no further factor u of q exists and helps solving Eq. (3.2) by ensuring $M^2u \mid \ell$.

This leads to step 2, which is motivated by the second case in Proposition 3.10: Eq. (3.2) now implies $M^2q \mid q \wedge Mq$, which is solved by finding $\tilde{u}$ such that $M\tilde{u} \mid \ell$. A difference to step 1 is that at step 2, candidates are looked for just $2-1=1$ level above the factors to be "covered". A similar calculation as previously explains that the algorithm finds $\tilde{u} = p_{1,2}p_{2,2}p_{3,2}p_{4,2}$, after rewriting ℓ in the form

$$\ell = M^2\big((2x-1)(x^2-x+1)(x^2-4x-1)(x^2-x-1)(181x^{13}-1198x^{12}+\cdots)\big) \\ -xM^2\big((2x-1)(x^2-x+1)(x^2-4x-1)(x^2-x-1)(44x^{13}-623x^{12}+\cdots)\big) \\ +x^2M^2\big((2x-1)(x^2-x+1)(x^2-4x-1)(x^2-x-1)(4x^{13}-382x^{12}+\cdots)\big).$$

From these factors, only $p_{2,2}$ is cyclotomic. But as the algorithm does not factor polynomials, the other factors cannot be discarded.

At step 3, the algorithm returns the bound

$$q^\star = u_1u_2G\tilde{u} = {p_{1,2}}^{1+1}{p_{2,2}}^2{p_{3,2}}^{1+1}{p_{4,2}}^{2+1}p_{5,2},$$

where the "+1" indicate factors that could have been saved if a cyclotomic test had been available. The operator L was indeed constructed so as to admit the two explicit rational solutions

$$\frac{2x}{(2x-1)(x^2-x-1)} \quad \text{and} \quad \frac{x-3}{(x^2-x+1)(x^2-4x-1)(x^6-x^3-1)},$$

whose denominators are effectively "covered" by q^*.

We remark that, during the steps of the algorithm, the degree of ℓ has dropped from its initial value 145 down to 84, then to 62.

Example 3.15. Let $b = 3$ and let us consider the Mahler equation

$$L = (2x^4-x^3-x+3)(2x^9-1)(x^{18}-x^9-1)\,M^2 \\ -(x^2+1)(2x^3-1)(x^4+1)(x^6-x^3-1)(2x^{10}-x^9-x+3)\,M \\ +x^2(2x-1)(x^2+x+1)(x^2-x+1)(x^2-x-1)(2x^{12}-x^9-x^3+3).$$

Following Algorithm 8, we expand $(2x^4-x^3-x+3)(2x^9-1)(x^{18}-x^9-1)$ to get ℓ, which step 1a rewrites

$$\ell = M^2(6x^3-9x^2-3x+3)+xM^2(-2x^3+3x^2+x-1)+ \\ x^3M^2(-2x^3+3x^2+x-1)+x^4M^2(4x^3-6x^2-2x+2).$$

(That is, $f_2 = f_5 = f_6 = f_7 = f_8 = 0$.) We get $u_1 = 2x^3-3x^2-x+1$, which factors into $(2x-1)(x^2-x-1)$. Step 1c resets ℓ to a polynomial that factors into

$(2x-1)(x^2-x-1)(2x^3-1)(2x^4-x^3-x+3)(x^6-x^3-1)$. Expanding ℓ as in step 1a, we now find

$$\begin{aligned}\ell = M^2(3-10x) + xM^2(-4-15x) + x^2M^2(-8-19x) + \\ x^3M^2(5+40x) + x^4M^2(5-10x) + x^5M^2(2x+9) + \\ x^6M^2(-25-16x) + x^7M^2(15+8x) + x^8M^2(23),\end{aligned}$$

so that $u_2 = 1$. We pass to step 2, which expands ℓ in the form

$$\begin{aligned}\ell = M(-16x^5+40x^4-10x^3-25x^2+5x+3) + \\ xM(8x^5-10x^4-15x^3+15x^2+5x-4) + \\ x^2M(2x^4-19x^3+23x^2+9x-8),\end{aligned}$$

and $\tilde{u} = (2x-1)(x^2-x-1)$. So, $q^\star = u_1\, G\tilde{u} = (2x-1)(x^2-x-1)(8x-1)(x^2-4x-1)$. This means that if $y = p/(x^{\bar{v}}q)$ is solution of $Ly = 0$, where $\bar{v} \geq 0$ and $p, q \in \mathbb{K}[x]$ satisfy $x \wedge q = p \wedge q = p \wedge x^{\bar{v}} = 1$, then q divides $q^\star$. Using the results of §2.2, we find that 0 could not be a pole of a solution in $\mathbb{K}(x)$ and therefore $\bar{v} = 0$. Consequently, $q^\star$ is a denominator bound.

Proposition 3.16. *Algorithm 8 runs in* $\mathrm{O}((\deg \ell_r)\ \mathrm{M}(d)\log d)$ *ops if* $b = 2$, *resp. in* $\mathrm{O}(b^{-r}\,(\deg \ell_r)\ \mathrm{M}(d)\log d)$ *ops if* $b \geq 3$, *and computes a polynomial* $q^\star$ *of degree at most* $\deg \ell_r$ *if* $b = 2$, *resp. at most* $(\deg \ell_r)/b^{r-1}$ *if* $b \geq 3$, *such that any rational function solution* y *of* (EQN) *can be written in the form* $y = p/(x^{\bar{v}}q^\star)$ *for some* $p \in \mathbb{K}[x]$ *and* $\bar{v} \in \mathbb{N}$.

Proof. For each $k \geq 1$ reached by the loop 1, let $\tilde{\ell}_k$ denote the value of ℓ considered at step 1a, so that the value assigned at step 1c is $\tilde{\ell}_{k+1}$. (In particular, $\tilde{\ell}_1 = \ell_r$.)

First, observe that, after step 1b in each loop iteration, u_k is by Lemma 3.13 a polynomial of maximal degree such that $M^r u_k \mid \tilde{\ell}_k$. In particular, the next value, $\tilde{\ell}_{k+1}$, computed at step 1c, is a polynomial. Set $\rho = b^r - \frac{b^r-1}{b-1}$, which is at least 1. Step 1c decreases the degree of ℓ by

$$\deg \tilde{\ell}_k - \deg \tilde{\ell}_{k+1} \geq \deg M^r u_k - \deg Tu_k \geq \rho \deg u_k \geq \rho.$$

In particular, the loop terminates after at most $\rho^{-1}(1 + \deg \ell_r)$ iterations, and therefore the whole algorithm terminates as well. Second, after step 2, $\tilde{u}$ is similarly a polynomial of maximal degree such that $M^{r-1}\tilde{u} \mid \tilde{\ell}_{t+1}$. Therefore, $b^{r-1}\deg \tilde{u}$ is bounded above by the degree of $\tilde{\ell}_{t+1}$, so that

$$\left(\sum_{k=1}^{t} \rho \deg u_k\right) + b^{r-1}\deg \tilde{u} \leq \left(\sum_{k=1}^{t} \deg \tilde{\ell}_k - \deg \tilde{\ell}_{k+1}\right) + \deg \tilde{\ell}_{t+1} \leq \deg \ell_r,$$

where t denotes, as in Algorithm 8, the last value of k for which $\deg u_k > 0$. The output from the algorithm is $q^\star = u_1 \cdots u_t\,(G\tilde{u})$. If $b = 2$, then $\rho = 1$ and $\deg q^\star = \left(\sum_k \deg u_k\right) + \deg \tilde{u}$ is bounded by $\deg \ell_r$; if $b \geq 3$, then

$$\rho = b^{r-1}\left(b - 2 + \frac{b-2}{b-1}\right) + \frac{1}{b-1} \geq b^{r-1}$$

and $\deg q^\star$ is bounded by $b^{-(r-1)}\deg \ell_r$.

Assume that $p/(x^{\bar{v}}q)$ is a solution written in lowest terms. Set $\tilde{q}_0 = q$ and, for k between 1 and t, define the polynomials $\tilde{q}_k = \tilde{q}_{k-1}/(u_k \wedge \tilde{q}_{k-1})$. Let us prove by an induction on k that, for $1 \leq k \leq t+1$: *(i)* $x \nmid \tilde{q}_{k-1}$; *(ii)* $M^r\tilde{q}_{k-1} \mid \tilde{\ell}_k\, T\tilde{q}_{k-1}$;

and *(iii)* $q \mid u_1 \cdots u_{k-1}\tilde{q}_{k-1}$. Initially when $k = 1$, we have $\tilde{q}_0 = q$ and $\tilde{\ell}_1 = \ell_r$, so the three properties hold by our assumption on a solution and Equation (3.2). Assume now that $x \nmid \tilde{q}_{k-1}$, $M^r\tilde{q}_{k-1} \mid \tilde{\ell}_k\, T\tilde{q}_{k-1}$ and $q \mid u_1 \cdots u_{k-1}\tilde{q}_{k-1}$. It follows from $\tilde{q}_{k-1} = (u_k \wedge \tilde{q}_{k-1})\,\tilde{q}_k \mid u_k\tilde{q}_k$ that $x \nmid \tilde{q}_k$ and $T\tilde{q}_{k-1} \mid (Tu_k)\,(T\tilde{q}_k)$. Furthermore,

$$(M^r(u_k \wedge \tilde{q}_{k-1}))\,(M^r\tilde{q}_k) = M^r\tilde{q}_{k-1} \mid \tilde{\ell}_k\, T\tilde{q}_{k-1} \mid \tilde{\ell}_k\,(Tu_k)\,(T\tilde{q}_k). \tag{3.3}$$

Write $M^r u_k = a_k\, M^r(\tilde{q}_{k-1} \wedge u_k)$ and $\tilde{\ell}_k = b_k\, M^r u_k$, for suitable polynomials a_k and b_k. Upon division by $M^r(u_k \wedge \tilde{q}_{k-1})$, Equation (3.3) becomes

$$M^r\tilde{q}_k \mid a_k b_k\,(Tu_k)\,(T\tilde{q}_k). \tag{3.4}$$

By construction, a_k and $M^r\tilde{q}_k$ are coprime, as they are the cofactors of $M^r(u_k \wedge \tilde{q}_{k-1})$ in, respectively, $M^r u_k$ and $M^r\tilde{q}_{k-1}$, so Equation (3.4) finally becomes

$$M^r\tilde{q}_k \mid \frac{\tilde{\ell}_k}{M^r u_k}\,(Tu_k)\,(T\tilde{q}_k) = \tilde{\ell}_{k+1}\,T\tilde{q}_k.$$

By the divisibility assumption on q and the definition of $\tilde{q}_k$,

$$q \mid u_1 \cdots u_{k-1}\tilde{q}_{k-1} = u_1 \cdots u_{k-1}\,(u_k \wedge \tilde{q}_{k-1})\,\tilde{q}_k \mid u_1 \cdots u_k\tilde{q}_k,$$

completing the proof by induction.

The loop terminates when ℓ no longer has any nonconstant factor of the form $M^r u$, with $\ell = \tilde{\ell}_{t+1}$. At this point, $M^r\tilde{q}_t \mid \tilde{\ell}_{t+1}\,T\tilde{q}_t$ and $q \mid u_1 \cdots u_t\tilde{q}_t$. If $\tilde{q}_t$ is constant, then $q \mid u_1 \cdots u_t \mid q^\star$. On the other hand, if $\tilde{q}_t$ is not constant, Proposition 3.10 applies, as $x \nmid \tilde{q}_t$, which implies that $\tilde{\ell}_{t+1}$ admits a factor of the form $M^{r-1}u$ such that $\tilde{q}_t \mid Gu$. By Lemma 3.13, step 2 computes a polynomial $\tilde{u}$ such that $M^{r-1}u \mid M^{r-1}\tilde{u}$. It follows by Lemma 3.1(c) that $u \mid \tilde{u}$, next that $\tilde{q}_t \mid G\tilde{u}$, so that q divides $q^\star$, again.

Let us turn to the complexity analysis. Applying M to a polynomial requires no arithmetic operation. Each execution of step 1b amounts to $b^r - 1$ gcds of polynomials of degree less than or equal to d/b^r, for a total cost of $\mathrm{O}(\mathrm{M}(d)\log d)$ ops. The same argument applies to step 2. Similarly, the chain of lcms at step 1c requires

$$\mathrm{O}\left(\sum_{i=0}^{r-1} \mathrm{M}(b^i \deg u_k)\log(b^i \deg u_k)\right) = \mathrm{O}(\mathrm{M}(d)\log d) \text{ ops},$$

as $(\sum_{i=0}^{r-1} b^i)\deg u_k = \mathrm{O}(d)$. Since there are at most $\rho^{-1}(1 + \deg \ell_r)$ iterations of steps 1b and 1c, the cost of step 1 is $\mathrm{O}(\rho^{-1}\,(\deg \ell_r)\,\mathrm{M}(d)\log d)$. If $b = 2$, then $\rho = 1$ and the cost of step 1 is $\mathrm{O}((\deg \ell_r)\,\mathrm{M}(d)\log d)$. If $b \geq 3$, then $\rho \geq b^{r-1}$ and the cost is $\mathrm{O}(b^{-r}\,(\deg \ell_r)\,\mathrm{M}(d)\log d)$.

The computation of $G\tilde{u}$ from $\tilde{u}$ at step 3 can be performed in $\mathrm{O}(\mathrm{M}(bd))$ ops [5, 13] and the final product can be computed in $\mathrm{O}(\mathrm{M}(d)\log d)$ ops using a product tree. □

Proposition 3.16 implicitly provides a bound on $\deg q$ that essentially (when $\bar{v} = 0$ and $\tilde{u} = 1$, exactly) matches that of Bell and Coons [4, Proposition 2]. However, a tighter bound holds, especially for $b = 2$.

Proposition 3.17. *With the notation above, q has degree at most $3\deg \ell_r/b^r$.*

Proof. Let $g = M^r q \wedge Tq$. On the one hand, (3.2) implies $M^r q \mid \ell_r g$, so that $b^r \deg q \leq \deg \ell_r + \deg g$. On the other hand, Mg divides $h = M^r q \vee Tq$ by definition of T, hence $g\,Mg$ divides $gh = (M^r q)\,(Tq)$, whence

$$(b+1)\deg g \leq \frac{b^{r+1} - 1}{b - 1}\deg q.$$

Comparing the two inequalities leads to

$$\deg q \le \frac{(b^2-1)\deg \ell_r}{b^{r+2}-b^{r+1}-b^r+1} \le \frac{(b^2-1)\deg \ell_r}{b^r(b^2-b-1)} \le \frac{3\deg \ell_r}{b^r}$$

since $(b^2-1)/(b^2-b-1) \le 3$ for $b \ge 2$. □

Remark 3.18. The previous discussion to find $q^\star$ is entirely based on (3.1) in the case $j = r$ and on expressing the solution y with a minimal denominator $x^{\bar v}q$. Noting that (3.1) actually holds also for $j \ne r$ and even if $p \wedge q \ne 1$, we may apply it with $0 \le j \le r-1$ to a potential solution written in the form $p/(x^{\bar v}q^\star)$ to get additional constraints involving $\ell_0, \dots, \ell_{r-1}$ that can be used to remove some factors from $q^\star$.

3.4. **An alternative bound.** We now describe an alternative method for computing denominator bounds. While it yields coarser bounds, our estimate for its computational cost is better, so that it may be a superior choice in some cases. The results of this subsection are not used in the sequel.

Proposition 3.19. *If $x^{\bar v}q \in \mathbb{K}[x]$ is the denominator of a rational solution of* (EQN) *written in lowest terms, then it holds that*

$$q \mid (G^r\ell_r)\,(G^{r+1}\ell_r)\cdots(G^{r+K}\ell_r), \qquad K = \lfloor \log_b(3\deg \ell_r)\rfloor - r.$$

Proof. Suppose f is monic irreducible and m is positive such that $f^m \mid q$, and consider the condition

$$M^{r+j}f \mid \bigvee_{i=0}^{r} M^i q. \tag{3.5}$$

Clearly, (3.5) is satisfied for $j = 0$, while it requires

$$b^{r+j}\deg f \le \frac{b^{r+1}-1}{b-1}\deg q,$$

which in turn implies $j \le \log_b \deg q$. Plugging in the bound from Proposition 3.17, we obtain $j \le \log_b(3\deg \ell_r) - r$.

Choose j maximal such that (3.5) holds. Then $M^{r+j}f$ cannot divide Tq, and by Lemma 3.3, $M^{r+j}f$ is squarefree. Let h be a monic irreducible factor of $M^{r+j}f$ not dividing Tq. In the rest of the proof, we write $\operatorname{sqrfree} p$ for the squarefree part of any polynomial p. For all $k \ge 0$, set $h_k = \operatorname{sqrfree}(G^k h)$, and denote by m_k the multiplicity of h_k as a factor of Tq. Thus m_0 is zero by definition of h. Continuing with $k \ge 0$, Lemma 3.1(b) implies $G^k h \mid MG^{k+1}h$, so that $h_k \mid \operatorname{sqrfree}(MG^{k+1}h) \mid M\operatorname{sqrfree}(G^{k+1}h) = Mh_{k+1}$. As $h_k^{m_k} \mid Tq$, we deduce that $h_k^{m_{k+1}} \mid Mh_{k+1}^{m_{k+1}} \mid MTq \mid Tq \wedge M^r q$, then, by using (3.2), $h_k^{m_{k+1}} \mid \ell_r Tq$. The definition of m_k then yields $h_k^{\delta_k} \mid \ell_r$ for $\delta_k = \max(m_{k+1} - m_k, 0)$.

Now, restrict k to the interval $j < k \le r + j$. Then, by Lemma 3.1(b),

$$h_k \mid G^k h \mid G^k M^{r+j} f = (M^{r+j-k}f)^{b^k}, \tag{3.6}$$

and as h_k is squarefree, h_k divides $M^{r+j-k}f$. Since $f^m \mid q$ and $0 \le r+j-k < r$, h_k^m divides Tq, implying $m_k \ge m$.

By Lemma 3.1(b) and Equation (3.6), $G^{r+j-k}h_k$ is $f^{b^{r+j}}$, so that f divides the former. Then,

$$f^{\delta_k} \mid G^{r+j-k}h_k^{\delta_k} \mid G^{r+j-k}\ell_r.$$

Input: A linear Mahler equation of the form (EQN).
Output: A basis of its space of rational function solutions.

(1) Set $\delta = \max \deg \ell_k$.
(2) If $\delta < b^{r-1}$: return $\{1\}$ if $L(1) = 0$, and $\emptyset$ otherwise.
(3) Compute $q^\star$ using Algorithm 8. Set $\bar{v} = \lfloor \delta/(b^r - b^{r-1}) \rfloor$.
(4) For $0 \le k \le r$, set $e_k = \lfloor b\delta/(b-1) \rfloor - b^k \bar{v}$ and
$$\tilde{\ell}_k = x^{e_k} \ell_k \prod_{0 \le i \le r,\ i \ne k} M^i q^\star.$$
Set $\tilde{L} = \tilde{\ell}_r M^r + \cdots + \tilde{\ell}_0$.
(5) Call Algorithm 5 on the equation $\tilde{L}p = 0$, with $w = \deg q^\star + 2\bar{v} + 1$, to compute a basis $(p_1, \dots, p_\sigma)$ of its polynomial solutions of degree less than w.
(6) Return $(p_k/(x^{\bar{v}} q^\star))_{1 \le k \le \sigma}$.

Algorithm 9. Rational solutions

Forming the product of these bounds for k ranging from 0 to j, we get $f^m \mid \prod_{k=0}^{j} G^k \ell_r$, as $m \le m_{j+1}$ and $m_0 = 0$. The result follows by considering all possible (f, m) such that $f^m \mid q$. □

Proposition 3.20. *One can compute a polynomial $q^* \in \mathbb{K}[x]$ of degree at most $d(\log_b d - r + 2)$ and such that $q \mid q^*$ in $\mathrm{O}(\mathrm{M}(d \log d) \log d)$ ops.*

Proof. If $\deg \ell_r < b^{r-1}$, return 1. This is a valid bound by Corollary 3.12. Otherwise, return the bound from Proposition 3.19. As with the previous bound, the $G^k \ell_r$ up to $k = r + K = \mathrm{O}(\log d)$ can be computed for a total of $\mathrm{O}(\mathrm{M}(bd) \log d)$ ops [5, 13]. The product then takes $\mathrm{O}(\mathrm{M}(d \log d) \log d)$ ops. □

3.5. **Computing numerators.** In order to obtain a basis of rational solutions y of (EQN), it suffices to obtain a bound $x^{\bar{v}} q^\star$ on denominators as in §3.3, to construct an auxiliary equation corresponding to the change of unknown functions $y = \tilde{y}/(x^{\bar{v}} q^\star)$, and to search for its polynomial solutions $\tilde{y}$. We first note the following consequence of Lemma 2.5, already proved by Bell and Coons [4, Prop. 2].

Proposition 3.21. *If $p, q \in \mathbb{K}[x]$, not necessarily coprime, satisfy $L(p/q) = 0$, then $\deg p$ is at most $\deg q + \lfloor d/(b^r - b^{r-1}) \rfloor$.*

The procedure to obtain rational solutions is summarized in Algorithm 9.

Proposition 3.22. *Algorithm 9 computes a basis of rational solutions of its input equation. Assuming $d \ge b^{r-1}$, it runs in $\tilde{\mathrm{O}}(d\,\mathrm{M}(d) + 2^r d^2 + \mathrm{M}(2^r d))$ ops when $b = 2$ and $\tilde{\mathrm{O}}(b^{-r} d\,\mathrm{M}(d))$ ops when $b \ge 3$. Assuming further $\mathrm{M}(n) = \tilde{\mathrm{O}}(n)$, it runs in $\tilde{\mathrm{O}}(2^r d^2) = \tilde{\mathrm{O}}(d^3)$ ops when $b = 2$ and in $\tilde{\mathrm{O}}(b^{-r} d^2)$ ops when $b \ge 3$.*

Proof. Define δ as in step 1, so that $\delta \le d$. If $\delta < b^{r-1}$, the algorithm will stop after step 2. In this case, Corollary 3.12 states that there are no nonconstant rational solution. Therefore, the vector space of rational solutions is $\mathbb{K}$ when $L(1) = 0$ and $\{0\}$ otherwise.

Otherwise, the algorithm continues with $d \geq b^{r-1}$. Assume that $y \in \mathbb{K}(x)$ is a rational solution of $Ly = 0$, and let $p = x^{\bar{v}} q^\star y$ for $q^\star$ and $\bar{v}$ computed as in step 3. By Proposition 3.16 combined with Lemma 2.2, p is a polynomial. By Proposition 3.21 combined with Lemma 2.5, it has degree at most $\deg(x^{\bar{v}} q^\star) + \bar{v} = \deg q^\star + 2\bar{v}$. Plugging $y = p/(x^{\bar{v}} q^\star)$ into $Ly = 0$ and multiplying the resulting equation by the polynomial $x^{\lfloor b\delta/(b-1) \rfloor} \prod_{i=0}^{r} M^i q^\star$, we see that p satisfies $\tilde{L}p = 0$, where $\tilde{L}$ is defined as in step 4. As $b^k \bar{v} \leq b\delta/(b-1)$ for $k \leq r$, the e_k are nonnegative and the $\tilde{\ell}_k$ are polynomials. Thus Algorithm 5 applies and, by Proposition 2.14, p belongs to the span of the p_k computed at step 5 of Algorithm 9. Conversely, for all k, the fraction $p_k/(x^{\bar{v}} p^\star)$ is a solution of $Ly = 0$.

After step 2, we have $b^r = \mathrm{O}(d)$, that is, $r = \tilde{\mathrm{O}}(1)$. By Proposition 3.16, the cost of step 3 is $\tilde{\mathrm{O}}(d\,\mathrm{M}(d))$ ops when $b = 2$ and $\tilde{\mathrm{O}}(b^{-r} d\,\mathrm{M}(d))$ ops when $b \geq 3$. Define

$$\tilde{d} = \frac{2b-1}{b-1} d + \frac{b^{r+1}-1}{b-1} \deg q^\star = \begin{cases} \mathrm{O}(2^r d), & b = 2, \\ \mathrm{O}(d), & b \geq 3, \end{cases} \tag{3.7}$$

where the asymptotic bounds follow from Proposition 3.16. Each polynomial $\tilde{\ell}_k$ defined at step 4 then satisfies

$$\deg \tilde{\ell}_k \leq e_k + \delta + \frac{b^{r+1}-1}{b-1} \deg q^\star \leq \tilde{d}$$

and is the product of $r+1$ polynomials, so their computation takes $\mathrm{O}(r\,\mathrm{M}(\tilde{d})) = \tilde{\mathrm{O}}(\mathrm{M}(\tilde{d}))$ ops. Observe as well that $1 \leq w = \mathrm{O}(\tilde{d}/b^r)$. According to Proposition 2.14, step 5 thus requires $\tilde{\mathrm{O}}(b^{-r}\tilde{d}^2 + \mathrm{M}(\tilde{d}))$ ops, which dominates the cost of step 4. Taking the bounds (3.7) into account, we get that step 5 is dominated by step 3 when $b \geq 3$, so that the total cost is $\tilde{\mathrm{O}}(d\,\mathrm{M}(d) + 2^r d^2 + \mathrm{M}(2^r d))$ ops when $b = 2$ and $\tilde{\mathrm{O}}(b^{-r} d\,\mathrm{M}(d))$ ops when $b \geq 3$. With fast multiplication, $\mathrm{M}(n) = \tilde{\mathrm{O}}(n)$, this simplifies to the announced complexity estimates. □

Example 3.23. We continue Example 3.15. We have seen that the denominator bound is $q^\star = (2x-1)(x^2-x-1)(8x-1)(x^2-4x-1)$. We set $\tilde{y} = q^\star y$, so that $Ly = 0$ if and only if $\tilde{L}\tilde{y} = 0$, where $\tilde{L} = \tilde{\ell}_2 M^2 + \tilde{\ell}_1 M^1 + \tilde{\ell}_0$ for

$$\begin{aligned}
\tilde{\ell}_2 &= (2x-1)(8x-1)(x^2-x-1)(x^2-4x-1) \times \\
&\qquad (4x^2+2x+1)(2x^4-x^3-x+3)(x^4+x^3+2x^2-x+1), \\
\tilde{\ell}_1 &= -(8x-1)(x^2+1)(x^2-4x-1)(2x^3-1)(x^4+1) \times \\
&\qquad (x^6-x^3-1)(4x^6+2x^3+1)(2x^{10}-x^9-x+3)(x^{12}+x^9+2x^6-x^3+1), \\
\tilde{\ell}_0 &= x^2(2x-1)(x^2+x+1)(x^2-x+1)(x^2-x-1) \times \\
&\qquad (4x^2+2x+1)(2x^3-1)(x^4+x^3+2x^2-x+1) \times \\
&\qquad (x^6-x^3-1)(4x^6+2x^3+1)(x^{12}+x^9+2x^6-x^3+1)(2x^{12}-x^9-x^3+3).
\end{aligned}$$

We have to compute the complete set of polynomial solutions of $\tilde{L}\tilde{y} = 0$. The degree of $\tilde{\ell}_2, \tilde{\ell}_1, \tilde{\ell}_0$ are respectively 16, 46, 54. Using Lemma 2.5, we find that the degree of a nonzero polynomial solution is necessarily 4 or 5. Following Algorithm 6, we equate the coefficients on both sides of $\tilde{L}\tilde{y} = 0$ up to degree 54, and we obtain that $\tilde{y} = \tilde{y}_0 + \cdots + x^5 \tilde{y}_5$ is solution of $\tilde{L}\tilde{y} = 0$ if and only if the vector $(\tilde{y}_0, \ldots, \tilde{y}_5)$ is solution of a system of $h = 163$ equations. A basis of solutions turns out to consist

of $(2x-1)(8x-1)(x^2-4x-1)$ and $(x^2-x-1)(8x-1)(x^2-4x-1)$. Consequently, a basis of rational-function solutions of $Ly=0$ consists of

$$\frac{1}{2x-1} \text{ and } \frac{1}{x^2-x-1}.$$

Remark 3.24. When Mahler equations are considered in difference Galois theory [10, 18], the interest tends to be in base fields on which M acts as an automorphism, such as $\mathbb{K}((x^{1/*}))$ and $\mathbb{K}(x^{1/*}) = \bigcup_{n=1}^{+\infty} \mathbb{K}(x^{1/n})$. By combining the strategy of Algorithm 9 with Proposition 2.19 about possible ramifications, we obtain an algorithm that computes a basis of solutions of (EQN) in $\mathbb{K}(x^{1/*})$. Assuming $\mathrm{M}(n) = \tilde{\mathrm{O}}(n)$, it runs in $\tilde{\mathrm{O}}(2^{3r}d^3)$ ops when $b=2$ and in $\tilde{\mathrm{O}}(b^r d^2)$ ops when $b \geq 3$. Note that, as in §2.7, these complexity bounds hold even if ℓ_0 is zero.

4. The case $\ell_0 = 0$ and an algorithm for computing gcrd's

In this section, we drop the assumption $\ell_0 \neq 0$. More precisely, we consider a linear Mahler equation of the form (EQN), with $\ell_0 = \cdots = \ell_{w-1} = 0$ and $\ell_r \ell_w \neq 0$. We call the integer w the *M-valuation of* (EQN) and $d = \max_{k=w,\dots,r} \deg \ell_k$ its *degree*. We define the *M-valuation* and the *degree* of the corresponding operator (OPR) similarly. The goal of this section is to compute a linear Mahler equation with M-valuation equal to 0, such that the new equation and (EQN) have the same set of series solutions in $\mathbb{K}((x))$.

The algorithm proposed here, Algorithm 11, can be seen as an improvement over an algorithm given by Dumas in his thesis [11, §3.2.1]. In particular, Algorithm 10, borrowed from [11], performs the subtask of splitting an operator of positive M-valuation into a system of operators of zero M-valuation while preserving the solution set in $\mathbb{K}((x))$. Dumas's algorithm next makes use of the right Euclidean structure of the algebra $\mathcal{M}(\mathbb{K})$ of linear Mahler operators with coefficients in $\mathbb{K}(x)$, and transforms the system into a single, equivalent equation by computing a gcrd (greatest common right divisor) via Euclidean divisions. The problem of this approach is that the degree of the obtained equation explodes in the process. To avoid this, we change the second step of algorithm in [11] so as to reuse Algorithm 10 and cancellations of trailing instead of leading coefficients.

The splitting process of Algorithm 10 is explained in terms of *section maps* S_i, each of which maps a polynomial in x and M to a polynomial in x and M, and whose collection plays the role of a partial inverse for M: for $0 \leq i < b$, let S_i be the $\mathbb{K}$-linear map that sends $x^j M^{k+1}$ to $x^{(j-i)/b} M^k$ if $(j-i)/b$ is an integer and to 0 otherwise.

Lemma 4.1. *Let L be a linear Mahler operator L of the form (OPR) and have degree d and positive M-valuation. Then, whenever $0 \leq i < b$, the section $S_i(L)$ has degree at most d/b. Additionally, L can be reconstructed from its sections by*

$$L = \sum_{i=0}^{b-1} x^i M\, S_i(L). \tag{4.1}$$

Proof. The degree bound and relation (4.1) are shown by immediate calculations. □

Lemma 4.2. *Let L be a linear Mahler operator of the form (OPR), with order r, M-valuation w, and degree d. Then, Algorithm 10 returns a set of nonzero linear Mahler operators of order at most $r-w$, M-valuation 0, and degree at most db^{-w}.*

Input: A linear Mahler operator L with coefficients in $\mathbb{K}[x]$.
Output: A set of linear Mahler operators with coefficients in $\mathbb{K}[x]$ and M-valuation zero.

(1) If $L = 0$, return $\emptyset$.
(2) If L has M-valuation 0, return $\{L\}$.
(3) Return the union of the results of calling the algorithm recursively on each section $S_i(L)$ for $0 \le i < b$.

Algorithm 10. Split of (opr).

Proof. This is shown by a straightforward induction on w. □

Instead of considering usual Euclidean divisions according to decreasing powers, which would compute a gcrd as in [11], we use in Algorithm 11 linear combinations that kill constant terms: given two nonzero Mahler operators L_1 and L_2 with coefficients in $\mathbb{K}[x]$, M-valuation zero, and coefficient of M^0 respectively c_1 and c_2, we write $R(L_1, L_2)$ for the operator $c_2L_1 - c_1L_2$, whose coefficient of M^0 is zero. We call this operator the *interreduction* of L_1 and L_2 and a step of the algorithm that replaces an operator L_1 by an interreduction $R(L_1, L_2)$ a *reduction step*.

Lemma 4.3. *Let $\mathcal{L}$ be a system of Mahler operators. Replacing an element L of $\mathcal{L}$ by its sections $S_0(L), \dots, S_{b-1}(L)$ does not change the set of solutions of $\mathcal{L}$ in $\mathbb{K}((x))$. Nor does replacing L_1 by the interreduction $R(L_1, L_2)$ where L_1, L_2 are distinct elements of $\mathcal{L}$.*

Proof. The second claim is obvious. Regarding the first one (already in [11, §3.2.1]), the decomposition (4.1) shows that any common solution of the $S_i(L)$ is a solution of L. If, conversely, y is an *unramified* solution of L, then the $x^i M S_i(L)\, y$, $0 \le i < b$, have disjoint support, hence $S_i(L)\, y = 0$ for all i. □

Here, the degree of $R(L_1, L_2)$ may well be the sum of the degrees of L_1 and L_2, but having generated a multiple of M makes it possible to apply splitting and keep degrees under control. This leads to Algorithm 11, whose correctness and complexity are given in the following proposition.

It is worth mentioning that, in general, the equation $\tilde{L}(y) = 0$ returned by Algorithm 11 does not have the same set of solutions in $\mathbb{K}((x^{1/*}))$ as the equation $L(y) = 0$. As an example, let $b = 2$ and consider $L = M^2 - xM$. We have $\tilde{L} = 1$, and the solution space in $\mathbb{K}((x^{1/*}))$ of $\tilde{L}(y) = 0$ is $\{0\}$. On the other hand, the solution space in $\mathbb{K}((x^{1/*}))$ of $L(y) = 0$ is the $\mathbb{K}$-vector space spanned by $x^{1/2}$.

Proposition 4.4. *The operator L has the same set of solutions in $\mathbb{K}((x))$ as the operator $\tilde{L}$ returned by Algorithm 11. This operator has order $\tilde{r} \le r - w$, M-valuation 0, and degree $\tilde{d} \le db^{-w}$. Furthermore, Algorithm 11 runs in $\mathrm{O}(rb^r\, \mathrm{M}(d/b^w))$ ops.*

Proof. Because $L \neq 0$ and by construction of Algorithm 10, the initial set $\mathcal{L}$ is nonempty. Next, by construction of Algorithm 11, at any time of a run, $\mathcal{L}$ is nonempty and contains only elements of outputs from Algorithm 10, so that, by Lemma 4.2, if Algorithm 11 terminates, its output must be nonzero and of M-valuation zero. Lemma 4.3 implies that the original operator L, the system $\mathcal{L}$ at

Input: A nonzero linear Mahler operator L of the form (OPR), order r, M-valuation w, and degree d.
Output: A linear Mahler operator $\tilde{L}$ of order $\tilde{r} \leq r - w$, M-valuation 0, and degree $\tilde{d} \leq db^{-w}$.

(1) Let $\mathcal{L}$ be the result of applying Algorithm 10 to L.
(2) While $\mathcal{L}$ has at least two elements:
   (a) choose L_1 with highest order in $\mathcal{L}$, then L_2 from $\mathcal{L} \setminus \{L_1\}$;
   (b) compute the result $\mathcal{L}'$ of applying Algorithm 10 to the interreduction $R(L_1, L_2)$;
   (c) replace $\mathcal{L}$ by $(\mathcal{L} \setminus \{L_1\}) \cup \mathcal{L}'$.
(3) Return the element $\tilde{L}$ of the singleton $\mathcal{L}$.

ALGORITHM 11. Normalization to $\ell_0 \neq 0$.

any time of the run, and therefore the final operator $\tilde{L}$, all share the same set of solutions in $\mathbb{K}((x))$.

Let us prove the bound on the order and the degree of $\tilde{L}$. By Lemma 4.2, the set $\mathcal{L}$ computed at step 1 consists of Mahler operators with orders bounded by $r - w$ and degrees bounded by db^{-w}. These bounds keep on holding after each run of the loop body at step 2: As the operators L_1 and L_2 chosen at step 2a satisfy the property, their combination $R(L_1, L_2)$ (including the case it is zero) has order bounded by $r - w$, degree bounded by $2db^{-w}$, and positive valuation. By Lemma 4.2, the set $\mathcal{L}'$ computed at step 2b consists of Mahler operators with orders bounded by $r - w - 1$ and degrees bounded by $2db^{-(w+1)}$. As $2/b \leq 1$, the set $\mathcal{L}$ retains the property after the update at step 2c. Therefore, if the algorithm terminates, it returns at step 3 an element of $\mathcal{L}$, therefore with the announced order and degree bounds.

We finally prove termination and complexity by a joint argument. To this end, we represent the process of Algorithm 11 by an oriented tree labeled by operators L_w^n, for integers n and words w on the alphabet $\{0, \dots, b-1\}$. These operators L_w^n will be the operators considered during the execution of the algorithm. This tree is rooted at the node labeled $L_\epsilon^0 = L$, and evolves by following the execution of Algorithm 11. Each time a section of an operator L_w^n is computed by the subtask of Algorithm 10, whether it be at step 1 or at step 2b, the tree is augmented by new edges from L_w^n to its subsection $L_{wj}^n = S_j(L_w^n)$. For each choice of $L_1 = L_w^n$ and $L_2 = L_{w'}^{n'}$ at step 2a, the tree is augmented by a new edge labeled $L_{w'}^{n'}$, from L_w^n to L_ϵ^{m+1}, if m is the larger upper index in the tree before reduction. Thus, one obtains that at each stage of the execution, the set $\mathcal{L}$ is equal to the collection of nonzero leaves of the current tree. Now, by construction of the tree and by design of the algorithm, a reduction step results either in a zero operator or in an operator with positive M-valuation that is immediately split to its sections. Therefore, following a path from the root to a leaf, two reduction edges can only appear if separated by at least one section edge. As section edges reduce orders by at least 1, while reduction edges do not increase orders, the tree has to be finite and the algorithm terminates. The only arithmetic operations of the algorithm are the polynomial products involved in the

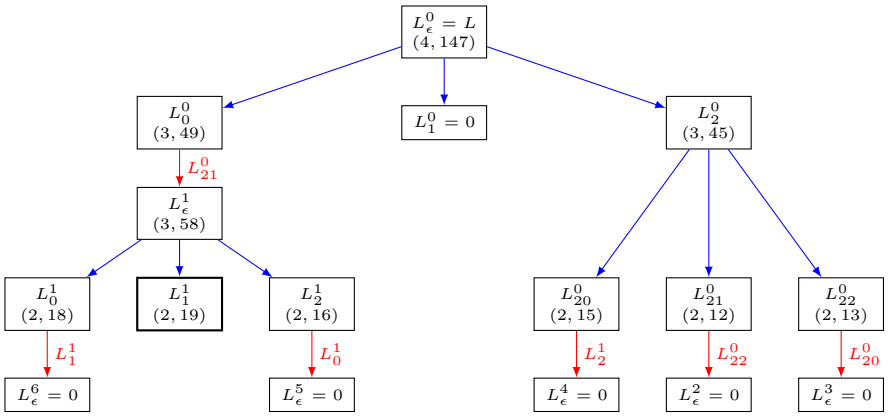

FIGURE 6. Execution of Algorithm 11 on the operator of Example 4.6. Each nonzero operator is given with a corresponding pair (order, degree). Operators are generated in the following order: $L^0_\epsilon = L$, L^0_0, L^0_1, L^0_2, L^0_{20}, L^0_{21}, L^0_{22}, L^1_ϵ, L^1_0, L^1_1, L^1_2, L^2_ϵ, L^3_ϵ, L^4_ϵ, L^5_ϵ, L^6_ϵ. Blue and red arrows respectively represent section and reduction steps. Labels on (red) arrows provide the auxiliary operators used for reduction. The process starts with $L^0_\epsilon = L$ and ends with L^1_1. Observe the strict decrease of orders along blue edges and large decrease along red edges. Also observe that degrees are divided by at least 3 on blue edges and, for the only nontrivial red edge of this example, how the reduction of L^0_0 by L^0_{21} induces an increase of the degree from 49 to 58, which is not more than $49 + 12$.

computation of the $R(L_1, L_2)$ at step 2b. It was proved above that any operator of $\mathcal{L}$ has degree bounded by d/b^w. Because operators all have order at most r and as the size of the tree bounds the number of reductions, the algorithm has total complexity $\mathrm{O}(rb^r\,\mathrm{M}(d/b^w))$. □

Remark 4.5. A slightly better complexity can be obtained by a variant of Algorithm 11, in which the L_1 at step 2a is not chosen as having maximal order, but according to a notion of depth in the tree introduced for the proof of Proposition 4.4. Doing so guarantees a better behavior of degrees, with a geometric decrease with depth, as opposed to the uniform bound d/b^w used in the proof above.

Define the depth β of a node L^n_w in the tree as the number of section edges from the root L^0_ϵ to L^n_w, and change the strategy at step 2a to choose L_1 among the elements of $\mathcal{L}$ of lowest depth. By another induction, L^n_w has order not more than $r - \beta$, as in the proof above, but its degree is not more than d/b^w if $\beta \le w$, and not more than $(2/b)^{\beta-w}(d/b^w)$ if $\beta > w$. A bound on the complexity becomes

$$\sum_{\beta=w}^{r} (r+1)b^\beta\,\mathrm{M}\left(\frac{2^{\beta-w}d}{b^\beta}\right) \le \mathrm{O}\left(r\,\mathrm{M}(2^r d/b^w)\right).$$

This bound is better than the original complexity $\mathrm{O}(rb^r\,\mathrm{M}(d/b^w))$ when $b \ge 3$. For $b = 2$, the new bound is not tight and the variant algorithm has the same complexity bound as Algorithm 11.

Example 4.6. We apply Algorithm 11 with $b = 3$ and the operator

$$L = \ell_1 M + \ell_2 M^2 + \ell_3 M^3 + \ell_4 M^4$$

with

$$\begin{aligned}
\ell_1 &= x^9(1 - x^{15} + x^{51} + x^{54} - x^{87} + x^{108})(1 - x^{12} + x^{24}),\\
\ell_2 &= -x^3\big(1 + x^6 - x^{20} - x^{21} + x^{30} + x^{32} + x^{33} + x^{36} - x^{44} - x^{45} + x^{54} + x^{56}\\
&\qquad + x^{57} + x^{60} - x^{68} - x^{69} + x^{80} + x^{81} + x^{84} + x^{90} - x^{92} - x^{93} + x^{104}\\
&\qquad + x^{105} + x^{108} + x^{114} - x^{116} - x^{117} + x^{138} + x^{144}\big),\\
\ell_3 &= \big(1 + x^3 - x^5 + x^{17} + x^{18} + x^{21} - x^{23} - x^{29} + x^{35} + x^{36} + x^{39} - x^{47} + x^{54}\\
&\qquad + x^{57} + x^{72} + x^{75} + x^{90} + x^{93} - x^{95} + x^{107} + x^{108} + x^{111} - x^{113} - x^{119}\\
&\qquad + x^{125} + x^{126} + x^{129} - x^{137} + x^{144} + x^{147}\big),\\
\ell_4 &= -(1 + x^{27} + x^{54})(1 - x^{27} + x^{54})(1 - x^5 + x^{17} + x^{18} - x^{29} + x^{36}).
\end{aligned}$$

Starting from $L^0_\epsilon = L$, we compute its sections (see Fig. 6, blue edges): first, $L^0_0 = S_0(L^0_\epsilon)$, which has M-valuation 0 so that the process of splitting stops for it; next, $L^0_1 = S_1(L^0_\epsilon)$, which is zero and is dropped; last, $L^0_2 = S_2(L^0_\epsilon)$, which has M-valuation 1. Splitting continues for the latter and provides $L^0_{20} = S_0(L^0_0)$, $L^0_{21} = S_1(L^0_2)$, $L^0_{22} = S_2(L^0_0)$, all with M-valuation 0. Note that during this splitting, the operators L^0_ϵ, $L^0_1 = 0$, and L^0_2 disappear. A reduction is made (see Fig. 6, red edges) where $R(L^0_0, L^0_{21}) = L^6_\epsilon$ replaces L^0_0. The process continues and, at the end, there only remains

$$\begin{aligned}
L^1_1 &= x^5(1 + x + x^2)(1 - x + x^2)(1 - x^4 + x^8)\\
&\quad - x^3(1 + x + x^2)(1 - x + x^2)(1 - x^2 + x^4 - x^6 + x^8)(1 + 2\,x^2 + x^4)M\\
&\quad + x^3(1 + x + x^2)(1 - x + x^2)(1 + x^3 + x^6)(1 - x^3 + x^6)M^2.
\end{aligned}$$

It is worth noting that L^1_1 has a content $c = x^3(1 + x + x^2)(1 - x + x^2)$, so that we can write $L^1_1 = c\bar{L}^1_1$ where $\bar{L}^1_1$ is a primitive polynomial (with respect to M). The computation shows that L is in the left ideal generated by $\bar{L}^1_1$ in the algebra $\mathcal{M}(\mathbb{Q})$. This and exhibiting the M-valuation $w = 1$ of L provides factorizations $L = L'M = L''M\bar{L}^1_1$. We can say that M^w has been pushed as much as possible to the left. Using Algorithm 9, we find that a basis of solutions of L^1_1 in $\mathbb{K}(x)$ is given by 1 and $\frac{x}{x^2-1}$. Since L^1_1 has order two, this also forms a basis of solutions of L^1_1 in $\mathbb{K}((x))$, as a consequence of Proposition 2.3, and by Proposition 4.4, a basis of solutions of L in $\mathbb{K}((x))$.

We now proceed to prove that Algorithm 11 indeed computes a gcrd with controlled degree. This is proved in Theorem 4.9 below, using the following lemmas.

Lemma 4.7. *For any operators P_1, P_2, and any integer i such that $0 \le i < b$, $S_i(P_1MP_2) = S_i(P_1M)P_2$.*

Proof. By linearity, it is sufficient to consider $P_1 = x^{j_1}M^{k_1}$ and $P_2 = x^{j_2}M^{k_2}$. Then, $P_1MP_2 = x^{j_1+b^{k_1+1}j_2}M^{k_1+k_2+1}$. Either b divides $j_1 - i$ and

$$S_i(P_1MP_2) = x^{(j_1-i)/b+b^{k_1}j_2}M^{k_1+k_2} = x^{(j_1-i)/b}M^{k_1}x^{j_2}M^{k_2} = S_i(P_1M)P_2,$$

or b does not divide $j_1 - i$ and both extreme terms are zero, thus equal again. □

Lemma 4.8. *For any operators P_1, P_2, and P, all of M-valuation 0, let c be the coefficient of M^0 in P. Then, $R(P_1P, P_2P) = cR(P_1, P_2)P$.*

Proof. The property holds, as obviously the coefficient of M^0 in a product is the product of the coefficients of M^0 in the factors. □

Theorem 4.9. *Steps 2 and 3 of Algorithm 11 compute a gcrd of the elements of the split $\mathcal{L}$ of L obtained at step 1. The degree of this particular gcrd is bounded by the maximal degree of the elements of $\mathcal{L}$.*

Proof. Let I denote the left ideal $\mathcal{M}(\mathbb{K})\mathcal{L}$ generated by $\mathcal{L}$ at any time in the run of the algorithm. Call G the monic gcrd of the elements of the set $\mathcal{L}$ as obtained from L at the end of step 1. By (4.1), G is a right factor of L. By the definition of $R(\cdot,\cdot)$ and because of (4.1) again, the ideal I can only increase during the run of the algorithm, so that during step 2, $\mathcal{M}(\mathbb{K})L \subset \mathcal{M}(\mathbb{K})G \subset I$.

We show by induction that G is a right factor of all elements of $\mathcal{L}$ at any time in step 2, in other words, that $I \subset \mathcal{M}(\mathbb{K})G$. This is true by the definition of G when entering the loop. The set $\mathcal{L}$ contains only elements with M-valuation 0, and it cannot be empty when entering the loop, so G has M-valuation 0 as well. At any step 2b, divisibility on the right by G is preserved for $R(L_1, L_2)$, by Lemma 4.8. As $R(L_1, L_2)$ has positive M-valuation, one can choose $P_2 = G$ and find P_1 so as to write $R(L_1, L_2) = P_1 M P_2$. By Lemma 4.7, it follows that divisibility on the right by G is also preserved for each element of $\mathcal{L}'$, then for each element of the next value of $\mathcal{L}$.

As a consequence, during step 2, I constantly equals $\mathcal{M}(\mathbb{K})G$. In particular, the final operator $\tilde{L}$ is proportional to G.

The degree bound was proved as part of Proposition 4.4. □

Remark 4.10. Note that the origin of the initial $\mathcal{L}$ as a split of L, at step 1 of Algorithm 11 plays no role in the proof of Theorem 4.9. Thus, Algorithm 11 implicitly contains an algorithm for computing the gcrd of any family $\mathcal{L}$ of operators of M-valuation zero.

Remark 4.11. We developed Algorithm 11 without targeting a gcrd and realized Theorem 4.9 (and Remark 4.10) only a posteriori. As Algorithm 11 indeed works by computing a gcrd as the original algorithm in [11], it is now instructive to compare the result of Proposition 4.4 with bounds on the size of gcrds of Mahler operators given by existing methods. Such a bound can be computed using a variant of the subresultant argument given by Grigor'ev [12, §5] in the differential case.

Let $L_1, \dots, L_n$ be operators of respective order $r_1 \geq r_2 \geq \cdots \geq r_n \geq 1$ and degree $d_1, \dots, d_n \leq \delta$. Let $G = U_1 L_1 + \cdots + U_n L_n$ be their greatest common right divisor. We can assume that the order of each term $U_i L_i$ is less than $t = r_1 + r_n$. Indeed, for all i, j the linear equation $V_{i,j} L_i = V_{j,i} L_j$ with $V_{i,j}$, resp. $V_{j,i}$, constrained to have degree at most r_j, resp. at most r_i, has nontrivial solutions. Via Euclidean divisions $U_i = Q_i V_{i,n} + R_i$, we obtain $G = \sum_i (Q_i V_{i,n} + R_i) L_i = \sum_i Q_i V_{n,i} L_n + \sum_i R_i L_i = \sum_i \tilde{U}_i L_i$ where the $\tilde{U}_i$ for $i \leq n-1$ have order less than r_n. The $n-1$ first terms $\tilde{U}_i L_i$ as well as G itself have order less than $r_1 + r_n$, hence the same must be true of $\tilde{U}_n L_n$.

Consider a Sylvester-like matrix $S \in \mathbb{K}[x]^{s \times t}$ with rows

$$\mathcal{R}(L_1), \mathcal{R}(ML_1), \dots, \mathcal{R}(M^{t-r_1-1}L_1), \dots, \mathcal{R}(L_n), \mathcal{R}(ML_n), \dots, \mathcal{R}(M^{t-r_n-1}L_n),$$

where, for any operator $L = \sum_k \ell_k M^k$, we denote $\mathcal{R}(L) = (\ell_{t-1}, \dots, \ell_0)$. Call $C_0, C_1, \dots, C_{t-1}$ the columns of S, listed from right to left (so that C_j contains the coefficients of M^j in $M^k L_i$), and $C_{j,0}, C_{j,1}, \dots, C_{j,s-1}$ the entries of C_j. Let m denote the order of G, and choose $J \subseteq \{m+1, \dots, t-1\}$ of cardinality $|J| =$

$\operatorname{rk} S - 1$ in such a way that the columns C_j with $j \in J$ form a basis of the span of $C_{m+1}, \dots, C_{t-1}$, while the C_j for $j \in \{m\} \cup J$ form a basis of the full column space of S. To see that such a J exists, consider a row echelon form of S: since $\mathcal{R}(G)$ belongs to the left image of S and G has minimal order among the nonzero elements of the ideal $\sum_i \mathcal{M}(\mathbb{K})L_i$, the rightmost pivot lies on column m. Further, let $I \subseteq \{0, \dots, s-1\}$ be such that the submatrix $(C_{j,i})$, $i \in I$, $j \in J \cup \{m\}$ of S is nonsingular. Call D_m the corresponding minor, and more generally define D_k as the determinant of the submatrix $(C_{j,i})$, $i \in I$, $j \in J$, extended on the right by a copy of C_k. Expanding D_k along the last column yields $D_k = \sum_{i=0}^{s-1} u_i C_{k,i}$, where the u_i do not depend on k. For each $k > m$, the determinant D_k is zero, as C_k is in the span of the C_j for $j \in J$. It follows that the vector $(0, \dots, 0, D_m, \dots, D_0)$ belongs to the left image of S. Thus, there is a gcrd of $L_1, \dots, L_n$ with polynomial coefficients whose coefficients are minors of S.

The entries of $\mathcal{S}$ have degree bounded by $\delta' = \max_{i=1}^{n}(b^{t-r_i-1}d_i)$. Therefore, the degree of G is as most $t\delta' \le 2r_1 b^{r_1-1}\delta \le r_1 b^{r_1}\delta$. Using fast polynomial linear algebra, it is plausible that one could actually compute G based on this approach with a complexity of the type $\tilde{\mathrm{O}}(\delta' t^\omega) = \tilde{\mathrm{O}}(b^{r_1}\delta)$. Now, the gcrd in the algorithm of [11] is that of a family of iterated sections of the input operator L. In terms of the order r and degree d of L, this family can involve elements simultaneously of order $r-1$ and degree $d/2$. Thus, Grigor'ev's approach (at least in a straightforward way) would lead to a complexity bound similar to that of Proposition 4.4, but an exponentially worse bound on the degree of the output for large r.

This result leaves open the question of devising algorithms for computing solutions of linear Mahler equations that run in polynomial time in r and d, for all possible combinations of these parameters, even when the trailing coefficient ℓ_0 of the equation is zero. In particular, it would be interesting to see if the bounds on the size of an operator equivalent to L implied by Algorithm 10 would be enough to extend the algorithms of §2–3 to the case where ℓ_0 is zero, without going through the explicit computation of such an operator.

We end the section by providing an extension of Algorithm 11, which computes a gcrd for a family of operators of arbitrary M-valuations.

Theorem 4.12. *Algorithm 12 computes a gcrd of the input operators $L_1, \dots, L_s$.*

Proof. Observe that the minimal M-valuation of operators in a family is the minimal M-valuation of elements of the left ideal generated by the family, in particular, the M-valuation of any gcrd of the family. This justifies the general design of the algorithm, with the factorization of M^w on the right at step 1.

By construction, the L_i''s thus obtained have orders at most $r - w$ and degrees at most d, and at least one, say L_1', has M-valuation zero. Let G' denote the monic gcrd of the L_i', which, as L_1', has M-valuation zero. By Lemma 4.7, G' is a right-hand factor of all elements of the set $\mathcal{L}$ computed at step 2. By a proof similar to the one for Theorem 4.9, it remains so for all subsequent values of $\mathcal{L}$, so for the $\tilde{L}$ of step 4 as well.

As $\tilde{L}$ is also obviously a right-hand factor of all previously computed operators, including the L_i''s, $\tilde{L}$ is a gcrd of the latter. This concludes the proof. □

Input: A finite family $\{L_i\}_{i=1}^s$ of linear Mahler operators with polynomial coefficients, orders at most r, minimal M-valuation w, and degrees at most d.
Output: A linear Mahler operator $\tilde{L}$ of order $\tilde{r} \leq r$, M-valuation w, and degree $\tilde{d} \leq d$.

(1) Write each L_i in the form $L_i' M^w$, for a polynomial L_i' in x and M.
(2) Let $\mathcal{L}$ be the union of the results of applying Algorithm 10 to the L_i''s.
(3) While $\mathcal{L}$ has at least two elements:
  (a) choose L_1 with highest order in $\mathcal{L}$, then L_2 from $\mathcal{L} \setminus \{L_1\}$;
  (b) compute the result $\mathcal{L}'$ of applying Algorithm 10 to the interreduction $R(L_1, L_2)$;
  (c) replace $\mathcal{L}$ by $(\mathcal{L} \setminus \{L_1\}) \cup \mathcal{L}'$.
(4) Write $\tilde{L}$ for the single element of the singleton $\mathcal{L}$ and return $\tilde{L} M^w$.

Algorithm 12. Computation of a gcrd of an arbitrary family.

References

1. Shreeram S. Abhyankar, *Two notes on formal power series*, Proc. Amer. Math. Soc. **7** (1956), no. 5, 903–905.
2. S. A. Abramov, *Rational solutions of linear differential and difference equations with polynomial coefficients*, Zh. Vychisl. Mat. i Mat. Fiz. **29** (1989), no. 11, 1611–1620, 1757.
3. ———, *Rational solutions of linear difference and q-difference equations with polynomial coefficients*, Programmirovanie (1995), no. no. 6, 3–11.
4. Jason P. Bell and Michael Coons, *Transcendence tests for Mahler functions*, Proc. Amer. Math. Soc. (2015), 9 pages. To appear. http://arxiv.org/abs/1511.07530.
5. Alin Bostan, Philippe Flajolet, Bruno Salvy, and Éric Schost, *Fast computation of special resultants*, J. Symbolic Comput. **41** (2006), no. 1, 1–29.
6. Manuel Bronstein, *On solutions of linear ordinary difference equations in their coefficient field*, J. Symbolic Comput. **29** (2000), no. 6, 841–877.
7. Claude Chevalley, *Introduction to the theory of algebraic functions of one variable*, Mathematical surveys and monographs, American Mathematical Society, Providence, R.I, 1951.
8. Gilles Christol, *Ensembles presque periodiques k-reconnaissables*, Theoret. Comput. Sci. **9** (1979), no. 1, 141–145.
9. Gilles Christol, Teturo Kamae, Michel Mendès France, and Gérard Rauzy, *Suites algébriques, automates et substitutions*, Bull. Soc. Math. France **108** (1980), no. 4, 401–419.
10. Thomas Dreyfus, Charlotte Hardouin, and Julien Roques, *Hypertranscendance of solutions of Mahler equations*, J. Eur. Math. Soc. (2015), 26 pages. To appear. http://arxiv.org/abs/1507.03361.
11. Philippe Dumas, *Récurrences mahlériennes, suites automatiques, études asymptotiques*, Thèse de doctorat, Université Bordeaux I, 1993, 241 pages. https://tel.archives-ouvertes.fr/tel-00614660.
12. D. Yu. Grigor'ev, *Complexity of factoring and calculating the gcd of linear ordinary differential operators*, J. Symbolic Comput. **10** (1990), no. 1, 7–37.
13. Peter Henrici, *Applied and computational complex analysis*, vol. III, Wiley Interscience, 1986.
14. Oscar H. Ibarra, Shlomo Moran, and Roger Hui, *A generalization of the fast LUP matrix decomposition algorithm and applications*, J. Algorithms **3** (1982), no. 1, 45–56.
15. Kurt Mahler, *Arithmetische Eigenschaften der Lösungen einer Klasse von Funktionalgleichungen*, Math. Ann. **103** (1929), no. 1, 532.

16. Kumiko Nishioka, *Mahler functions and transcendence*, Lecture Notes in Mathematics, vol. 1631, Springer Verlag, Berlin, 1996.
17. Federico Pellarin, *An introduction to Mahler's method for transcendence and algebraic independence*, t-motives: Hodge structures, transcendence and other motivic aspects (G. Boeckle, D. Goss, U. Hartl, and M. Papanikolas, eds.), European Mathematical Society, 2016, 47 pages. To appear. Proceedings of BIRS, Banff, Canada, 2009. http://arxiv.org/abs/1005.1216.
18. Julien Roques, *On the algebraic relations between Mahler functions*, Trans. Amer. Math. Soc. (2015), 36 pages. To appear. https://www-fourier.ujf-grenoble.fr/~jroques/mahler.pdf.
19. ———, *On the local structure of Mahler modules*, https://www-fourier.ujf-grenoble.fr/~jroques/OTLSOMM.pdf, 2016.
20. Joris van der Hoeven, *Relax, but don't be too lazy*, J. Symbolic Comput. **34** (2002), 479–542.
21. Robert John Walker, *Algebraic curves*, Springer Verlag, New York, Paris, 1978, reprint from the 1950 edition, published by Princeton University Press.

Frédéric Chyzak, INRIA, Université Paris-Saclay (France)
E-mail address: frederic.chyzak@inria.fr

Thomas Dreyfus, Univ Lyon, Université Claude Bernard Lyon 1, CNRS UMR 5208, Institut Camille Jordan, 43 blvd. du 11 novembre 1918, F-69622 Villeurbanne cedex, France
E-mail address: dreyfus@math.univ-lyon1.fr

Philippe Dumas, INRIA, Université Paris-Saclay (France)
E-mail address: philippe.dumas@inria.fr

Marc Mezzarobba, CNRS (France), Sorbonne Universités, UPMC Univ Paris 06, CNRS, LIP6 UMR 7606, 4 place Jussieu 75005 Paris
E-mail address: marc@mezzarobba.net