On solutions of Linear Ordinary Difference Equations in their Coefficient Field

Manuel Bronstein

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

On solutions of linear ordinary difference equations in their coefficient field

Manuel Bronstein

N° 3797

Novembre 1999

THÈME 2

ISSN 0249-6399 ISRN INRIA/RR--3797--FR+ENG

INRIA
SOPHIA ANTIPOLIS

On solutions of linear ordinary difference equations in their coefficient field

Manuel Bronstein

Thème 2 — Génie logiciel
et calcul symbolique
Projet CAFÉ

Rapport de recherche n° 3797 — Novembre 1999 — 43 pages

Abstract: We extend the notion of monomial extensions of differential fields, *i.e.* simple transcendental extensions in which the polynomials are closed under differentiation, to difference fields. The structure of such extensions provides an algebraic framework for solving generalized linear difference equations with coefficients in such fields. We then describe algorithms for finding the denominator of any solution of those equations in an important subclass of monomial extensions that includes transcendental indefinite sums and products. This reduces the general problem of finding the solutions of such equations in their coefficient fields to bounding their degrees. In the base case, this yields in particular a new algorithm for computing the rational solutions of q–difference equations with polynomial coefficients.

Key-words: difference equations, q–difference equations, rational solutions, hypergeometric coefficients

Unité de recherche INRIA Sophia Antipolis
2004, route des Lucioles, B.P. 93, 06902 Sophia Antipolis Cedex (France)
Téléphone : 04 92 38 77 77 - International : +33 4 92 38 77 77 — Fax : 04 92 38 77 65 - International : +33 4 92 38 77 65

Sur les solutions des équations linéaires ordinaires aux différences dans leur corps de base

Résumé : Nous généralisons le concept d'extension monomiale d'un corps différentiel aux corps aux différences. La structure de ces extensions donne un cadre algébrique pour résoudre les équations linéaires aux différences généralisées à coefficients dans ces corps. Nous décrivons ensuite des algorithmes de calcul du dénominateur des solutions de ces équations dans une classe importante d'extensions, qui contient les sommes et produits indéfinis. Cela réduit la résolution de ces équations au problème de la majoration du degré des solutions. Comme cas particulier, on obtient un nouvel algorithme de calcul des solutions rationnelles d'équations aux q–différences à coefficients polynomiaux.

Mots-clés : équations aux différences, équations aux q–différences, solutions rationnelles, coefficients hypergéométriques

Introduction

An important problem in the theory of difference equations is to determine whether a given difference equation has a "closed–form" solution. An appropriate notion of "closed–form", which generalizes the concept of Liouvillian solutions of differential equations, together with an algorithm for computing such solutions, has been recently described in [13]. That algorithm reduces the problem to computing the hypergeometric solutions of associated equations, but in many cases it turns out that computing their rational solutions is sufficient [7]. This is the problem that we address in this paper, namely given a difference field k with its automorphism σ, $g \in k$ and a linear ordinary difference operator L with coefficients in k, to compute all the solutions in k of the equation $Ly = g$. There are known solutions to this problem when $k = C(x)$ and σ is the automorphism over C given by $\sigma x = x + 1$ [3], or $\sigma x = qx$ [4, 5][1] but no generalization to other automorphisms or more general coefficient fields. In the theory of linear ordinary differential equations, the concepts of Liouvillian [21] and monomial [8, 10] extensions of differential fields has led to extensions of rational techniques that solve a similar problem with more general functions allowed in the coefficients [9, 21]. In the case of difference fields, Karr introduced $\Pi\Sigma$–fields and used them to develop summation algorithms that allow more general summands [17, 16]. In his conclusion to [17], he states (considering the summation problem as equivalent to solving first–order difference equations):

> The techniques of this paper rely very heavily upon linearity, suggesting that the generalization to n^{th} order (or simultaneous) linear difference equations may not be too difficult.

In this paper, we describe an appropriate algebraic framework for the above generalization by approaching the problem from the point of view of differential fields, and generalizing the notion of monomial extensions to σ–derivations, *i.e.* derivations satisfying the modified Leibniz rule $\delta(ab) = \sigma(a)\delta(b)+\delta(a)b$ for an arbitrary endomorphism σ. After introducing the basic properties of those objects in Section 1, we define monomial extensions and generalize most of their differential properties in Section 2, thereby obtaining a theory valid for both differential and generalized difference fields. We then generalize the specialization technique of [11] in Section 3 by showing that the existence of a nontrivial special polynomial allows us to compute the Taylor series solutions of an arbitrary linear functional equation, therefore to compute its polynomial solutions of any given degree. Denominators can only be handled in a restricted class of extension, essentially the *first–order linear extensions* of [17, 16], which we study in Section 4, in particular determining the structure of the special semigroup in those extensions. Section 5 generalizes Abramov's dispersion to monomial extensions and defines a factorization called the *orbital decomposition*, which make the link between the dispersion and Karr's specification of equivalence, and can provide a more efficient way of computing dispersions in polynomial rings for which irreducible factorization is available. Finally, Section 6 generalizes the algorithms of [3, 4, 5] to first–order linear extensions. We

[1] An error in [4] has been corrected in [5].

do not provide a general algorithm for bounding the degree of polynomial solutions, so we do not claim to have a complete algorithm for solving generalized difference equations in towers of monomial extensions. However, we have reduced this problem for arbitrary automorphisms and coefficients fields that are $\Pi\Sigma$–fields in the sense of [17, 16] to bounding the degree of polynomial solutions. Since this problem is solved for q–difference equations with polynomial coefficients [1, 6], we obtain a new algorithm for computing the rational solutions of such equations.

By convention, all integral domains and fields are commutative, but rings are not necessarily commutative. All rings and fields are of characteristic 0 and ideals are two–sided ideals. Given a ring R, its subring of units will be denoted R^*. We recall, and use throughout, that R^* is closed under any endomorphism of R, that automorphisms of an integral domain map irreducibles to irreducibles, and that all endomorphisms of a field are injective.

1 σ–derivations

We introduce in this section the generalization of derivations that will be used throughout this paper and recall their basic properties, together with the notion of skew–polynomials. Recall that the *center* of a ring R is the subring

$$Z(R) = \{a \in R \text{ such that } ax = xa \text{ for every } x \in R\}\ .$$

Definition 1 *Let R be a ring (resp. field) and σ an endomorphism of R. A* σ–derivation *is a map $\delta : R \to R$ satisfying*

$$\delta(a+b) = \delta a + \delta b \quad \textit{and} \quad \delta(ab) = \sigma a\, \delta b + \delta a\, b \quad \textit{for any } a, b \in R\,. \tag{1}$$

The triple (R, σ, δ) is called a σ–differential ring (resp. field). *An element $a \in R$ is called* invariant *if $\sigma a = a$,* periodic *if $\sigma^n a = a$ for some integer $n > 0$,* semi–invariant *if $\sigma a = ua$ for $u \in R^*$ and* semi–periodic *if $\sigma^n a = ua$ for $u \in R^*$ and $n > 0$. The set*

$$Const_{\sigma,\delta}(R) = \{a \in R \textit{ such that } \sigma a = a \textit{ and } \delta a = 0\}$$

is called the constant subring (resp. subfield) *of R with respect to σ and δ. A subring (resp. subfield) of R is called a* σ–differential subring (resp. subfield) *if it is closed under σ and δ.*

We write R_σ for the invariants of R, R^σ for its semi–invariants, $R_{\sigma^*} = \bigcup_{n>0} R_{\sigma^n}$ for its periodic elements and $R^{\sigma^*} = \bigcup_{n>0} R^{\sigma^n}$ for its semi–periodic elements. Some standard properties of derivations are straightforward to generalize.

Proposition 1 *For a given endomorphism σ, the set $\Omega_\sigma(R)$ of all the σ–derivations of R is a left $Z(R)$–module.*

Proof. Let $\delta_1, \delta_2 \in \Omega_\sigma(R)$ and $c \in Z(R)$. Let $\delta = c\delta_1 + \delta_2$ and $a, b \in R$. Then,

$$\delta(a+b) = c\delta_1(a+b) + \delta_2(a+b) = c\delta_1 a + c\delta_1 b + \delta_2 a + \delta_2 b = \delta a + \delta b\,,$$

and

$$\begin{aligned} \delta(ab) &= c\delta_1(ab) + \delta_2(ab) = c\sigma a\,\delta_1 b + c\delta_1 a\; b + \sigma a\;\delta_2 b + \delta_2 a\; b \\ &= \sigma a\;(c\delta_1 b + \delta_2 b) + (c\delta_1 a + \delta_2 a)b = \sigma a\;\delta b + \delta a\; b \end{aligned}$$

so $\delta \in \Omega_\sigma(R)$. Since the zero-map on R is a σ–derivation, $\Omega_\sigma(R)$ is a left $Z(R)$–module. □

Lemma 1 *Let (R, σ, δ) be a σ–differential ring (resp. field). Then,*

(i) *If R is a field, then*

$$\delta\frac{a}{b} = \frac{b\delta a - a\delta b}{b\sigma b} \tag{2}$$

for any $a, b \in R$, $b \neq 0$.

(ii) *$Const_{\sigma,\delta}(R)$ is a σ–differential subring (resp. subfield) of R.*

(iii) *For any $a_1, \ldots, a_n \in R$ and $n \geq 1$,*

$$\delta\left(\prod_{i=1}^{n} a_i\right) = \sum_{i=1}^{n}\left(\prod_{j=1}^{i-1}\sigma a_j\right)\delta(a_i)\left(\prod_{j=i+1}^{n} a_j\right). \tag{3}$$

Proof. (i) Suppose that R is a field, and let $a, b \in R$ with $b \neq 0$, and $c = a/b$. Then, $a = bc$, so

$$\delta a = \delta(bc) = \sigma b\;\delta c + c\delta b = \sigma b\;\delta\frac{a}{b} + \frac{a}{b}\,\delta b\,.$$

Hence,

$$\delta\frac{a}{b} = \frac{1}{\sigma b}\Big(\delta a - \frac{a}{b}\,\delta b\Big) = \frac{b\delta a - a\delta b}{b\sigma b}\,.$$

(ii) Let $C = \mathrm{Const}_{\sigma,\delta}(R)$. Since σ is an endomorphism, $\sigma 0 = 0$ and $\sigma 1 = 1$. Since δ is additive, $\delta(0) = \delta(0+0) = \delta(0) + \delta(0)$, so $0 \in C$. In addition, $\delta(1) = \delta(1 \times 1) = \delta(1) + \delta(1)$, so $1 \in C$. It follows from the definition of C that it is closed under σ and δ. Since σ and δ are additive, $\sigma(-a) = -\sigma a$ and $\delta(-a) = -\delta a$ for any $a \in R$. Let $c, d \in C$. Then, $\sigma(c-d) = \sigma c - \sigma d = c - d$ and $\delta(c-d) = \delta c - \delta d = 0 - 0 = 0$, so $c - d \in C$. In addition, $\sigma(cd) = \sigma c\;\sigma d = cd$ and $\delta(cd) = \sigma c\;\delta d + \delta c\;d = 0 + 0 = 0$, so $cd \in C$ and C is a σ–differential subring of R. Suppose that R is a field and that $d \neq 0$. Then, $\delta(1/d) = -\delta d/(d\sigma d) = 0$. In addition, $1 = \sigma(d \times 1/d) = \sigma(d)\sigma(1/d) = d\sigma(1/d)$, which implies that $1/d \in C$, hence that C is a σ–differential subfield of R.

(iii) By induction on n. The result is trivial for $n = 1$, so suppose that it holds for a given $n \geq 1$. We then have

$$\begin{aligned}
\delta\left(\prod_{i=1}^{n+1} a_i\right) &= \sigma\left(\prod_{i=1}^{n} a_i\right)\delta(a_{n+1}) + \delta\left(\prod_{i=1}^{n} a_i\right)a_{n+1} \\
&= \left(\prod_{i=1}^{n} \sigma a_i\right)\delta(a_{n+1}) + \left(\sum_{i=1}^{n}\left(\prod_{j=1}^{i-1}\sigma a_j\right)\delta(a_i)\left(\prod_{j=i+1}^{n} a_j\right)\right)a_{n+1} \\
&= \sum_{i=1}^{n+1}\left(\prod_{j=1}^{i-1}\sigma a_j\right)\delta(a_i)\left(\prod_{j=i+1}^{n+1} a_j\right).
\end{aligned}$$

□

A consequence of (3) is that for any a in a commutative σ–differential ring, we have

$$\delta(a^n) = \delta(a)\sum_{i=0}^{n-1} a^i\sigma(a)^{n-1-i} \quad \text{for } n \geq 1\,. \tag{4}$$

For σ–differential fields, this yields the σ–logarithmic derivative identity:

$$\frac{\delta(\prod_{i=1}^{n} a_i^{e_i})}{\prod_{i=1}^{n} a_i^{e_i}} = \sum_{i=1}^{n}\frac{\sigma\left(\prod_{j=1}^{i-1} a_j^{e_j}\right)}{\prod_{j=1}^{i-1} a_j^{e_j}}\frac{\delta a_i}{a_i}\sum_{j=0}^{e_i-1}\frac{\sigma(a_j^j)}{a_j^j}\,.$$

A σ–differential ring (R, σ, δ) is called a differential ring when $\sigma = 1_R$, a generalized difference ring when $\delta = \alpha(\sigma - 1_R)$ for some $\alpha \in R$, and a difference ring when $\delta = 0_R$. Because fields are commutative, it turns out that any σ–differential field is essentially either a differential or a generalized difference field.

Lemma 2 *Let (R, σ, δ) be a commutative σ–differential ring. Then,*

(i) *There are $\alpha, \beta \in R$ such that*

$$\alpha\delta = \beta(\sigma - 1_R)\,. \tag{5}$$

(ii) *If $\sigma \neq 1_R$ then α can be chosen to be nonzero in (5).*

(iii) *If $\delta \neq 0_R$ then β can be chosen to be nonzero in (5).*

Proof. Since R is commutative, $\delta(ab) = \delta(ba)$ for any $a, b \in R$, so applying (1) to both sides gives $\sigma a\ \delta b + \delta a\ b = \sigma b\ \delta a + \delta b\, a$ and, after rearranging,

$$(\sigma(a) - a)\,\delta b = (\sigma(b) - b)\,\delta a\,. \tag{6}$$

(i) Choosing any element $a \in R$ and letting $\alpha = \sigma(a) - a$ and $\beta = \delta a$, it follows from (6) that $\alpha\delta = \beta(\sigma - 1_R)$.

(ii) If $\sigma \neq 1_R$ then we can pick in (i) an element $a \in R$ such that $\sigma a \neq a$, which implies that $\alpha \neq 0$.
(iii) If $\delta \neq 0_R$ then we can pick in (i) an element $a \in R$ such that $\delta a \neq 0$, which implies that $\beta \neq 0$. □

As a consequence, if R is a field and $\sigma \neq 1_R$, then δ is a multiple of $\sigma - 1_R$, while if R is a field and $\delta \neq 0$, then σ is of the form 1_R plus a multiple of δ. It also means that the invariants of a σ–differential integral domain are the whole domain if σ is the identity, the constant subring otherwise. The semi–invariants and semi–periodic elements will be important for our algorithms so we describe their basic properties.

Lemma 3 *Let (R, σ, δ) be a σ–differential ring (resp. field).*

(i) *R_σ, R^σ, R_{σ^*} and R^{σ^*} all contain 0 and 1 and are all closed under σ. If σ is an automorphism of R, then $R_{\sigma^{-1}} = R_\sigma$, $R^{\sigma^{-1}} = R^\sigma$, $R_{\sigma^{-1*}} = R_{\sigma^*}$ and $R^{\sigma^{-1^*}} = R^{\sigma^*}$.*

(ii) *R_σ and R_{σ^*} are subrings (resp. subfields) of R. If R is commutative, then R^σ and R^{σ^*} are multiplicative monoids (resp. groups) containing R^*.*

(iii) *If R is commutative, and $\sigma^n a = ba$ for some integer $n > 0$ and $a, b \in R \setminus \{0\}$, then $\sigma(\Pi_n^\sigma a) = b\Pi_n^\sigma a$ where $\Pi_n^\sigma a = \prod_{i=0}^{n-1} \sigma^i a$. In particular $a \in R^{\sigma^n} \Rightarrow \Pi_n^\sigma a \in R^\sigma$.*

(iv) *If R is a unique factorization domain and σ is an automorphism of R, then R^{σ^*} is closed under taking factors, i.e. $a \in R^{\sigma^*} \setminus \{0\} \Rightarrow b \in R^{\sigma^*}$ for any $b \in R$ such that $b \mid a$.*

Proof. (i) 0 and 1 are in all four sets since they are invariant. Let $a \in R^{\sigma^n}$ for some $n > 0$ and $u \in R^*$ be such that $\sigma^n a = ua$. Then, $\sigma^n(\sigma a) = \sigma(\sigma^n a) = \sigma(ua) = \sigma(u)\sigma a$, which implies that R^{σ^n} is closed under σ, hence that R^σ and R^{σ^*} are closed under σ. Taking $u = 1$ in the above equation shows that R_{σ^n} is closed under σ, hence that R_σ and R_{σ^*} are closed under σ. If σ is an automorphism of R, then $v = \sigma^{-n}(u^{-1}) \in R^*$ and $\sigma^{-n} a = va$, which implies that $R^{\sigma^{-1^*}} = R^{\sigma^*}$. The other statements follow from taking $n = 1$ and/or $u = 1$.
(ii) Let $n, m > 0$, $a \in R_{\sigma^n}$ and $b \in R_{\sigma^m}$. Then, $\sigma^{nm}(a - b) = \sigma^{nm}(a) - \sigma^{nm}(b) = a - b$ and $\sigma^{nm}(ab) = \sigma^{nm}(a)\sigma^{nm}(b) = ab$, which implies that R_{σ^*} is a subring of R. Taking $n = m = 1$ shows that R_σ is a subring of R. Suppose now that R is commutative and let $u \in R^*$. Since $\sigma u = (u^{-1}\sigma u)u$ and $u^{-1}\sigma u \in R^*$, we have $u \in R^\sigma$, so $R^* \subseteq R^\sigma \subseteq R^{\sigma^*}$. Let now $a \in R^{\sigma^n}$, $b \in R^{\sigma^m}$ and $u, v \in R^*$ be such that $\sigma^n a = ua$ and $\sigma^n b = vb$. Then,

$$\sigma^{nm}(ab) = \sigma^{nm}(a)\sigma^{nm}(b) = \left(\prod_{i=0}^{m-1} \sigma^{in} u\right) a \left(\prod_{j=0}^{n-1} \sigma^{im} v\right) b = wab$$

where $w \in R^*$, implying that $ab \in R^{\sigma^*}$. Taking $n = m = 1$ shows that R^σ is a multiplicative monoid. If R is a field, then $\sigma^n(1/a) = 1/\sigma^n(a) = u^{-1}(1/a)$, which implies that R_{σ^*} and R_σ are subfields of R and that R^{σ^*} and R^σ are multiplicative groups.

(iii) This is verified directly:

$$\sigma(\Pi_n^\sigma a) = \sigma\left(\prod_{i=0}^{n-1}\sigma^i a\right) = \prod_{i=1}^{n}\sigma^i a = ba\prod_{i=1}^{n-1}\sigma^i a = b\Pi_n^\sigma a\,.$$

(iv) Let $a \in R^{\sigma^n}$ for some $n > 0$ and $u \in R^*$ be such that $\sigma^n a = ua$. Then, $c = \Pi_n^\sigma a \in R^\sigma$ by (iii) so $\sigma c = vc$ for some $v \in R^*$. Let $p_1, \ldots, p_m$ be the distinct irreducible factors of c in R. Since σ maps irreducibles to irreducibles, $\sigma^j p_i$ is an irreducible factor of c for any $j \geq 0$ and $1 \leq i \leq m$. Since the set $\{p_1, \ldots, p_m\}$ is finite, it follows that for each i, there are integers $e_i > f_i \geq 0$ and $c_i \in R^*$ such that $\sigma^{e_i} p_i = c_i \sigma^{f_i} p_i$, hence that $p_i \in R^{\sigma^*}$ since it is a semi–invariant of $\sigma^{e_i - f_i}$. Since R^{σ^*} is a multiplicative monoid containing $\{p_1, \ldots, p_n\}$ and R^*, it contains all the factors of c, and therefore all the factors of a since $a \mid c$. □

We now recall the notion of a skew–polynomial, which is a generalization of linear ordinary differential operators to σ–derivations.

Definition 2 *Let (R, σ, δ) be a σ–differential ring and X be an indeterminate over R. The* skew–polynomial ring over R, *denoted $(R[X]; \sigma, \delta)$, is the ring of univariate polynomials with the usual polynomial addition and the multiplication given by $Xa - \sigma(a)X = \delta a$ for any $a \in R$.*

Univariate skew–polynomials were first introduced in [19], who studied in particular their factorization properties. An important property that we use in the sequel is the existence of a right Euclidean division when R is a field: given $a, b \in R[X; \sigma, \delta]$ with $b \neq 0$, one can compute unique $q, r \in R[X; \sigma, \delta]$ such that $a = qb + r$ and either $r = 0$ or $\deg(r) < \deg(b)$. This implies the existence of a greatest common right divisor and of a least common left multiple of a and b (see [12] for additional properties and the corresponding algorithms).

Definition 3 *Let (R, σ, δ) be a σ–differential ring and M be a left R–module. A map $\theta : M \to M$ is called* R–pseudo–linear (with respect to σ and δ) *if*

$$\theta(u + v) = \theta u + \theta v \quad \textit{and} \quad \theta(au) = \sigma a\ \theta u + \delta a\ u$$

for any $a \in R$ and $u, v \in M$. We write $End_{R,\sigma,\delta}(M)$ for the set of all the R–pseudo–linear maps of M.

Note that $\mathrm{End}_{R,1_R,0_R}(M) = \mathrm{End}_R(M)$, that $\delta \in \mathrm{End}_{R,\sigma,\delta}(M)$ and that every R–pseudo–linear map is linear with respect to $\mathrm{Const}_{\sigma,\delta}(R)$. The following lemma generalizes the multiplicative change of variable formula of linear ordinary differential equations.

Lemma 4 *Let (R, σ, δ) be a σ–differential ring, M be a left R–module and θ be an R–pseudo–linear map of M. Let $a \in R$ be such that $\sigma a = ab$ and $\delta a = ac$ for some $b, c \in R$. Then, $\theta^n(au) = a(b\theta + c)^n u$ for any $u \in M$ and any integer $n \geq 0$.*

Proof. The result is trivial for $n = 0$, so assume that it holds for a given $n \geq 0$. Then,

$$\begin{aligned}\theta^{n+1}(au) &= \theta\theta^n(au) = \theta(a(b\theta + c)^n u) = \sigma(a)\theta((b\theta + c)^n u) + \delta(a)(b\theta + c)^n u \\ &= ab\theta((b\theta + c)^n u) + ac(b\theta + c)^n u = a(b\theta + c)(b\theta + c)^n u = a(b\theta + c)^{n+1} u\,.\end{aligned}$$

□

Pseudo–linear maps of a commutative ring viewed as a module over itself must be of a very special form, which implies that linear equations involving a pseudo–linear map of a field are equivalent either to differential or generalized difference equations.

Lemma 5 *Let (R, σ, δ) be a σ–differential ring. Then,*

(i) $\{\gamma\sigma + \delta$ *for* $\gamma \in Z(R)\} \subseteq End_{R,\sigma,\delta}(R)$.

(ii) *If R is commutative, then $End_{R,\sigma,\delta}(R) = \{\gamma\sigma + \delta$ for $\gamma \in R\}$.*

(iii) *If R is a field and $\sigma \neq 1_R$, then for any $a_0, \ldots, a_n \in R$ and any θ in $End_{R,\sigma,\delta}(R)$, there are $b_0, \ldots, b_n$ in R such that*

$$\sum_{i=0}^{n} a_i \theta^i = \sum_{i=0}^{n} b_i \sigma^i\,.$$

Proof. (i) Let $\theta = \gamma\sigma + \delta$ for $\gamma \in Z(R)$ and let $a, b \in R$. We have $\theta(a + b) = \theta a + \theta b$ since σ and δ are additive. Furthermore,

$$\begin{aligned}\theta(ab) &= \gamma\sigma(ab) + \delta(ab) = \gamma\sigma a\ \sigma b + \sigma a\ \delta b + \delta a\ b \\ &= \sigma(a)(\gamma\sigma b + \delta b) + \delta a\ b = \sigma a\ \theta b + \delta a\ b\end{aligned}$$

so $\theta \in \mathrm{End}_{R,\sigma,\delta}(R)$.
(ii) If R is commutative, then $Z(R) = R$. Let $\theta \in \mathrm{End}_{R,\sigma,\delta}(R)$. Then, $\theta(a) = \theta(a \times 1) = \sigma a\ \theta 1 + \delta a$ for any $a \in R$, so $\theta = \gamma\sigma + \delta$ where $\gamma = \theta 1 \in R$. The reverse inclusion is proven in (i).
(iii) If R is a field and $\sigma \neq 1_R$, then $\delta = \alpha(\sigma - 1_R)$ for some $\alpha \in R$ by Lemma 2. By (ii), this implies that $\theta = (\gamma + \alpha)\sigma - \alpha$ where $\gamma = \theta 1$, and expanding $\sum_{i=0}^{n} a_i((\gamma + \alpha)X - \alpha)^i$ in the skew–polynomial ring $R[X; \sigma, \delta]$ produces $b_0, \ldots, b_n$. □

Definition 4 *An ideal I of (R, σ, δ) is called a* σ–differential ideal *if it is closed under σ and δ.*

It follows from Lemma 5 that a σ–differential ideal of a commutative ring R is closed under any $\theta \in \mathrm{End}_{R,\sigma,\delta}(R)$. The following lemma provides the basis of modular algorithms for solving linear functional equations.

Lemma 6 *Let (R, σ, δ) be a σ–differential ring, I be a σ–differential ideal of R, and $\pi : R \to R/I$ be the canonical projection. Then, σ and δ induce respectively an endomorphism σ^* of R/I and a σ^*–derivation δ^* of R/I such that $\sigma^* \circ \pi = \pi \circ \sigma$ and $\delta^* \circ \pi = \pi \circ \delta$. Furthermore, if R is commutative, then any $\theta \in End_{R,\sigma,\delta}(R)$ induces $\theta^* \in End_{R/I,\sigma^*,\delta^*}(R/I)$ satisfying $\theta^* \circ \pi = \pi \circ \theta$.*

Proof. Define σ^* and δ^* as follows: for $x \in R/I$, let $a \in R$ be such that $\pi(a) = x$, and set $\sigma^* x = \pi(\sigma a)$ and $\delta^* x = \pi(\delta a)$. Suppose that $\pi(a) = \pi(b) = x$ for $a, b \in R$. Then, $a - b \in I$, so $\sigma(a - b) \in I$ and $\delta(a - b) \in I$ since I is a σ–differential ideal. This implies that $\pi(\sigma a) = \pi(\sigma b)$ and $\pi(\delta a) = \pi(\delta b)$, hence that σ^* and δ^* are well-defined. We have $\sigma^* \circ \pi = \pi \circ \sigma$ and $\delta^* \circ \pi = \pi \circ \delta$ by definition. Let $x, y \in R/I$ and let $a, b \in R$ be such that $\pi(a) = x$ and $\pi(b) = y$. Then, $\pi(a + b) = x + y$ and $\pi(ab) = xy$, so

$$\sigma^*(x + y) = \pi(\sigma(a + b)) = \pi(\sigma a + \sigma b) = \pi(\sigma a) + \pi(\sigma b) = \sigma^* a + \sigma^* b$$

and similarly, $\sigma^*(xy) = \sigma^* x \, \sigma^* y$ and $\delta^*(x + y) = \delta^*(x) + \delta^*(y)$. Finally,

$$\delta^*(xy) = \pi(\delta(ab)) = \pi(\sigma a \, \delta b + \delta a \, b) = \pi(\sigma a)\pi(\delta b) + \pi(\delta a)\pi(b) = \sigma^* x \, \delta^* y + \delta^* x \, y$$

so δ^* is a σ^*–derivation of R/I. Suppose that R is commutative and let $\theta \in \mathrm{End}_{R,\sigma,\delta}(R)$, and $\theta^* = \pi(\theta 1)\sigma^* + \delta^*$. Since R/I is commutative, Lemma 5 implies that $\theta^* \in \mathrm{End}_{R/I,\sigma^*,\delta^*}(R/I)$ and that

$$\theta^*(\pi a) = \pi(\theta 1)\sigma^*(\pi a) + \delta^*(\pi a) = \pi(\theta(1)\sigma a + \delta a) = \pi(\theta a)$$

for any $a \in R$. □

2 σ–differential extensions

We generalize in this section the notions of differential extensions and monomial extensions to σ–differential fields.

Definition 5 *Let (R, σ, δ) and (R', σ', δ') be σ–differential rings. We say that (R', σ', δ') is a* σ–differential extension *of (R, σ, δ) if R is a subring of R' and $\sigma' a = \sigma a$ and $\delta' a = \delta a$ for any $a \in R$.*

It follows immediately that $\mathrm{Const}_{\sigma,\delta}(R) \subseteq \mathrm{Const}_{\sigma',\delta'}(R')$. In addition, if R' (and therefore R) is commutative, then Lemma 5 implies that for any $\theta \in \mathrm{End}_{R,\sigma,\delta}(R)$, $\theta' = \theta(1)\sigma' + \delta'$ is the unique extension of θ to an element of $\mathrm{End}_{R',\sigma',\delta'}(R')$. We thus consider $\mathrm{End}_{R,\sigma,\delta}(R)$ to be a subset of $\mathrm{End}_{R',\sigma',\delta'}(R')$ whenever R' is commutative. When there is no confusion, we simply say that R' is a σ–differential extension of R and use the same notations for the endomorphisms, associated derivations and pseudo–linear maps on R and R'. We first show that injective σ–derivations on an integral domain can be extended uniquely to its quotient field.

Proposition 2 *Let (R,σ,δ) be a σ–differential ring with R an integral domain and σ injective. Let F the quotient field of R. Then there exists a unique endomorphism τ of F and a unique τ–derivation Δ of F such that (F,τ,Δ) is a σ–differential extension of (R,σ,δ).*

Proof. Define $\tau : F \to F$ and $\Delta : F \to F$ as follows: for any $x \in F$, write $x = a/b$ where $a, b \in R$, $b \neq 0$, and let $\tau x = \sigma a/\sigma b$ and $\Delta x = (b\delta a - a\delta b)/(b\sigma b)$. Note that $\sigma b \neq 0$ since σ is injective. Suppose that $x = a/b = c/d$ for $a, b, c, d \in R$. Then, $ad = bc$, so $\sigma a\ \sigma d = \sigma b\ \sigma c$, which implies that $\sigma a/\sigma b = \sigma c/\sigma d$, hence that τ is well–defined. In addition,

$$\begin{aligned}\frac{b\delta a - a\delta b}{b\sigma b} - \frac{d\delta c - c\delta d}{d\sigma d} &= \frac{d\sigma d\ b\delta a - d\sigma d\ a\delta b - b\sigma b\ d\delta c + b\sigma b\ c\delta d}{bd\sigma b\ \sigma d} \\ &= \frac{bd\delta(da - bc) + bc\delta(bd) - ad\delta(db)}{bd\sigma b\ \sigma d} \\ &= \frac{bd\delta(da - bc) + (bc - ad)\delta(bd)}{bd\sigma b\ \sigma d} = 0\end{aligned}$$

which implies that Δ is well–defined. Writing $a \in R$ as $a/1$, we get

$$\tau a = \frac{\sigma a}{\sigma 1} = \sigma a \quad \text{and} \quad \Delta a = \frac{\delta a - a\delta 1}{1\sigma 1} = \delta a\,.$$

Let now $x, y \in F$ and write $x = a/b, y = c/d$ where $a, b, c, d \in R$. We have

$$\tau(xy) = \tau\frac{ac}{bd} = \frac{\sigma a}{\sigma b}\frac{\sigma c}{\sigma d} = \tau x\ \tau y$$

and

$$\tau(x+y) = \tau\frac{ad+bc}{bd} = \frac{\sigma a\ \sigma d + \sigma b\ \sigma c}{\sigma b\ \sigma d} = \frac{\sigma a}{\sigma b} + \frac{\sigma c}{\sigma d} = \tau x + \tau y\,,$$

so τ is an endomorphism of F. Finally,

$$\begin{aligned}\Delta(x+y) &= \Delta\frac{ad+bc}{bd} = \frac{bd\delta(da+bc) - (ad+bc)\delta(bd)}{bd\sigma b\ \sigma d} \\ &= \frac{bd\delta(da+bc) - ad\delta(db) - bc\delta(bd)}{bd\sigma b\ \sigma d} = \frac{d\sigma d\ (b\delta a - a\delta b) + b\sigma b\ (d\delta c - c\delta d)}{bd\sigma b\ \sigma d} \\ &= \frac{b\delta a - a\delta b}{b\sigma b} + \frac{d\delta c - c\delta d}{d\sigma d} = \Delta x + \Delta y\end{aligned}$$

and

$$\begin{aligned}\Delta(xy) = \Delta\frac{ac}{bd} &= \frac{bd\delta(ac) - ac\delta(db) + bc(\delta(da) - \delta(ad))}{bd\sigma b\ \sigma d} \\ &= \frac{\sigma a\ b(d\delta c - c\delta d) + c\sigma d\ (b\delta a - a\delta b)}{bd\sigma b\ \sigma d} = \tau x\ \Delta y + y\Delta x\,,\end{aligned}$$

which implies that Δ is a τ–derivation of F, hence that (F,τ,Δ) is a σ–differential extension of (R,σ,δ).

Let now (F, τ_1, Δ_1) and (F, τ_2, Δ_2) be σ–differential extensions of (R, σ, δ) and let $x \in F$. Write $x = a/b$ where $a, b \in R$ and $b \neq 0$. Since τ_1 and τ_2 are endomorphisms that agree with σ on R, we have

$$\tau_1 x = \frac{\tau_1 a}{\tau_1 b} = \frac{\sigma a}{\sigma b} = \frac{\tau_2 a}{\tau_2 b} = \tau_2 x$$

so $\tau_1 = \tau_2$. Using (2) and that Δ_1 and Δ_2 agree with δ on R, we have

$$\Delta_1 x = \frac{b\Delta_1 a - a\Delta_1 b}{b\tau_1 b} = \frac{b\delta a - a\delta b}{b\sigma b} = \frac{b\Delta_2 a - a\Delta_2 b}{b\tau_2 b} = \Delta_2 x\,,$$

which shows that (F, τ, Δ) as defined above is the unique σ–differential extension of (R, σ, δ) to F. □

As in the differential case, we define monomial extensions to be simple transcendental extensions for which $k[t]$ is closed under σ and any pseudo–linear map, in particular δ.

Definition 6 *Let (k, σ, δ) be a σ–differential field and K be a field and a σ–differential extension of k. We say that $t \in K$ is a* monomial over k *(with respect to σ and δ) if t is transcendental over k, $\sigma t \in k[t]$ and $\delta t \in k[t]$.*

Lemma 7 *Let (k, σ, δ) be a σ–differential field and t be a monomial over k. Then, $k[t]$ and $k(t)$ are closed under σ, δ and any $\theta \in End_{k,\sigma,\delta}(k)$.*

Proof. Let $p = \sum_i a_i t^i \in k[t]$. Then, $\sigma p = \sum_i \sigma(a_i)\sigma(t)^i \in k[t]$ since $\sigma t \in k[t]$. In addition, using (4) we get

$$\delta p = \sum_i \delta(a_i t^i) = \sum_i \left(\delta(a_i)t^i + \sigma(a_i)\delta(t) \sum_{j=0}^{i-1} t^j \sigma(t)^{i-1-j} \right) \in k[t]$$

since $\sigma t \in k[t]$ and $\delta t \in k[t]$. Therefore $k[t]$ is closed under σ and δ. Since $\sigma(p/q) = \sigma(p)/\sigma(q)$ for $p, q \in k[t]$, $k(t)$ is closed under σ, and (2) implies that $k(t)$ is closed under δ. Let now $\theta \in \mathrm{End}_{k,\sigma,\delta}(k)$. Since $k(t)$ is a σ–differential extension of k, $\theta(1)\sigma + \delta \in \mathrm{End}_{k(t),\sigma,\delta}(k(t))$ is the unique extension of θ to $k(t)$. Since $k[t]$ is closed under σ and δ and $\theta 1 \in k$, $k[t]$ is also closed under θ. □

Definition 7 *Let (k, σ, δ) be a σ–differential field and t be a monomial over k. We say that $p \in k[t]$ is* special with respect to σ and δ *if $p \mid \sigma p$ and $p \mid \delta p$, and write*

$$\mathcal{S}_{k[t]:k} = \{p \in k[t] \text{ such that } p \text{ is special}\}\,.$$

When the monomial extension is clear from the context, we omit the subscripts and simply write $\mathcal{S}$. When $\sigma = 1_{k(t)}$, p is special if and only if $p \mid \delta p$, so the above definition generalizes the one given in the differential case in [10]. Special polynomials generate σ–differential ideals, so there is an induced endomorphism and its associated derivation on the quotient rings. More importantly, those maps turn out to make $k[t]/(p)$ a σ–differential extension of k.

Lemma 8 *(p) is a σ–differential ideal of $k[t]$ for any $p \in \mathcal{S}_{k[t]:k}$. Furthermore, if $p \notin k$, then $(k[t]/(p), \sigma^*, \delta^*)$ is a σ–differential extension of (k, σ, δ), where σ^* and δ^* are as in Lemma 6.*

Proof. Let $p \in \mathcal{S}_{k[t]:k}$. Then, $p \mid \sigma p$ and $p \mid \delta p$ by definition, so (p) is a σ–differential ideal of $k[t]$. Suppose that $p \notin k$. Then, $k[t]/(p)$ is an extension of k, and by Lemma 6, $\sigma^* \circ \pi = \pi \circ \sigma$ and $\delta^* \circ \pi = \pi \circ \delta$. Therefore, $\sigma^* a = \sigma^* \pi(a) = \pi(\sigma a) = \sigma a$ and $\delta^* a = \delta^* \pi(a) = \pi(\delta a) = \delta a$ for any $a \in k$, which implies that $(k[t]/(p), \sigma^*, \delta^*)$ is a σ–differential extension of (k, σ, δ). □

As in the differential case, new constants in extensions are closely linked to nontrivial special polynomials.

Lemma 9 *Let (k, σ, δ) be a σ–differential field and t be a monomial over k. If $c \in Const_{\sigma,\delta}(k(t))$, then both the numerator and denominator of c are special.*

Proof. Write $c = a/b$ where $a, b \in k[t]$, $b \neq 0$ and $\gcd(a, b) = 1$. Then, $a/b = c = \sigma c = \sigma(a)/\sigma(b)$, which implies that $a\sigma b = b\sigma a$, hence that $a \mid \sigma a$ and $b \mid \sigma b$. Similarly,

$$0 = \delta c = \frac{b\delta a - a\delta b}{b\sigma b},$$

which implies that $b\delta a = a\delta b$, hence that $a \mid \delta a$ and $b \mid \delta b$. □

It turns out that $\mathcal{S}_{k[t]:k}$ is the monoid of polynomials that divide their image under any pseudo–linear map.

Lemma 10 *Let (k, σ, δ) be a σ–differential field and t be a monomial over k. Then,*

(i) *$\mathcal{S}_{k[t]:k} = \{p \in k[t]$ such that $p \mid \theta p$ for every $\theta \in End_{k,\sigma,\delta}(k)\}$.*

(ii) *$\mathcal{S}_{k[t]:k}$ is a multiplicative monoid containing k.*

Proof. (i) From Lemma 5, we have $\mathrm{End}_{k,\sigma,\delta}(k) = \{\gamma\sigma + \delta$ for $\gamma \in k\}$. Let $p \in \mathcal{S}_{k[t]:k}$. Then $p \mid \sigma p$ and $p \mid \delta p$, so $p \mid \gamma\sigma p + \delta p$ for any $\gamma \in k$. Conversely, suppose that $p \mid \theta p$ for any $\theta \in \mathrm{End}_{k,\sigma,\delta}(k)$. Taking $\gamma = 0$ implies that $p \mid \delta p$. Taking then $\gamma = 1$ implies that $p \mid \sigma p + \delta p$, hence that $p \mid \sigma p$, and therefore that $p \in \mathcal{S}_{k[t]:k}$.
(ii) $\mathcal{S}_{k[t]:k}$ obviously contains k, hence 1. Let $p, q \in \mathcal{S}_{k[t]:k}$ and let $a, b, c, d \in k[t]$ be such that $\sigma p = ap$, $\sigma q = bq$, $\delta p = cp$ and $\delta q = dq$. We then have $\sigma(pq) = apbq$ and $\delta(pq) = apdq + cpq$, which implies that $pq \in \mathcal{S}_{k[t]:k}$. □

Unlike in the differential case, factors of special polynomials are not necessarily special, as the following example illustrates.

Example 1 *Let t be an indeterminate over $\mathbb{Q}$, σ the the automorphism of $\mathbb{Q}(t)$ over $\mathbb{Q}$ that maps t to $1 - t$, and δ be the zero map on $\mathbb{Q}(t)$. Then, t is a monomial over $\mathbb{Q}$ and $t^2 - t$ is special, but its factors t and $t - 1$ are not special.*

The factors of special polynomials will be characterized for a restricted class of monomial extensions in Section 4.

3 Polynomial solutions

We consider in this section the problem of finding solutions $y \in k[t]$ and $c_1, \ldots, c_m \in \mathrm{Const}_{\sigma,\delta}(k)$ of equations of the form

$$a_n\theta^n y + a_{n-1}\theta^{n-1}y + \ldots + a_1\theta y + a_0 y = c_1 g_1 + \ldots + c_m g_m \tag{7}$$

where t is a monomial over k, $a_0, \ldots, a_n \in k[t]$, $g_1, \ldots, g_m \in k(t)$ and $\theta \in \mathrm{End}_{k,\sigma,\delta}(k)$. Because $k[t]$ is closed under θ, any denominator of the right hand side can be eliminated, yielding linear constraints for the c_i's.

Lemma 11 *Let (k, σ, δ) be a σ–differential field, t be a monomial over k, $\theta \in End_{k,\sigma,\delta}(k)$, $y, a_0, \ldots, a_n \in k[t]$, $g_1, \ldots, g_m \in k(t)$ and $c_1, \ldots, c_m \in Const_{\sigma,\delta}(k)$ be such that (7) is satisfied. Let d_i be the denominator of g_i for $1 \leq i \leq m$, $d = lcm(d_1, \ldots, d_m)$, and $q_1, \ldots, q_m, r_1, \ldots, r_m \in k[t]$ be such that $dg_i = dq_i + r_i$ and either $r_i = 0$ or $\deg(r_i) < \deg(d)$ for each i. Then,*

$$\sum_{i=1}^{m} c_i r_i = 0 \tag{8}$$

and

$$a_n\theta^n y + a_{n-1}\theta^{n-1}y + \ldots + a_1\theta y + a_0 y = c_1 q_1 + \ldots + c_m q_m\,. \tag{9}$$

Proof. Since $g_i = q_i + r_i/d$ for each i and $k[t]$ is closed under θ by Lemma 7, we obtain from (7) that

$$\frac{\sum_{i=1}^{m} c_i r_i}{d} = \sum_{i=0}^{n} a_i\theta^i y - \sum_{i-1}^{m} c_i q_i \in k[t]\,.$$

Since $\deg\left(\sum_{i=1}^{m} c_i r_i\right) < \deg(d)$, it follows that $\sum_{i=1}^{m} c_i r_i = 0$, which implies (9). □

Equating the coefficients of the powers of t on both sides of (8) yields a homogeneous system of linear equations for the c_i's, *i.e.* a matrix M with coefficients in k such that $M(c_1, c_2, \ldots, c_m)^T = 0$. As in the differential case, such constraints are equivalent to linear constraints with constant coefficients, as shown by the following proposition.

Proposition 3 *Let (k, σ, δ) be a σ–differential field, A be a matrix with entries in k, and $\mathbf{u}$ be a vector with entries in k. Then, using only elementary row operations on A and $\mathbf{u}$, we can either prove that $Ax = \mathbf{u}$ has no constant solution, or we can compute a matrix B and a vector $\mathbf{v}$, both with entries in $Const_{\sigma,\delta}(k)$, such that the constant solutions of $Ax = \mathbf{u}$ are exactly all the solutions of $Bx = \mathbf{v}$. Furthermore, if $\mathbf{u} = 0$, then $\mathbf{v} = 0$.*

Proof. Let $C = \mathrm{Const}_{\sigma,\delta}(k)$, and write R_i for the i^{th} row of A, and a_{ij} for the j^{th} entry of R_i. By applying the usual Gaussian elimination, we can compute an equivalent system in row-reduced echelon form, so suppose that A is in that form. If all the entries of A are in C, let $B = A$ and $\mathbf{v} = \mathbf{u}$. Otherwise, let j be the smallest index such that the j^{th} column

of A has a non-constant entry, and let i be such that $a_{ij} \notin C$. Then, either $\sigma a_{ij} \neq a_{ij}$ or $\delta a_{ij} \neq 0$ (or both) so we add the row

$$R_{m+1} = \begin{cases} \frac{\sigma R_i - R_i}{\sigma a_{ij} - a_{ij}} & = & \left(\frac{\sigma a_{i1} - a_{i1}}{\sigma a_{ij} - a_{ij}}, \ldots, \frac{\sigma a_{ir} - a_{ir}}{\sigma a_{ij} - a_{ij}}\right) & \text{if } \sigma a_{ij} \neq a_{ij} \\ \frac{\delta R_i}{\delta a_{ij}} & = & \left(\frac{\delta a_{i1}}{\delta a_{ij}}, \ldots, \frac{\delta a_{ir}}{\delta a_{ij}}\right) & \text{if } \sigma a_{ij} = a_{ij} \end{cases}$$

at the bottom of A, and the entry

$$u_{m+1} = \begin{cases} \frac{\sigma u_i - u_i}{\sigma a_{ij} - a_{ij}} & \text{if } \sigma a_{ij} \neq a_{ij} \\ \frac{\delta u_i}{\delta a_{ij}} & \text{if } \sigma a_{ij} = a_{ij} \end{cases}$$

at the bottom of $\mathbf{u}$. By our choice of j, the first nonzero entry in R_{m+1} is a 1 in column j, so we add adequate multiples of R_{m+1} to all the other rows to ensure that $a_{ij} = 0$ for $i = 1 \ldots m$. We now have a new matrix $\tilde{A}$ and a new vector $\tilde{\mathbf{u}}$ with one more row, but with only constant entries in columns 1 through j. Repeating this, we eventually obtain a matrix B and a vector $\mathbf{v}$ such that all the entries of B are in C. By construction, $\mathbf{v} = 0$ if $\mathbf{u} = 0$. Since we have only performed elementary row operations to A and added extra equations that were consequences of the existing equations, any solution of $Bx = \mathbf{v}$ must be a solution of $Ax = \mathbf{u}$.

Case 1, $\mathbf{v}$ *has a nonconstant entry:* let x be a constant solution of $Ax = \mathbf{u}$. Then all the entries of Bx are constant, in contradiction with $Bx = \mathbf{v}$. Hence $Ax = \mathbf{u}$ has no constant solution if $\mathbf{v}$ has a nonconstant entry.

Case 2, all the entries of $\mathbf{v}$ *are in* C*:* we have already seen that any solution of $Bx = \mathbf{v}$ must be a solution of $Ax = \mathbf{u}$. Conversely, let x be a constant solution of $Ax = \mathbf{u}$. In order for x to satisfy $Bx = \mathbf{v}$, it only has to satisfy $R_{m+1}x = u_{m+1}$, where R_{m+1} is the extra row added in the reduction step. If $\sigma a_{ij} \neq a_{ij}$ we have

$$\begin{aligned} R_{m+1}x &= \frac{(\sigma a_{i1} - a_{i1})x_1 + \ldots + (\sigma a_{ir} - a_{ir})x_r}{\sigma a_{ij} - a_{ij}} \\ &= \frac{\sigma(a_{i1}x_1 + \ldots + a_{ir}x_r)}{\sigma a_{ij} - a_{ij}} - \frac{a_{i1}x_1 + \ldots + a_{ir}x_r}{\sigma a_{ij} - a_{ij}} \\ &= \frac{\sigma(R_i x)}{\sigma a_{ij} - a_{ij}} - \frac{R_i x}{\sigma a_{ij} - a_{ij}} = \frac{\sigma u_i}{\sigma a_{ij} - a_{ij}} - \frac{u_i}{\sigma a_{ij} - a_{ij}} = u_{m+1} \end{aligned}$$

while if $\sigma a_{ij} = a_{ij}$ we have

$$R_{m+1}x = \frac{(\delta a_{i1})x_1 + \ldots + (\delta a_{ir})x_r}{\delta a_{ij}} = \frac{\delta(a_{i1}x_1 + \ldots + a_{ir}x_r)}{\delta a_{ij}} = \frac{\delta(R_i x)}{\delta a_{ij}} = \frac{\delta u_i}{\delta a_{ij}} = u_{m+1}$$

so x is a solution of $Bx = \mathbf{v}$. □

In the presence of a nontrivial special in the extension, we can reduce the problem of finding solutions of bounded degree of (7) to solving similar equations in an algebraic

extension of k. Given a σ–differential ring R and $\theta \in \mathrm{End}_{R,\sigma,\delta}(R)$, we say that we can *effectively solve parameterized linear θ–equations over R* if given $a_0, \ldots, a_n, g_1, \ldots, g_m \in R$, we can effectively find $h_1, \ldots, h_r \in R$ and a matrix M with $r+m$ columns and entries in $\mathrm{Const}_{\sigma,\delta}(R)$ such that $y \in R$ and $c_1, \ldots, c_m \in \mathrm{Const}_{\sigma,\delta}(R)$ satisfy (7) if and only if $y = \sum_{k=1}^{r} y_k h_k$ where $y_1, \ldots, y_r \in \mathrm{Const}_{\sigma,\delta}(R)$ and $M(y_1, \ldots, y_r, c_1, \ldots, c_m)^T = 0$. Note that this implies in particular being able to find all the solutions in R of homogeneous and inhomogeneous θ–equations with coefficients in R. In the statement of the following theorem, we use the facts that for $p \in \mathcal{S} \setminus k$, $k[t]/(p)$ is a σ–differential extension of k (Lemma 8) and $\theta \in \mathrm{End}_{k,\sigma,\delta}(k)$ induces $\theta^* \in \mathrm{End}_{k[t]/(p),\sigma^*,\delta^*}(k[t]/(p))$ (Lemma 6).

Theorem 1 *Let (k, σ, δ) be a σ–differential field, t be a monomial over k, $p \in \mathcal{S} \setminus k$ and $\theta \in End_{k,\sigma,\delta}(k)$. Suppose that $Const_{\sigma,\delta}(k(t)) = Const_{\sigma^*,\delta^*}(k[t]/(p)) = Const_{\sigma,\delta}(k)$. If we can solve parameterized linear θ–equations over k and parameterized linear θ^*–equations over $k[t]/(p)$, then for any $N \in \mathbb{Z}$ and any $a_0, \ldots, a_n, g_1, \ldots, g_m \in k(t)$, we can find $h_1, \ldots, h_r \in k[t]$ and a matrix M with $r+m$ columns and entries in $Const_{\sigma,\delta}(k)$ such that $y \in k[t]$ and $c_1, \ldots, c_m \in Const_{\sigma,\delta}(k)$ satisfy (7) with $\deg(y) \le N$ if and only if $y = \sum_{k=1}^{r} y_k h_k$ where $y_1, \ldots, y_r \in Const_{\sigma,\delta}(k)$ and $M(y_1, \ldots, y_r, c_1, \ldots, c_m)^T = 0$.*

Proof. Let $C = \mathrm{Const}_{\sigma,\delta}(k(t)) = \mathrm{Const}_{\sigma^*,\delta^*}(k[t]/(p)) = \mathrm{Const}_{\sigma,\delta}(k)$. Multiplying if necessary the equation by a common denominator for the a_i's and dividing by their content, we can assume that $a_0, \ldots, a_n \in k[t]$ and that $\gcd(a_0, \ldots, a_n) = 1$. Using Lemma 11, we get a set of linear constraints with coefficients in k for $c_1, \ldots, c_m$, and $q_1, \ldots, q_m \in k[t]$ such that we are reduced to finding solutions $y \in k[t]$ of degree at most N of (9). By Proposition 3 the linear constraints for the c_i's can be reduced to have their coefficients in C.
If $N < 0$, then $y = 0$ together with $\sum_{i=1}^{m} c_i q_i = 0$, which can be reduced to linear constraints with coefficients in C, is the only solution.
If $N = 0$, then $y \in k$, so write $a_i = \sum_{j=0}^{d} a_{ij} t^j$ and $q_i = \sum_{j=0}^{d} q_{ij} t^j$ where d is large enough and $a_{ij}, q_{ij} \in k$. Our equation becomes

$$\sum_{j=0}^{d} t^j \sum_{i=0}^{n} a_{ij} \theta^i y = \sum_{j=0}^{d} t^j \sum_{i=1}^{m} c_i q_{ij}$$

so equating the coefficients of equal powers of t on both sides we get either new linear constraints for the c_j's (when the left–hand side is 0) or parameterized linear θ–equations over k for y, which we can solve by our hypothesis. As earlier, the linear contraints can be reduced to linear constraints with coefficients in C.
If $N > 0$, let $R = k[t]/(p)$ and $\pi : k[t] \to R$ be the reduction modulo p. Write $y = y_0 + pz$ where $y_0, z \in k[t]$ and $\deg(y_0) < \deg(p)$, $a_i = \sum_{j=0}^{d} a_{ij} p^j$ and $q_i = \sum_{j=0}^{d} q_{ij} p^j$ where d is large enough and $a_{ij}, q_{ij} \in k[t]$ satisfy $\deg(a_{ij}) < \deg(p)$ and $\deg(q_{ij}) < \deg(p)$. Our equation becomes

$$\sum_{j=0}^{d} p^j \sum_{i=0}^{n} a_{ij} \theta^i y = \sum_{j=0}^{d} p^j \sum_{i=1}^{m} c_i q_{ij} \,.$$

By Lemma 8, R is a σ–differential extension of k, and by Lemma 6, θ induces a pseudo–linear map θ^* on R, which satisfies $\theta^* \circ \pi = \pi \circ \theta$. Applying π to the above equation and noting that $\pi(y) = y_0$, $\pi(a_i) = a_{i0}$ and $\pi(q_i) = q_{i0}$, we get

$$\sum_{i=0}^{n} a_{i0}\theta^{*\,i} y_0 = \sum_{i=1}^{m} c_i q_{i0}\,.$$

Since $\gcd(a_0, \ldots, a_n) = 1$, there is at least one index i for which $a_{i0} \neq 0$, so the above is a nonzero linear θ^*–equation with coefficients in R. Using the induction hypothesis we compute $h_1, \ldots, h_r \in R$ and a matrix A with entries in C such that for any solution $y_0 \in R$, we must have $y_0 = \sum_{s=1}^{r} e_s h_s$ and $A(e_1, \ldots, e_r, c_1, \ldots, c_m)^T = 0$. Considering $h_1, \ldots, h_r$ as elements of $k[t]$, let $u_1, \ldots, u_r, v_1, \ldots, v_r \in k[t]$ be such that $\deg(u_s) < \deg(p)$ for each s and

$$\sum_{i=0}^{n} a_{i0}\theta^i h_s = u_s + p v_s \qquad \text{for } 1 \leq s \leq r\,.$$

Summing over s we get

$$\sum_{s=1}^{r} e_s u_s = \sum_{s=1}^{r} e_s \sum_{i=0}^{n} a_{i0}\theta^i h_s - p\sum_{s=1}^{r} e_s v_s = \sum_{i=0}^{n} a_{i0}\theta^i \left(\sum_{s=1}^{r} e_s h_s\right) - p\sum_{s=1}^{r} e_s v_s$$

and applying π yields

$$\sum_{s=1}^{r} e_s u_s = \sum_{i=0}^{n} a_{i0}\theta^{*\,i} \left(\sum_{s=1}^{r} e_s h_s\right) = \sum_{i=1}^{m} c_i q_{i0}$$

whenever $A(e_1, \ldots, e_r, c_1, \ldots, c_m)^T = 0$. Replacing y by $\sum_{s=1}^{r} e_s h_s + pz$ in our equation and using Lemma 4 as well as the above equalities, we get

$$\begin{aligned}
\sum_{i=1}^{m} c_i q_i &= \sum_{i=0}^{n} a_i\theta^i \left(pz + \sum_{s=1}^{r} e_s h_s\right) = \sum_{i=0}^{n} a_i\theta^i(pz) + \sum_{i=0}^{n} a_i\theta^i \left(\sum_{s=1}^{r} e_s h_s\right) \\
&= p\sum_{i=0}^{n} a_i \left(\frac{\sigma p}{p}\theta + \frac{\delta p}{p}\right)^i z + p\sum_{i=0}^{n} \frac{a_i - a_{i0}}{p}\theta^i \left(\sum_{s=1}^{r} e_s h_s\right) + \sum_{i=0}^{n} a_{i0}\theta^i \left(\sum_{s=1}^{r} e_s h_s\right) \\
&= p\sum_{i=0}^{n} a_i \left(\frac{\sigma p}{p}\theta + \frac{\delta p}{p}\right)^i z + p\sum_{s=1}^{r} e_s \sum_{i=0}^{n} \frac{a_i - a_{i0}}{p}\theta^i h_s + \sum_{i=1}^{m} c_i q_{i0} + p\sum_{s=1}^{r} e_s v_s\,.
\end{aligned}$$

Therefore,

$$\sum_{i=0}^{n} a_i \left(\frac{\sigma p}{p}\theta + \frac{\delta p}{p}\right)^i z = \sum_{i=1}^{m} c_i \frac{q_i - q_{i0}}{p} - \sum_{s=1}^{r} e_s \left(v_s + \sum_{i=0}^{n} \frac{a_i - a_{i0}}{p}\theta^i h_s\right).$$

The above is a linear parameterized θ–equation with coefficients and right–hand side in $k[t]$, so we solve it with the bound $N - \deg(p)$ for $\deg(z)$ using the same method. This process eventually terminates since the degree bound is reduced at each step. □

Note that the above algorithm can be used without a bound on the degree of the polynomial solutions in order to compute formal power series solutions in $k[[p]]$. That modified algorithm does not terminate, but a basis of the polynomial solutions is produced along the way, as illustrated by the following example.

Example 2 *Consider the recurrence equation*

$$y(n+2) - (n! + n)y(n+1) + n(n! - 1)y(n) = 0 \tag{10}$$

whose coefficients are in $(k(t), \sigma, \delta)$ *where* $k = \mathbb{Q}(n)$, t *is an indeterminate over* k, $\delta = 0$, *and* σ *is the automorphism of* $k(t)$ *over* $\mathbb{Q}$ *that maps* n *to* $n+1$ *and* t *to* $(n+1)t$, *i.e.* $t = n!$. *As will be proven later (Corollaries 1 and 2),* n *is a monomial over* $\mathbb{Q}$, t *is a monomial over* k, $Const_{\sigma,\delta}(k(t)) = Const_{\sigma,\delta}(k) = \mathbb{Q}$, *and* $p = t$ *is the only monic irreducible special of* $k[t]$. *Applying the algorithm of Theorem 1 to look for solutions* $y \in k[t]$ *of (10), we write* $y = Y + tz$ *and specialize at* $t = 0$ *to get*

$$Y_{n+2} - nY_{n+1} - nY_n = 0\,.$$

Using the algorithm of [3], we find that the above equation has no nonzero solution in $\mathbb{Q}(n)$, *implying that* $Y = 0$. *Replacing* y *by* tz *in (10) and using Lemma 4 we get the new equation*

$$(n+2)(n+1)z_{n+2} - (t+n)(n+1)z_{n+1} + n(t-1)z_n = 0\,. \tag{11}$$

Writing $z = Z + tu$ *and specializing at* $t = 0$, *we get*

$$(n+2)(n+1)Z_{n+2} - n(n+1)Z_{n+1} - nZ_n = 0\,,$$

whose solution space in $\mathbb{Q}(n)$ *is* $Z = c_1 h_1$ *where* $h_1 = 1/n$ *and* c_1 *is an arbitrary constant. Replacing* z *by* $c_1 h_1 + tu$ *in (11) and using Lemma 4 we get the new equation*

$$(n+2)^2(n+1)^2 u_{n+2} - (t+n)(n+1)^2 u_{n+1} + n(t-1)u_n = 0\,,$$

which is homogeneous, implying that $u = 0$ *is a solution, therefore that*

$$y = \frac{t}{n} = \frac{n!}{n} = (n-1)!$$

is a solution of (10) in $\mathbb{Q}(n)[n!]$.

Finally, we remark that in the case of q–difference equations with polynomial coefficients, our algorithm provides an efficient alternative to either the undetermined coefficient method or the method proposed in [1], since each specialization yields a single linear algebraic equation for the next term of the series (we use the bounding method of [1] followed by repeated specialization at $x = 0$).

Example 3 *[1] Consider the q–difference equation*

$$\begin{aligned}(1-q^{10}-(q-q^{10})x)y(q^2x) &- (1-q^{20}-(q^2-q^{20})x)y(qx)\\ &+ q^{10}(1-q^{10}-(q^2-q^{11})x)y(x)=0 \qquad (12)\end{aligned}$$

whose coefficients are in $(k(x),\sigma,\delta)$ where $k=\mathbb{Q}(q)$, q is transcendental over $\mathbb{Q}$, x is an indeterminate over k, $\delta=0$, and σ is the automorphism of $k(x)$ over k that maps x to qx. As will be proven later (Corollary 2), x is a monomial over k, $Const_{\sigma,\delta}(k(x))=k$ and $p=x$ is the only monic irreducible special of $k[x]$. Applying the algorithm of Theorem 1 to look for solutions $y\in k[x]$ of (12), we write $y=Y+xz$ and specialize at $x=0$ to get

$$(1-q^{10})Y-(1-q^{20})Y+q^{10}(1-q^{10})Y=0\,.$$

The above is the linear algebraic equation $0Y=0$, whose solution space in k is $Y=e_1h_1$ where $h_1=1$ and e_1 is an arbitrary constant. Replacing y by e_1h_1+xz in (12) and using Lemma 4 we get the new equation

$$\begin{aligned}q^2(1-q^{10}-(q-q^{10})x)z(q^2x) &- q(1-q^{20}-(q^2-q^{20})x)z(qx)\\ +q^{10}(1-q^{10}-(q^2-q^{11})x)z(x) &= -e_1(q^{21}-q^{20}-q^{12}+q^{10}+q^2-q)\,. \qquad (13)\end{aligned}$$

Writing $z=Z+xu$ and specializing at $x=0$, we get

$$(q^{21}-q^{20}-q^{12}+q^{10}+q^2-q)Z=-e_1(q^{21}-q^{20}-q^{12}+q^{10}+q^2-q)$$

whose solution space in k is $Z=e_2h_2$ together with the linear constraint $e_1+e_2=0$, where $h_2=1$ and e_2 is a constant. Replacing z by e_2h_2+xu in (13) and using Lemma 4 we get the new equation

$$\begin{aligned}q^4(1-q^{10}-(q-q^{10})x)u(q^2x) &- q^2(1-q^{20}-(q^2-q^{20})x)u(qx)\\ &+ q^{10}(1-q^{10}-(q^2-q^{11})x)u(x)=0\,,\end{aligned}$$

which is homogeneous, implying that $u=0$ is a solution, therefore that $y=1-x$ is a solution of (12) in $\mathbb{Q}(q)[x]$. Continuing this process would eventually yield the second polynomial solution $1-x+x^{10}$, as found in [1].

4 Unimonomial extensions

In order to study rational rather than polynomial solutions of equations, we now turn our attention to the analogues of the Liouvillian extensions of differential fields. Those extensions were introduced and studied in [17, 16] in the context of symbolic summation and are a special type of monomial extensions.

Definition 8 *Let (k,σ,δ) be a σ–differential field and K be a field and a σ–differential extension of k. We say that $t\in K$ is a* unimonomial over k *(with respect to σ and δ) if σ is an automorphism of k and t is a monomial over k such that* $\deg_t(\sigma t)=1$.

It is easily checked that σ is an automorphism of $k(t)$ when t is a unimonomial. Note that in the ordinary differential case ($\sigma = 1_K$) monomials and unimonomials are the same notions. As a consequence of Lemma 3, we can describe the factors of the special polynomials in unimonomial extensions.

Lemma 12 *Let (k, σ, δ) be a σ–differential field and t be a unimonomial over k. Then, $\mathcal{S} \subseteq k[t]^\sigma$ and equality holds if $\delta = 0$. Furthermore, if $q \in \mathcal{S}$ then any factor of q is in $k[t]^{\sigma^*}$.*

Proof. Since t is a unimonomial over k, $\deg_t(\sigma p) = \deg_t(p)$ for any $p \in k[t]$, which implies that $\mathcal{S} \subseteq k[t]^\sigma$. If $\delta = 0$, then any p dividing σp is special, so $\mathcal{S} = k[t]^\sigma$. The last statement follows from Lemma 3 and the fact that $\mathcal{S} \subseteq k[t]^\sigma \subseteq k[t]^{\sigma^*}$. □

Example 4 *Going back to Example 1 we had $t^2 - t \in \mathcal{S}$ while t and $t - 1$ were not special. However, $\sigma^2 t = t$ and $\sigma^2(1 - t) = 1 - t$.*

The following example shows that when $\delta \neq 0$, the semi–invariants of σ are not always special, even when t is a unimonomial and $\sigma \neq 1$.

Example 5 *Let t be an indeterminate over $\mathbb{Q}$, σ the the automorphism of $\mathbb{Q}(t)$ over $\mathbb{Q}$ that maps t to $2-t$, and δ be the inner derivation $(1-t)^{-1}(\sigma-1)$. We have $\delta t = (\sigma(t)-t)/(1-t) = 2$, so t is a unimonomial over $\mathbb{Q}$. The polynomial $t - 1$ is a semi–invariant of σ, but is not special, since $\delta(t - 1) = 2$.*

For a σ–differential field k and $a, b \in k$ we introduce the notation

$$V_{a,b}(k) = \{w \in k \text{ such that } \sigma w = aw + b\}.$$

We also say that an element a of a σ–differential field k is a *σ–radical over k* if $\sigma z = a^n z$ for some $z \in k^*$ and an integer $n > 0$. Note that $V_{a,b}(k)$ has at most one element when a is not a σ–radical over k: if $\sigma w = aw + b$ and $\sigma z = az + b$ for $w, z \in k$, then $\sigma(w - z) = a(w - z)$, which implies that $w = z$. Karr [16] used $V_{a,b}(k)$ to characterize the semi–invariants of σ in extensions where $\sigma t = at + b$ and either $V_{a,b}(k)$ is empty or a is not a σ–radical over k.

Theorem 2 *[16, Theorem 2.1] Let (k, σ, δ) be a σ–differential field with σ an automorphism of k, K be a field and a σ–differential extension of k, and $t \in K$ be such that $\sigma t = at + b$ for $a, b \in k$. The following are equivalent:*

(i) $k[t]^\sigma \neq k$.

(ii) $V_{a,b}(k)$ *is not empty.*

(iii) *There exists $g \in k(t) \setminus k$ such that $\sigma g/g \in k$.*

Note that $w \in V_{a,b}(k)$ implies that $\sigma u = au$ where $u = t - w$. This means that a unimonomial extension with a nontrivial semi–invariant can always be written as $k(u)$ where $\sigma u/u \in k$.

Example 6 *Going back to Example 1 we had* $t^2 - t \in \mathcal{S}$, *so* $\sigma w = 1 - w$ *for some* $w \in \mathbb{Q}$. *This equation is indeed solved by* $w = 1/2$, *and* $k(t) = k(t - 1/2)$ *with* $t - 1/2 \in \mathcal{S}$. *Note that even though* $V_{-1,1}(\mathbb{Q}) = \{1/2\}$ *is a singleton,* -1 *is a* σ*–radical over* $\mathbb{Q}$ *since* $\sigma c = (-1)^2 c$ *for any* $c \in \mathbb{Q}$.

Lemma 13 *[16] Let* (k, σ, δ) *be a* σ*–differential field with* σ *an automorphism of* k, K *be a field and a* σ*–differential extension of* k, *and* $t \in K^*$ *be algebraic over* k *such that* $\sigma t = at + b$ *for* $a, b \in k$. *Then,* $V_{a,b}(k)$ *is not empty. Furthermore, if* $b = 0$ *then either* $a = 0$ *or* a *is a* σ*–radical over* k.

Proof. If $a = 0$ then $\sigma^{-1} b \in V_{a,b}(k)$, so suppose that $a \neq 0$. We then follow the proof outlined in Theorem 2.3 of [16]: let $g = X^m + \sum_{i=0}^{m-1} a_i X^i$ be the minimal polynomial for t over k where $m > 0$. Then,

$$0 = \sigma(g(t)) = (at + b)^m + \sum_{i=0}^{m-1} \sigma(a_i)(at + b)^i \,,$$

which implies that $h = a^m g$ where $h = (aX + b)^m + \sum_{i=0}^{m-1} \sigma(a_i)(aX + b)^i$. Equating the coefficients of X^{m-1} on both sides yields

$$a^{m-1}\sigma(a_{m-1}) + m a^{m-1} b = a^m a_{m-1} \,,$$

which implies that $\sigma a_{m-1} = a a_{m-1} - mb$, hence that $w = -a_{m-1}/m \in V_{a,b}(k)$. If $b = 0$ and $a \neq 0$, we follow the proof of Theorem 2.2 of [16]: since $t \neq 0$, $a_j \neq 0$ for some $j < m$. Equating the coefficients of X^j on both sides yields $a^j \sigma a_j = a^m a_j$, which implies that $\sigma z = a^n z$ where $n = m - j > 0$ and $z = a_j \in k^*$. □

As a consequence, adjoining a solution of a first–order equation that does not have any solution in k, creates a transcendental extension with no new constant or special.

Corollary 1 *[16] Let* (k, σ, δ) *be a* σ*–differential field with* σ *an automorphism of* k, K *be a field and a* σ*–differential extension of* k, *and* $t \in K$ *be such that* $\sigma t = at + b$ *for* $a, b \in k$. *If* $V_{a,b}(k)$ *is empty, then* t *is a unimonomial over* k, $Const_{\sigma,\delta}(k(t)) = Const_{\sigma,\delta}(k)$ *and* $\mathcal{S} = k[t]^\sigma = k[t]^{\sigma^*} = k$.

Proof. If $V_{a,b}(k)$ is empty, then t is transcendental over k by Lemma 13. Furthermore, $\sigma g / g \notin k$ for any $g \in k(t) \setminus k$ by Theorem 2, which implies that $k[t]^\sigma = k$, hence that $\mathcal{S} = k$ by Lemma 12. Lemma 9 then implies that $\mathrm{Const}_{\sigma,\delta}(k(t)) = \mathrm{Const}_{\sigma,\delta}(k)$. Let $p \in k[t]^{\sigma^n}$ for some $n > 0$. Then, $q = \prod_{i=0}^{n-1} \sigma^i p \in k[t]^\sigma$ by Lemma 3, so $q \in k$, which implies that $p \in k$, hence that $k[t]^{\sigma^*} = k$. □

Adjoining a solution of a first–order equation whose leading coefficient is not a σ–radical over k creates a transcendental extension with no new constant and known semi–invariants.

Corollary 2 *[16] Let (k,σ,δ) be a σ–differential field with σ an automorphism of k, K be a field and a σ–differential extension of k, $t \in K$ be such that $\sigma t = at + b$ for $a, b \in k$. If a is not a σ–radical over k, then t is a unimonomial over k, $Const_{\sigma,\delta}(k(t)) = Const_{\sigma,\delta}(k)$ and*

$$k[t]^{\sigma^*} = k[t]^{\sigma} = k \cup \{c(t-w)^m \text{ such that } c \in k, w \in V_{a,b}(k), m \in \mathbb{Z}, m \geq 0\}. \qquad (14)$$

Proof. If $V_{a,b}(k)$ is empty, then the results follow by Corollary 1, so suppose that $V_{a,b}(k)$ is not empty, and let $w \in V_{a,b}(k)$ and $u = t - w$. Then, $\sigma u = au$, and, since a is not a σ–radical over k, Lemma 13 implies that u, and hence t, is transcendental over k. We now follow the proof of Theorem 2.2 of [16]: let $p \in k[t]^{\sigma} \setminus k$, $c \in k^*$ be its leading coefficient and $q = c^{-1}p$. We have $\sigma q = \sigma(c^{-1})\sigma p$, which implies that $q \in k[t]^{\sigma}$. Write $q = u^m + \sum_{i=0}^{m-1} a_i u^i$ where $a_i \in k$. Then,

$$\sigma q = a^m u^m + \sum_{i=0}^{m-1} \sigma(a_i) a^i u^i = a^m q,$$

which implies that $\sigma(a_i) = a^{m-i}a_i$ for $0 \leq i < m$. Since a is not a σ–radical over k, we must have $a_i = 0$ for $0 \leq i < m$, and $p = cu^m = c(t-w)^m$. Conversely, $\sigma(c(t-w)^m) = \sigma(c)a^m(t-w)^m$, which proves that $k[t]^{\sigma}$ is given by (14). Let $p \in k[t]^{\sigma^n}$ for some $n > 0$. Then, $q = \prod_{i=0}^{n-1} \sigma^i p \in k[t]^{\sigma}$ by Lemma 3, so $q = c(t-w)^m$ for $c \in k$ and $m \geq 0$. Since $p \mid q$, $t - w$ is the only possible monic irreducible factor of p, which implies that $k[t]^{\sigma^*} = k[t]^{\sigma}$. Let $d \in \mathrm{Const}_{\sigma,\delta}(k(t))$ and write $d = p/q$ where $p, q \in k[t]$ are such that $\gcd(p,q) = 1$. Then, $p, q \in \mathcal{S}$ by Lemma 9, so $p, q \in k[t]^{\sigma}$ by Lemma 12, which implies that $d = c(t-w)^m$ for $c \in k$ and $m \in \mathbb{Z}$. If $c = 0$, then $d \in \mathrm{Const}_{\sigma,\delta}(k)$, so suppose that $c \neq 0$. Since $1/d$ is also a constant, we can assume that $m \leq 0$. We have, $\sigma d = \sigma(c)a^m(t-w)^m$, which implies that $\sigma c = a^{-m}c$. Since a is not a σ–radical over k, we must have $m = 0$, so $\mathrm{Const}_{\sigma,\delta}(k(t)) = \mathrm{Const}_{\sigma,\delta}(k)$. □

Note that $V_{a,b}(k) = V_{1,0}(k) = k$ when σ is the identity on $k(t)$, so Corollaries 1 and 2 do not give information for differential extensions. It is possible to have σ be the identity on k however. When a is a σ–radical over k, it is possible for $V_{a,b}(k)$ to be a singleton and for the right–hand side of (14) to form only a proper subset of the semi–invariants, as Example 6 illustrates, since $V_{-1,1}(\mathbb{Q}) = \{1/2\}$ but $t^2 - t \in \mathcal{S}$.

We can now generalize the ordinary differential definitions of primitives and exponentials and obtain necessary conditions on them for the specials to be fully characterized.

Definition 9 *Let (k,σ,δ) be a σ–differential field and K be a σ–differential extension of k. We say that $t \in K$ is a* primitive over k *if $\sigma t - t \in k$ and $\delta t \in k$. We say that $t \in K^*$ is an* hyperexponential over k *if $\sigma t/t \in k$ and $\delta t/t \in k$.*

If σ is the identity over K, then the above definitions simply coincide with the corresponding ones for differential fields [10]. Otherwise, they define their discrete analogues: if $\sigma t - t = \eta \in k$, then for integers $n \leq m$,

$$\sigma^{m+1}t - \sigma^n t = \sum_{i=n}^{m} \left(\sigma^{i+1}t - \sigma^i t\right) = \sum_{i=n}^{m} \sigma^i(\sigma t - t) = \sum_{i=n}^{m} \sigma^i \eta$$

so t is an antidifference of η. Similarly, if $\sigma t/t = \eta \in k$, then for integers $n \leq m$,

$$\frac{\sigma^{m+1}t}{\sigma^n t} = \prod_{i=n}^{m} \frac{\sigma^{i+1}t}{\sigma^i t} = \prod_{i=n}^{m} \sigma^i\left(\frac{\sigma t}{t}\right) = \prod_{i=n}^{m} \sigma^i \eta$$

so t is an hypergeometric term over k. Note that $\sigma t/t \in k \setminus \{1\}$ does not necessarily imply that t is special, as the following example points out.

Example 7 *Let t be an indeterminate over $\mathbb{Q}$, σ the the automorphism of $\mathbb{Q}(t)$ over $\mathbb{Q}$ that maps t to $2t$ and δ be the inner derivation $t^{-1}(\sigma - 1)$. We have $\delta t = 1$, so t is a unimonomial over $\mathbb{Q}$ but t is not special.*

The necessary condition for a primitive to be transcendental with no new specials or constants is simply that it is not redundant.

Theorem 3 *Let (k, σ, δ) be a σ–differential field where σ is an automorphism of k, K be a field and a σ–differential extension of k and $t \in K$ be a primitive over k. If k contains no element w satisfying $\sigma w - w = \sigma t - t$ and $\delta w = \delta t$, then t is a unimonomial over k, $Const_{\sigma,\delta}(k(t)) = Const_{\sigma,\delta}(k)$ and $\mathcal{S} = k$. Furthermore, if σ is not the identity on K, then $k[t]^\sigma = k[t]^{\sigma^*} = k$.*

Proof. Suppose first that σ is the identity on K. Then δ is an ordinary derivation on K and $\sigma w - w = \sigma t - t = 0$ for any $w \in k$. Therefore, k contains no element w satisfying $\delta w = \delta t$ and the result follows by Theorem 5.1.1 of [10]. Suppose now that σ is not the identity on K and let $\eta = \sigma t - t \in k$. Since $\delta = u(\sigma - 1)$ for some $u \in K$ by Lemma 2, we have $\delta w = \delta t = u\eta$ for any $w \in V_{1,\eta}(k)$. Therefore $V_{1,\eta}(k)$ must be empty and the results follow by Corollary 1. □

The condition for hyperexponentials is somewhat stronger, as it requires that the extension cannot be replaced by constants and algebraic extensions. We say that an element a of a σ–differential field (k, σ, δ) is a *logarithmic derivative of a k–radical* if $na = \delta w/w$ for some integer $n \neq 0$ and $w \in k^*$.

Theorem 4 *Let (k, σ, δ) be a σ–differential field where σ is an automorphism of k, K be a field and a σ–differential extension of k and $t \in K^*$ be an hyperexponential over k. If either (i) $\sigma t/t$ is not a σ–radical over k, or (ii) $\sigma t = t$ and $\delta t/t$ is not a logarithmic derivative of a k–radical, then t is a unimonomial over k, $Const_{\sigma,\delta}(k(t)) = Const_{\sigma,\delta}(k)$ and $\mathcal{S} = \{ct^m$ such that $c \in k, m \in \mathbb{Z}, m \geq 0\}$. Furthermore, if $\sigma t \neq t$, then $k[t]^\sigma = k[t]^{\sigma^*} = \mathcal{S}$.*

Proof. Suppose first that $\eta = \sigma t/t \in k$ is not a σ–radical over k. Then, $V_{\eta,0}(k) = \{0\}$ since it has at most one element, and Corollary 2 implies that t is a unimonomial over k, $\mathrm{Const}_{\sigma,\delta}(k(t)) = \mathrm{Const}_{\sigma,\delta}(k)$ and $k[t]^\sigma = \{ct^m, c \in k, m \in \mathbb{Z}, m \geq 0\}$. We have $t \in \mathcal{S}$ since $\delta t/t \in k$, so $ct^m \in \mathcal{S}$ for $c \in k$ and $m \geq 0$ by Lemma 10. Since $S \subseteq k[t]^\sigma$ by Lemma 12, it follows that $\mathcal{S} = \{ct^m$ such that $c \in k, m \in \mathbb{Z}, m \geq 0\}$.
Suppose now that $\sigma t = t$ and that $\delta t/t$ is not a logarithmic derivative of a k–radical. This implies in particular that $\delta t \neq 0$, hence that δ is not a multiple of $\sigma - 1$. Lemma 2 then

implies that σ is the identity on K, so δ is an ordinary derivation on K and and the result follows by Theorem 5.1.2 of [10].
If in addition, $\sigma t \neq t$, then $\sigma t/t$ is not a σ–radical over k, and Corollary 2 implies that $k[t]^\sigma = k[t]^{\sigma^*} = \mathcal{S}$. □

The restriction $\sigma t = t$ in hypothesis (ii) of the above theorem cannot be removed, as the following example illustrates.

Example 8 *Let $K = \mathbb{Q}(\sqrt{2})$, σ be the automorphism of K over $\mathbb{Q}$ that maps $\sqrt{2}$ to $-\sqrt{2}$ and δ be the inner derivation $\sigma - 1$. Then, $\sqrt{2}$ is hyperexponential over $\mathbb{Q}$ and $\delta\sqrt{2}/\sqrt{2} = -2$ is not the logarithmic derivative of a $\mathbb{Q}$–radical, but K is algebraic over $\mathbb{Q}$.*

5 The dispersion

The key quantity needed to compute denominators of rational solutions of linear difference equations is the dispersion, which was first introduced with respect to the shift in [2] for computing rational sums. We generalize its definition and properties in this section to more general coefficients and morphisms.

Definition 10 *Let $R[X]$ be a polynomial ring over a unique factorization domain R and ϕ be any mapping from $R[X]$ into itself. For any $p, q \in R[X] \setminus \{0\}$, we define the* spread of p and q with respect to ϕ *to be*

$$Spr_\phi(p,q) = \{m \in \mathbb{Z}, m \geq 0 \text{ such that } \deg(\gcd(p, \phi^m q)) > 0\}$$

and the dispersion of p and q with respect to ϕ *to be*

$$Dis_\phi(p,q) = \begin{cases} -1 & \text{if } Spr_\phi(p,q) \text{ is empty,} \\ \max(Spr_\phi(p,q)) & \text{if } Spr_\phi(p,q) \text{ is finite and nonempty,} \\ +\infty & \text{if } Spr_\phi(p,q) \text{ is infinite.} \end{cases}$$

When ϕ is an endomorphism of $R[X]$, we also define the dispersion of a fraction $f \in R(X)^*$ to be

$$Dis_\phi(f) = \max(Dis_\phi(p), Dis_\phi(p,q), Dis_\phi(q,p), Dis_\phi(q))$$

where $p, q \in R[X] \setminus \{0\}$ are such that $f = p/q$, q is primitive and $\gcd(p,q) = 1$.

We also write $\mathrm{Spr}_\phi(p)$ and $\mathrm{Dis}_\phi(p)$ for $\mathrm{Spr}_\phi(p,p)$ and $\mathrm{Dis}_\phi(p,p)$ respectively. Note that $0 \in \mathrm{Spr}_\phi(p)$ for $p \in R[X] \setminus R$, which implies that $\mathrm{Dis}_\phi(p) \geq 0$. The dispersion of p can be infinite however, for example $\mathrm{Dis}_{1_{R[X]}}(p) = +\infty$ for $p \in R[X] \setminus R$ where $1_{R[X]}$ is the identity map on $R[X]$. We also use the following equivalent characterisation of the spread: $m \in \mathrm{Spr}_\phi(p,q)$ if and only if $\mathrm{res}(p, \phi^m q) = 0$, where res denotes the resultant in $R[X]$.

Example 9 *Let $R[X]$ be a polynomial ring over a unique factorization domain R, and $q \in R[X] \setminus \{0\}$. For any irreducible $p \in R[X]$, we have $p^{n+1} \mid q$ if and only if $p^n \mid \gcd(q, dq/dX)$. It follows that $p^{n+1} \mid q$ if and only if $p \mid \gcd(q, d^n q/dX^n)$, hence that*

$$Spr_{d/dX}(q) = \{n \geq 0 \text{ such that } p^{n+1} \mid q \text{ for some irreducible } p \in R[X]\}$$

and therefore

$$Dis_{d/dX}(q) = \begin{cases} -1 & \text{if } q \in R, \\ \max\{n > 0 \text{ such that } p^n \mid q \text{ for some } p \in R[X] \setminus R\} - 1 & \text{if } q \notin R. \end{cases}$$

Lemma 14 *Let $R[X]$ be a polynomial ring over a unique factorization domain R and ϕ be an injective endomorphism of $R[X]$. Then, for any $a \in R \setminus \{0\}$ and any $p, q \in R[X] \setminus \{0\}$, $Spr_\phi(p,q) = Spr_{a\phi}(p,q)$ and $Dis_\phi(p,q) = Dis_{a\phi}(p,q)$.*

Proof. Since ϕ is an endomorphism, we have

$$(a\phi)^m q = \left(\prod_{i=0}^{m-1} \phi^i a\right) \phi^m q$$

for any integer $m \geq 0$. Therefore,

$$\operatorname{res}(p, (a\phi)^m q) = \operatorname{res}\left(p, \left(\prod_{i=0}^{m-1} \phi^i a\right) \phi^m q\right) = \left(\prod_{i=0}^{m-1} \phi^i a\right)^{\deg(p)} \operatorname{res}(p, \phi^m q)\,.$$

Since ϕ is injective and $a \neq 0$, $\phi^i a \neq 0$ for $i \geq 0$, which implies that $\operatorname{res}(p, (a\phi)^m q) = 0$ if and only if $\operatorname{res}(p, \phi^m q) = 0$, hence that $\operatorname{Spr}_\phi(p,q) = \operatorname{Spr}_{a\phi}(p,q)$, and the equality of the dispersions follows. □

Dispersion computations can be reduced to squarefree polynomials, and the dispersion of a product is related to the dispersions of its components.

Lemma 15 *Let $R[X]$ be a polynomial ring over a unique factorization domain R, ϕ be an endomorphism of $R[X]$ and $p_1, \ldots, p_n, q_1, \ldots, q_m \in R[X] \setminus \{0\}$. Then,*

(i)

$$Spr_\phi(p_1^{e_1} \ldots p_n^{e_n}, q_1^{f_1} \ldots q_m^{f_m}) = \bigcup_{i=1}^{n} \bigcup_{j=1}^{m} Spr_\phi(p_i, q_j) \quad \left(= Spr_\phi(p_1 \ldots p_n, q_1 \ldots q_m) \right)$$

and

$$Dis_\phi(p_1^{e_1} \ldots p_n^{e_n}, q_1^{f_1} \ldots q_m^{f_m}) = \max_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} (Dis_\phi(p_i, q_j)) \quad \left(= Dis_\phi(p_1 \ldots p_n, q_1 \ldots q_m) \right)$$

for any integers $e_i, f_j > 0$.

(ii) *If $Spr_\phi(p_i, p_j)$ is empty for $i \neq j$, then*

$$Spr_\phi(p_1^{e_1} \ldots p_n^{e_n}) = \bigcup_{i=1}^{n} Spr_\phi(p_i) \quad \text{and} \quad Dis_\phi(p_1^{e_1} \ldots p_n^{e_n}) = \max_{1 \leq i \leq n} (Dis_\phi(p_i))$$

for any integers $e_i > 0$.

(iii) *If* $n = m$, $Spr_\phi(p_i, p_j)$, $Spr_\phi(q_i, q_j)$, $Spr_\phi(p_i, q_j)$ *and* $Spr_\phi(q_j, p_i)$ *are all empty for* $i \neq j$, *and* $\gcd(p_i, q_i) = 1$ *for all* i, *then*

$$Dis_\phi(f_1^{e_1} \ldots f_n^{e_n}) = \max_{1 \leq i \leq n} (Dis_\phi(f_i))$$

for any integers $e_i > 0$, *where* $f_i = p_i/q_i$.

Proof. (i) Let $s \in \mathrm{Spr}_\phi(p_1^{e_1} \ldots p_n^{e_n}, q_1^{f_1} \ldots q_m^{f_m})$ and $p \in R[X]$ be an irreducible common factor of $p_1^{e_1} \ldots p_n^{e_n}$ and $\phi^s(q_1^{f_1} \ldots q_m^{f_m})$, Since p is irreducible, it divides one of the p_i's, so let i_0 be such that $p \mid p_{i_0}$. Similarly, p divides one of the $\phi^s(q_j)$'s, so let j_0 be such that $p \mid \phi^s(q_{j_0})$. Then, $s \in \mathrm{Spr}_\phi(p_{i_0}, q_{j_0})$, so $\mathrm{Spr}_\phi(p_1^{e_1} \ldots p_n^{e_n}, q_1^{f_1} \ldots q_m^{f_m}) \subseteq \cup_{i=1}^n \cup_{j=1}^m \mathrm{Spr}_\phi(p_i, q_j)$. Conversely, any irreducible factor of $\gcd(p_i, \phi^s(q_j))$ divides $p_1^{e_1} \ldots p_n^{e_n}$ and $\phi^s(q_1^{f_1} \ldots q_m^{f_m})$, which proves the reverse inclusion. The statement about the dispersion then follows from the definition.
(ii) The statement follows from taking $m = n$, $q_i = p_i$ and $f_i = e_i$ in (i).
(iii) Let $a = \prod_{i=1}^n p_i^{e_i}$ and $b = \prod_{i=1}^n q_i^{e_i}$. Since an empty spread means that the arguments are coprime and since $\gcd(p_i, q_i) = 1$, it follows that $\gcd(a, b) = 1$. Furthermore, $\mathrm{Dis}_\phi(p_i, q_j) = \mathrm{Dis}_\phi(q_j, p_i) = -1$ for $i \neq j$, so using parts (i) and (ii) we get

$$\begin{aligned}
\mathrm{Dis}_\phi(f_1^{e_1} \ldots f_n^{e_n}) &= \max\{\mathrm{Dis}_\phi(a), \mathrm{Dis}_\phi(a,b), \mathrm{Dis}_\phi(b,a), \mathrm{Dis}_\phi(b)\} \\
&= \max\{\max_{1 \leq i \leq n} (\mathrm{Dis}_\phi(p_i)), \max_{1 \leq i,j \leq n} (\mathrm{Dis}_\phi(p_i, q_j)), \\
&\qquad \max_{1 \leq i,j \leq n} (\mathrm{Dis}_\phi(q_j, p_i)), \max_{1 \leq i \leq n} (\mathrm{Dis}_\phi(q_i))\} \\
&= \max_{1 \leq i \leq n} \{\mathrm{Dis}_\phi(p_i)), \mathrm{Dis}_\phi(p_i, q_i), \mathrm{Dis}_\phi(q_i, p_i), \mathrm{Dis}_\phi(q_i)\} = \max_{1 \leq i \leq n} (\mathrm{Dis}_\phi(f_i)) .
\end{aligned}$$

□

Since some of the additional properties of the dispersion hold only with respect to automorphisms of $R[X]$, we recall that any automorphism ϕ of $R[X]$ that maps R onto R preserves the degree. Indeed, since $\deg(\phi(p)) = \deg(\phi(X))\deg(p)$ for any $p \in R[X]$, taking $p = \phi^{-1}(X)$ shows that $\deg(\phi(X)) = 1$. Since $K[X]^* = K^*$ when K is a field, any automorphism of $K[X]$ maps K onto K. In order to use parts (ii) and (iii) of Lemma 15 we have to compute $\mathrm{Spr}_\phi(p_i, q_j)$ whenever $i \neq j$. In the case of automorphisms mapping R onto R, the following lemma allows the spreads for the pairs (i, j) and (j, i) to be computed together.

Lemma 16 *Let* $R[X]$ *be a polynomial ring over a unique factorization domain* R, ϕ *be an automorphism of* $R[X]$ *mapping* R *onto* R, $p, q \in R[X] \setminus \{0\}$ *and*

$$S(p, q) = \{m \in \mathbb{Z} \text{ such that } \deg(\gcd(p, \phi^m q)) > 0\} .$$

Then,

$$Spr_\phi(p, q) = \{m \text{ for } m \in S(p, q) \text{ such that } m \geq 0\} = Spr_{\phi^{-1}}(q, p)$$

and

$$Spr_\phi(q, p) = \{-m \text{ for } m \in S(p, q) \text{ such that } m \leq 0\} = Spr_{\phi^{-1}}(p, q) .$$

Furthermore for any $n \in \mathbb{Z}$, $S(\phi^n p, q) = \{m + n \text{ for } m \in S(p, q)\}$.

Proof. $\mathrm{Spr}_\phi(p,q)$ is the set of the nonnegative elements of $S(p,q)$ by definition. Let now $m \geq 0$ be in $S(p,q)$ and $g = \gcd(p, \phi^m q)$. Then, $\phi^{-m} g$ divides both $\phi^{-m} p$ and q. Since ϕ^{-1} preserves degrees, this implies that $m \in \mathrm{Spr}_{\phi^{-1}}(q,p)$. Conversely, let $m \in \mathrm{Spr}_{\phi^{-1}}(q,p)$ and $g = \gcd(q, \phi^{-m} p)$. Then, $\phi^m g$ divides both $\phi^m q$ and p, which implies that $m \in \mathrm{Spr}_\phi(p,q)$. For the second equality, $\mathrm{Spr}_{\phi^{-1}}(p,q) = \{-m \text{ for } m \in S(p,q), m \leq 0\}$ by definition. Applying the first equality, we get $\mathrm{Spr}_{\phi^{-1}}(p,q) = \mathrm{Spr}_\phi(q,p)$. For the last statement, let $n \in \mathbb{Z}$, $m \in S(p,q)$ and $g = \gcd(p, \phi^m q)$. Then, $\phi^n g$ divides both $\phi^n p$ and $\phi^{m+n} q$, which implies that $m + n \in S(\phi^n p, q)$. Conversely, let $k \in S(\phi^n p, q)$ and $g = \gcd(\phi^n p, \phi^k q)$. Then, $\phi^{-n} g$ divides both p and $\phi^{k-n} q$, which implies that $k - n \in S(p,q)$. □

We now characterize the polynomials with infinite dispersion, first in the differential case.

Theorem 5 *Let (k, D) be a differential field and t be a monomial over k. Then, for any $q \in k[t] \setminus \{0\}$, $Dis_D(q) = +\infty$ if and only if q has a nontrivial special factor.*

Proof. Suppose first that $p \mid q$ where $p \in \mathcal{S} \setminus k$. Then, $q = pr$ and $Dp = hp$ for some $r, h \in k[t]$, which implies by Lemma 4 that $D^m q = D^m(pr) = p(D+h)^m r$ hence that $p \mid D^m q$ for any integer $m > 0$, so $\mathrm{Dis}_D(q) = +\infty$. Conversely, let $q = u \prod_j q_j^{e_j}$ be the irreducible factorization of q where $u \in k^*$ the q_j's are distinct monic irreducibles and $e_j > 0$, and suppose that all the q_j's are not special. Then $\gcd(q_j, Dq_j) = 1$ for each j, which implies [10, Lemma 3.4.4] that $\gcd(q, Dq) = \prod_j q_j^{e_j - 1}$, hence that

$$\gcd(q, D^m q) = \prod_j q_j^{\max(0, e_j - m)}$$

for any integer $m \geq 0$. If $q \in k^*$, then $\mathrm{Dis}_D(q) = -1$. Otherwise, $q \notin k$ and $\mathrm{Dis}_D(q) = \max_j(e_j) - 1$. Therefore, $\mathrm{Dis}_D(q) = +\infty$ implies that q has a special irreducible factor. □

We obtain a similar result in the difference case, namely that having an infinite dispersion with respect to an automorphism mapping R onto R is equivalent to having a nontrivial semi–periodic factor.

Theorem 6 *Let $R[X]$ be a polynomial ring over a unique factorization domain R and ϕ be an endomorphism of $R[X]$.*

(i) *Let $p \in R[X] \setminus R$ and $n, m \in \mathbb{Z}$ be such that $n \geq 0$, $\phi^n p \notin R$, $m > 0$ and $p \mid \phi^m p$. Then, $Dis_\phi(h\phi^n p, qp) = +\infty$ for any $q, h \in R[X] \setminus \{0\}$.*

(ii) *Let $q, r \in R[X] \setminus \{0\}$ and suppose that ϕ is an automorphism mapping R onto R. Then, $Dis_\phi(q, r) = +\infty$ if and only if r has a nontrivial factor $p \in R[X]^{\phi^*} \setminus R$ such that $\phi^n p \mid q$ for some $n \geq 0$.*

(iii) *Let $q \in R[X] \setminus \{0\}$ and suppose that ϕ is an automorphism mapping R onto R. Then, $Dis_\phi(q) = +\infty$ if and only if q has a nontrivial factor $p \in R[X]^{\phi^*} \setminus R$.*

Proof. (i) Let $r \in R[X]$ be such that $\phi^m p = rp$. Since ϕ is a morphism, it follows that

$$\begin{aligned}\phi^{n+sm}(qp) &= \phi^{n+sm}(q)\phi^{n+sm}(p) = \phi^{n+sm}(q)\phi^n(\phi^{sm}(p)) \\ &= \phi^{n+sm}(q)\phi^n\left(\left(\prod_{i=0}^{s-1}\phi^{im}r\right)p\right) = \phi^{n+sm}(q)\left(\prod_{i=0}^{s-1}\phi^{n+im}r\right)\phi^n p\end{aligned}$$

for any $q \in R[X] \setminus \{0\}$ and any integer $s > 0$, hence that $n + sm \in \mathrm{Spr}_\phi(h\phi^n p, qp)$ for any $h \in R[X] \setminus \{0\}$ and any integer $s > 0$, so $\mathrm{Dis}_\phi(h\phi^n p, qp) = +\infty$.
(ii) Since ϕ is an automorphism mapping R onto R, it maps irreducibles to irreducibles. Suppose that $\mathrm{Dis}_\phi(q, r) = +\infty$ and let $q = u\prod_{j=1}^M q_j^{e_j}$ and $r = v\prod_{j=1}^N h_j^{f_j}$ be the irreducible factorizations of q and r, where $u, v \in R \setminus \{0\}$, $e_j > 0$ and $f_j > 0$. By Lemma 15, $S = \mathrm{Spr}_\phi(q_s, h_t)$ is infinite for some pair s, t. Since q_s and h_t are irreducible, for each $m \in S$, there exists $u_m \in R^*$ such that $\phi^m h_t = u_m q_s$. Since S is infinite, there are integers $n, m \in S$ such that $n > m \geq 0$. We have

$$\phi^n h_t = u_n q_s = u_n u_m^{-1} u_m q_s = u_n u_m^{-1}\phi^m h_t\,,$$

which implies that $h_t \in R[X]^{\phi^*}$ since it is a semi–invariant of ϕ^{n-m}. Furthermore, $\phi^n h_t = u_n q_s \mid q$. Conversely, if $p \mid r$ and $\phi^n p \mid q$ for some $p \in R[X]^{\phi^*} \setminus R$ and $n \geq 0$, then $\mathrm{Dis}_\phi(q, r) = +\infty$ by (i) since $\deg(\phi^n p) = \deg(p) > 0$.
(iii) If $\mathrm{Dis}_\phi(q) = +\infty$, then q has a nontrivial factor $p \in R[X]^{\phi^*} \setminus R$ by (ii). Conversely, if $p \mid q$ for some $p \in R[X]^{\phi^*} \setminus R$, then $\mathrm{Dis}_\phi(q) = +\infty$ by (i). □

We can now generalize the splitting factorizations of [10] to monomial extensions of σ–differential fields.

Definition 11 *Let (k, σ, δ) be a σ–differential field, t be a monomial over k and $\theta \in End_{k,\sigma,\delta}(k)$. For any $p \in k[t]$, we say that $p = p_\infty\overline{p}$ is a* splitting factorization of p with respect to θ *if $p_\infty, \overline{p} \in k[t]$, $Dis_\theta(q) = +\infty$ for every irreducible factor q of p_∞, and $Dis_\theta(q) \in \mathbb{Z}$ for every irreducible factor q of $\overline{p}$. We call $\overline{p}$ and p_∞ the* finite *and* infinite *parts of p respectively (they are defined up to multiplication by an element of k^*).*

Note that $\gcd(p_\infty, \overline{p}) = 1$ in any splitting factorization of $p \neq 0$. When $\sigma = 1$ and $\theta = \delta$, Theorem 5 implies that p_∞ is the special part of p, hence that the above factorization coincides with the one defined in [10] in the differential case. When t is a unimonomial over k and $\theta = \sigma$, Theorem 6 implies that the irreducible factors of p_∞ are exactly those factors of p that are semi–periodic w.r.t. σ. For an arbitrary $\theta \in \mathrm{End}_{k,\sigma,\delta}(k)$, splitting–factorizations can be computed if we have algorithms for computing Dis_θ and for factoring elements of $k[t]$ into irreducibles, since it is then sufficient to check which irreducible factors of p have finite dispersion. The situation is simpler in the case of primitive or hyperexponential extensions satisfying the hypotheses of Theorem 3 or 4, where we can compute splitting factorizations *a priori* in the following ways:

- If t is a primitive satisfying the hypothesis of Theorem 3, then $\mathcal{S} = k$. If σ is the identity on $k(t)$, then the infinite part of p is in k for any splitting factorization of p

with respect to δ. If σ is not the identity on $k(t)$, then $k[t]^{\sigma^*} = k$ by Theorem 3, so Theorem 6 implies that the infinite part of p is in k for any splitting factorization of p with respect to σ.

- If t is an hyperexponential satisfying the hypothesis of Theorem 4, then any special is of the form ct^m for $c \in k$. If σ is the identity on $k(t)$, then $p_\infty = ct^m$ and $\gcd(t, \overline{p}) = 1$ in any splitting factorization of p with respect to δ. If $\sigma t \neq t$, then any semi–periodic polynomial w.r.t. σ is of the form ct^m for $c \in k$ by Theorem 4, so $p_\infty = ct^m$ and $\gcd(t, \overline{p}) = 1$ in any splitting factorization of p with respect to σ.

A further refinement of the splitting factorization is useful for computing dispersions and when considering the action of a skew–polynomial on a rational function.

Definition 12 *Let $R[X]$ be a polynomial ring over a unique factorization domain R, ϕ be an endormorphism of $R[X]$ and $p \in R[X] \setminus R$. We say that $q \in R[X]$ is* p–orbital (with respect to ϕ) *if q can be written as $q = u \prod_{i=1}^{n} \phi^i(p)^{e_i}$ where $u \in R$ and $e_i \geq 0$. We say that $f \in R(X)$ is p–orbital (with respect to ϕ) if f can be written as the quotient of two p–orbital polynomials. An* orbital decomposition *of $h \in R[X]$ (resp. $h \in R(X)$) with respect to ϕ is a factorization $h = h_1 \dots h_m$ such that each $h_i \in R[X]$ (resp. $h_i \in R(X)$) is p_i-orbital for some irreducible $p_i \in R[X]$ and $Spr_\phi(p_i, p_j)$ is empty for $i \neq j$.*

For a given $p \in R[X] \setminus R$, we write $\mathcal{O}_p^\phi$ for the set of p-orbital polynomials. It can be immediately checked that it is a multiplicative monoid containing R and p, and that it is closed under ϕ. It is not in general closed under taking factors, except in the following case, which also guarantees the existence of orbital decompositions.

Lemma 17 *Let $R[X]$ be a polynomial ring over a unique factorization domain R and ϕ be an automorphism of $R[X]$ mapping R onto R.*

(i) *Any $f \in R[X]$ (resp. $R(X)$) has an orbital decomposition.*

(ii) *If $p \in R[X]$ is irreducible, then $q \in \mathcal{O}_p^\phi \setminus \{0\} \Rightarrow h \in \mathcal{O}_p^\phi$ for any factor h of q.*

(iii) *If $p \in R[X]$ is irreducible and $p \notin R[X]^{\phi^*}$, then any p–orbital $f \in R[X] \setminus \{0\}$ (resp. $R(X)^*$) has a unique decomposition $f = u \prod_{i=\alpha}^{\beta} \phi^i(p)^{e_i}$ where $u \neq 0$ is in R (resp. the quotient field of R), $e_i \in \mathbb{N}$ (resp. $\mathbb{Z}$), and $e_\alpha e_\beta \neq 0$.*

(iv) *Let $p \in R[X]$ be irreducible such that $p \notin R[X]^{\phi^*}$, and $q, q' \in \mathcal{O}_p^\phi \setminus \{0\}$ with decompositions $q = u \prod_{i=\alpha}^{\beta} \phi^i(p)^{e_i}$ and $q' = u' \prod_{j=\alpha'}^{\beta'} \phi^j(p)^{e'_j}$. Then,*

$$Spr_\phi(q, q') = \{i - j \text{ such that } i \geq j, e_i > 0 \text{ and } e'_j > 0\}.$$

Furthermore, if $e_\beta > 0$ and $e'_{\alpha'} > 0$, then $Dis_\phi(q, q') = \max(-1, \beta - \alpha')$. Let $f \in R(X)^*$ be p–orbital with decomposition $f = v \prod_{i=\alpha''}^{\beta''} \phi^i(p)^{e_i}$. If $e_{\alpha''} e_{\beta''} \neq 0$, then $Dis_\phi(f) = \beta'' - \alpha''$.

(v) *Let $p_1, p_2 \in R[X] \setminus R$, $q_1 \in \mathcal{O}^\phi_{p_1}$ and $q_2 \in \mathcal{O}^\phi_{p_2}$. If $Spr_\phi(p_1, p_2)$ and $Spr_\phi(p_2, p_1)$ are both empty, then $Spr_\phi(q_1, q_2)$ and $Spr_\phi(q_2, q_1)$ are both empty.*

Proof. (i) Let $f \in R[X]$ (resp. $R(X)$) and let $f = u\prod_{i=1}^n p_i^{e_i}$ be its irreducible factorization (where $e_i \in \mathbb{N}$, resp. $\mathbb{Z}$), and suppose that $\mathrm{Spr}_\phi(p_i, p_j)$ is not empty for some $i \neq j$. Then, $p_i \mid \phi^m p_j$ for some integer $m \geq 0$, which implies that $p_i = v\phi^m p_j$ for some $v \in R^*$ since $\phi^m p_j$ is irreducible. Replacing p_i by $v\phi^m p_j$ in the factorization and repeating this process yields an orbital decomposition of f after at most n steps.
(ii) Write $q = u\prod_{i=1}^n \phi^i(p)^{e_i}$ and let $h \in R[X]$ be any factor of q. Then, any irreducible factor of h must divide $\phi^i p$ for some i. But $\phi^i p$ is irreducible for each i, so any irreducible factor of h is of the form $u_i\phi^i p$ for $u_i \in R^*$, which implies that $h \in \mathcal{O}^\phi_p$.
(iii) Let $f = u\prod_i \phi^i(p)^{e_i} = v\prod_j \phi^j(p)^{f_j}$ and suppose that $e_{i_0} \neq f_{i_0}$ for some index i_0. Since each $\phi^i p$ is irreducible, the unicity of the prime factorization implies that $\phi^{i_0} p = w\phi^{i_1} p$ for some index i_1 and $w \in R^*$, which implies in turn that $\phi^{|i_1 - i_0|}(p)/p \in R^*$, hence that $p \in R[X]^{\phi^*}$. Therefore, $p \notin R[X]^{\phi^*}$ implies that that $e_i = f_i$ for each i, hence that the lower and upper bounds of the product are uniquely determined if they correspond to nonzero exponents. If follows that $u = v$.
(iv) Let $m \in \mathrm{Spr}_\phi(q, q')$ and h be an irreducible factor of $\gcd(q, \phi^m q')$. Since $h \mid q$, $h \in \mathcal{O}_p$ by (ii), so let $s \geq 0$ be such that $\phi^s p \mid h$. Since $\phi^s p \mid q$, $\alpha \leq s \leq \beta$ and $e_s > 0$. Since $\phi^s p \mid \phi^m q'$, $\alpha' + m \leq s \leq \beta' + m$ and $e'_{s-m} > 0$. Therefore $m = i - j$ where $i = s \geq j = s - m$, $e_i > 0$ and $e'_j > 0$. Conversely, let $m = i - j$ where $i \geq j$, $e_i > 0$ and $e'_j > 0$. Then, $\phi^i p \mid q$ and $\phi^j p \mid q'$, which implies that $\phi^{j+m} p \mid \phi^m q'$. But $j + m = i$, so $\phi^i p \mid \gcd(q, \phi^m q')$ and $m \in \mathrm{Spr}_\phi(q, q')$. The result about the $\mathrm{Dis}_\phi(q, q')$ follows immediately since $\beta \geq \alpha'$ implies that $\beta - \alpha' \in \mathrm{Spr}_\phi(q, q')$. Let now $f = u\prod_{i=\alpha''}^{\beta''} \phi^i(p)^{e_i}$ with $e_{\alpha''} e_{\beta''} \neq 0$, $I = \{i \text{ such that } e_i > 0\}$, $J = \{i \text{ such that } e_i < 0\}$, $v, w \in R \setminus \{0\}$ be such that $\gcd(v, w) = 1$ and $u = v/w$, $a = u\prod_{i \in I} \phi^i(p)^{e_i}$ and $b = v\prod_{j \in J} \phi^j(p)^{-e_j}$. Then $f = a/b$ and since $p \notin R[X]^{\sigma^*}$, $\gcd(a, b) = 1$. By what we have just proven, $\mathrm{Dis}_\phi(a) = \max(I) - \min(I)$, $\mathrm{Dis}_\phi(b) = \max(J) - \min(J)$, $\mathrm{Dis}_\phi(a, b) = \max(-1, \max(I) - \min(J))$ and $\mathrm{Dis}_\phi(b, a) = \max(-1, \max(J) - \min(I))$. It follows that

$$\begin{aligned}\mathrm{Dis}_\phi(f) &= \max(\max(I) - \min(I), \max(I) - \min(J), \max(J) - \min(I), \max(J) - \min(J)) \\ &= \max(\max(I), \max(J)) - \min(\min(I), \min(J)) = \beta'' - \alpha''\,.\end{aligned}$$

(v) Write $q_1 = u_1\prod_i \phi^i(p_1)^{e_i}$, $q_2 = u_2\prod_j \phi^j(p_2)^{f_j}$ and let $m \in \mathrm{Spr}_\phi(q_1, q_2)$ and $p \in R[X]$ be an irreducible common factor of q_1 and $\phi^m(q_2)$. Then $p \mid \phi^i p_1$ for some i and $p \mid \phi^{j+m} p_2$ for some j. If $i \leq j + m$, then $\phi^{-i} p$, which is irreducible, divides p_1 and $\phi^{j+m-i} p_2$, implying that $j + m - i \in \mathrm{Spr}_\phi(p_1, p_2)$. Similarly, $j + m \leq i$ implies that $i - (j + m) \in \mathrm{Spr}_\phi(p_2, p_1)$, so $\mathrm{Spr}_\phi(q_1, q_2)$ is empty. The proof that $\mathrm{Spr}_\phi(q_2, q_1)$ is empty follows by symmetry. □

Note that a consequence of part (v) of Lemma 17 is that the components of an orbital decomposition are two by two coprime. Orbital decompositions reduce computing spreads in polynomial rings for which an irreducible factorization algorithm is available, to computing spreads of irreducibles.

Theorem 7 *Let $R[X]$ be a polynomial ring over a unique factorization domain R and ϕ be an automorphism of $R[X]$ mapping R onto R. If there are algorithms for factoring elements of $R[X]$ into irreducibles, and for computing $Spr_\phi(p,q)$ for any irreducible $p,q \in R[X]$, then there is an algorithm for deciding whether $Spr_\phi(a,b)$ is finite for any $a,b \in R[X]$, and for computing it when it is finite.*

Proof. Since we can factor into irreducibles and compute the spreads of irreducibles, Lemma 17 shows that orbital decompositions exist and can be computed, so let $a = a_1 \dots a_n$ and $b = b_1 \dots b_m$ be orbital decompositions of a and b. By Lemma 15, $\mathrm{Spr}_\phi(a,b) = \cup_{i=1}^{n} \cup_{j=1}^{m} \mathrm{Spr}_\phi(a_i,b_j)$ so we are reduced to computing $\mathrm{Spr}_\phi(a_i,b_j)$ for all pairs i,j. Since $\mathrm{Spr}_\phi(a_i,b_j)$ is empty whenever $a_i \in R$ or $b_j \in R$, we only consider the pairs for which $a_i \notin R$ and $b_j \notin R$. Let $p_i, q_j \in R[X]$ be irreducibles such that $a_i \in \mathcal{O}_{p_i}^\phi$ and $b_j \in \mathcal{O}_{q_j}^\phi$. If $\mathrm{Spr}_\phi(p_i,q_j)$ and $\mathrm{Spr}_\phi(q_j,p_i)$ are both empty, then $\mathrm{Spr}_\phi(a_i,b_j)$ is empty by Lemma 17. If $\mathrm{Spr}_\phi(p_i,q_j)$ or $\mathrm{Spr}_\phi(q_j,p_i)$ is not empty, then either $\phi^s p_i \mid q_j$ or $\phi^s q_j \mid p_i$ for some integer $s \geq 0$, which implies that $a_i, b_j \in \mathcal{O}_p^\phi$ where p is either p_i or q_j. If $p \in R[X]^{\phi^*}$, then it follows from Theorem 6 that $\mathrm{Dis}_\phi(a_i,b_j) = +\infty$, hence that $\mathrm{Spr}_\phi(a_i,b_j)$ is infinite. Otherwise, $p \notin R[X]^{\phi^*}$ and $\mathrm{Spr}_\phi(a_i,b_j)$ is given by Lemma 17. □

Even when computing dispersions can be done by computing resultants rather than factoring (for example this is the case when ϕ is the identity on R and ϕX is either $X+1$ or qX for some q in R), the algorithm of Theorem 7 can be more efficient if irreducible factorization is fast: rather than computing the resultant of a and $\phi^m b$ for given $a,b \in R[X]$ (or of their squarefree parts as suggested in [18]), we can compute the resultants of all their pairs of irreducible factors. We can also halve the number of resultants to be computed, since Lemma 16 implies that $\mathrm{Spr}_\phi(p_i,p_j)$ and $\mathrm{Spr}_\phi(p_j,p_i)$ are both empty if and only if $S(p_i,p_j)$ is empty.

Example 10 *Let $a = 2x^7 + 19x^6 + 63x^5 + 81x^4 + 27x^3 \in \mathbb{Q}[x]$ and ϕ be the automorphism of $\mathbb{Q}[x]$ over $\mathbb{Q}$ that maps x to $x+1$. The resultant of a and $\phi^m a$ is a polynomial of degree 49, containing 16 terms with 16–digit coefficients, wich factors as*

$$4m^{19}(2m+5)^3(2m+1)^3(2m-1)^3(2m-5)^3(m-3)^9(m+3)^9\,,$$

implying that $Spr_\phi(a) = \{0,3\}$ and that $Dis_\phi(a) = 3$. The squarefree part of a is $a^* = 2x^3 + 7x^2 + 3x$, and the resultant of a^* and $\phi^m a^*$ is

$$64m^9 - 992m^7 + 3844m^5 - 900m^3 = 4m^3(m+3)(2m+1)(m-3)(2m+5)(2m-1)(2m-5)\,,$$

also implying that $Spr_\phi(a) = \{0,3\}$ and that $Dis_\phi(a) = 3$. We can instead factor a^*, obtaining $a^* = x(x+3)(2x+1)$, and then compute $res_x(x+3, \phi^m(x)) = m-3$. This shows that $Spr_\phi(x+3,x) = \{3\}$, so we replace the factorization by $a^* = (x\phi^3 x)(2x+1)$ and compute $res_x(x, \phi^m(2x+1)) = 2m+1$, which implies that the above is an orbital decomposition of a^*. Lemma 17 implies that $Spr_\phi(x\phi^3 x) = \{0,3\}$ and $Spr_\phi(2x+1) = \{0\}$, and Lemma 15 concludes that $Spr_\phi(a) = \{0,3\}$ and $Dis_\phi(a) = 3$.

But the main application of Theorem 7 is that together with an algorithm of [17], it provides a complete algorithm for computing spreads and dispersions in an important class of nested unimonomial extensions, namely the $\Pi\Sigma$–fields of [17, 16]. Indeed, given a unimonomial t over such a field F, and $p, q \in F[t]$ irreducible, $\mathrm{Spr}_\sigma(p,q)$ is connected to Karr's $\mathrm{spec}(q,p)$ by the following relation: $\mathrm{Spr}_\phi(p,q)$ is empty if and only if $\mathrm{spec}(q,p) = *$ or $\mathrm{spec}(q,p) < 0$. Otherwise, $\mathrm{spec}(q,p) \geq 0$, which implies that $\mathrm{Spr}_\sigma(p,q)$ is infinite if $q \in F[t]^{\sigma^*}$ (Theorem 6), and that $\mathrm{Spr}_\sigma(p,q) = \{\mathrm{spec}(q,p)\}$ otherwise. Theorem 9 of [17] gives an algorithm for computing spec whenever $F(t)$ is a $\Pi\Sigma$–extension of F and the orbit problem (see [15]) is solvable in $\mathrm{Const}_\sigma(F)$. This means that spreads and dispersions can be computed in such fields.

Definition 13 *Let $R[X]$ be a polynomial ring over a unique factorization domain R, ϕ be an automorphism of $R[X]$ mapping R onto R, $p \in R[X] \setminus R[X]^{\phi^*}$ be irreducible, $q \in \mathcal{O}_p^\phi$ and $q = u\prod_i \phi^i(p)^{e_i}$ be its decomposition (unique by Lemma 17). The* right–max *of q is the set*

$$B^+(q) = \{i \text{ such that } e_i > 0 \text{ and } e_i > e_j \text{ for } j > i\} = \{i_1 < i_2 < \ldots < i_s\}$$

and the left–max *of q is the set*

$$B^-(q) = \{i \text{ such that } e_i > 0 \text{ and } e_i > e_j \text{ for } j < i\}\,. = \{j_1 < j_2 < \ldots < j_r\}\,.$$

Furthermore, we say that $a \in R[X]$ is a right–bound *for q if $\phi^{i_h}(p)^{e_{i_h} - e_{i_{h+1}}} \mid a$ for $1 \leq h \leq s$ where $e_{i_{s+1}} = 0$ by convention. Similary, $b \in R[X]$ is a* left–bound *for q if $\phi^{j_h}(p)^{e_{j_h} - e_{j_{h-1}}} \mid b$ for $1 \leq h \leq r$ where $e_{j_0} = 0$. Let $d \in R[X]$ have no irreducible factor in $R[X]^{\phi^*}$. We say that d is* bounded *by (a,b) if a is a right–bound of each component of its orbital decomposition, and b is a left–bound of each such component.*

Note that if d is bounded by (a,b), then it is bounded by (qa, rb) for any $q, r \in R[X] \setminus \{0\}$. Furthermore, each component d_p of the orbital decomposition of d is bounded by (a_p, b_p), where a_p and b_p are the corresponding components in the orbital decompositions of a and b. Given $a, b \in R[X]$, we want to compute a common multiple of all the primitive polynomials $q \in R[X]$ having no factor in $R[X]^{\phi^*}$ and bounded by (a,b). We first show that those polynomials have a bounded dispersion whenever $\mathrm{Spr}_\phi(a,b)$ is finite.

Lemma 18 *Let $R[X]$ be a polynomial ring over a unique factorization domain R, ϕ be an automorphism of $R[X]$ mapping R onto R and $a, b, d \in R[X]$ be such that $d \neq 0$ and d has no irreducible factor in $R[X]^{\phi^*}$ and is bounded by (a,b). Then, $Dis_\phi(d) \leq Dis_\phi(a,b)$.*

Proof. Let $d = q_1 \ldots q_s$ be the orbital decomposition of d and $m = \mathrm{Dis}_\phi(d)$. Since $m = \max_{1 \leq i \leq s}(\mathrm{Dis}_\phi(q_i))$ by Lemma 15, let q be one of the q_i's satisfying $m = \mathrm{Dis}_\phi(q)$, let $p \in R[X] \setminus R[X]^{\phi^*}$ be the irreducible such that $q \in \mathcal{O}_p^\phi$ and write $q = u\prod_{i=\alpha}^{\beta} \phi^i(p)^{e_i}$ where $u \in R \setminus \{0\}$, $e_\alpha > 0$ and $e_\beta > 0$. Then, $\alpha = \min(B^-(q))$ and $\beta = \max(B^+(q))$, which implies that $\phi^\alpha p \mid b$ and $\phi^\beta p \mid a$, hence that $\phi^\beta \mid \gcd(a, \phi^{\beta-\alpha} b)$. Therefore, $\beta - \alpha \in \mathrm{Spr}_\phi(a,b)$. But $\mathrm{Dis}_\phi(q) = \beta - \alpha$ by Lemma 17, which proves the lemma. □

The following generalizes Theorem 2 of [4].

Lemma 19 *Let $R[X]$ be a polynomial ring over a unique factorization domain R, ϕ be an automorphism of $R[X]$ mapping R onto R, $a, b \in R[X] \setminus \{0\}$, $m \in \mathbb{Z}$ be such that $m \geq Dis_\phi(a,b)$, d be the primitive part of $\gcd(a, \phi^m b)$, $a' = a/d$, $b' = b/\phi^{-m}d$ and $c = \prod_{i=0}^{m} \phi^{-i}d$. If $q \in R[X] \setminus \{0\}$ has no irreducible factor in $R[X]^{\phi^*}$ and is bounded by (a,b), then $q' = q/\gcd(c,q)$ is bounded by a' and b'.*

Proof. If $m > \mathrm{Dis}_\phi(a,b)$, then $c = d = 1$, which implies that $a' = a$, $b' = b$ and $q' = q$, hence that q' is bounded by a' and b', so assume from now on that $m = \mathrm{Dis}_\phi(a,b)$. Suppose first that $a, b, q \in \mathcal{O}_p^\phi$ for some irreducible $p \in R[X] \setminus R[X]^{\phi^*}$, and write $a = u \prod_{i=\alpha}^{\beta} \phi^i(p)^{a_i}$ and $b = v \prod_{i=\gamma}^{\delta} \phi^i(p)^{b_i}$ where $a_\alpha > 0$, $a_\beta > 0$, $b_\gamma > 0$ and $b_\delta > 0$. Since $m = \mathrm{Dis}_\phi(a,b) \geq 0$, we must have $\gamma \leq \beta$ and $m = \beta - \gamma$. Therefore, $d = \phi^\beta(p)^\mu$ where $\mu = \min(a_\beta, b_\gamma) > 0$, and $c = \prod_{i=\gamma}^{\beta} \phi^i(p)^\mu$. Since $q \in \mathcal{O}_p^\phi$ is bounded by (a,b), we can write $q = w \prod_{i=\gamma}^{\beta} \phi^i(p)^{e_i}$ where $e_i \geq 0$ for each i (we can have $e_\gamma = 0$ and/or $e_\beta = 0$). Therefore, $q' = w \prod_{i=\gamma}^{\beta} \phi^i(p)^{f_i}$ where $f_i = \max(e_i - \mu, 0)$, which implies that $e_i \leq f_i + \mu$ for each i. Let $i \in B^+(q')$. Then, $f_i > 0$, which implies that $e_i = f_i + \mu$, and $f_i > f_j$ for $j > i$, which implies that $e_i > f_j + \mu \geq e_j$ for $j > i$, hence that $i \in B^+(q)$. In a similar way, $B^-(q') \subseteq B^-(q)$. Let now $i \in B^+(q)$. If $e_i \leq \mu$, then $f_i = 0$ and $i \notin B^+(q')$. If $e_i > \mu$, then $f_i = e_i - \mu > 0$. Let $j > i$. If $f_j = 0$, then $f_i > f_j$. Otherwise, $f_j = e_j - \mu < e_i - \mu = f_i$, so $i \in B^+(q')$. Therefore, if $B^+(q) = \{i_1 < i_2 < \ldots < i_s\}$, then $B^+(q') = \{i_1 < \ldots < i_{s'}\}$ where $i_{s'}$ is the last index whose corresponding exponent is greater than μ. Similarly, if $B^-(q) = \{j_1 < j_2 < \ldots < j_r\}$, then $B^-(q') = \{j_{r'} < \ldots < j_r\}$ where $j_{r'}$ is the first index whose corresponding exponent is greater than μ. Let $i_h \in B^+(q')$ for $1 \leq h < s'$. Then, $\phi^{i_h}(p)^{e_{i_h} - e_{i_{h+1}}} \mid a$. Since $i_h < i_{h+1} \leq \beta$, $\phi^{i_h}(p)$ does not divide d, so $\phi^{i_h}(p)^{e_{i_h} - e_{i_{h+1}}} \mid a'$. In addition,

$$f_{i_h} - f_{i_{h+1}} = (e_{i_h} - \mu) - (e_{i_{h+1}} - \mu) = e_{i_h} - e_{i_{h+1}} ,$$

so $\phi^{i_h}(p)^{f_{i_h} - e_{i_f+1}} \mid a'$. We have $\phi^{i_{s'}}(p)^{e_{i_{s'}} - e_{i_{s'}+1}} \mid a$ and $e_{i_{s'+1}} \leq \mu$, which implies that $f_{i_{s'+1}} = 0$, hence that $f_{i_{s'}} - f_{i_{s'}+1} = e_{i_{s'}} - \mu \leq e_{i_{s'}} - e_{i_{s'}+1}$. If $i_{s'} < \beta$, then $\phi^{i_{s'}}(p)$ does not divide d, so $\phi^{i_{s'}}(p)^{e_{i_{s'}} - e_{i_{s'}+1}} \mid a'$, which implies that $\phi^{i_{s'}}(p)^{f_{i_{s'}} - f_{i_{s'}+1}} \mid a'$. If $i_{s'} = \beta$, then $e_{i_{s'+1}} = 0$, which implies that $\phi^{i_{s'}}(p)^{e_{i_{s'}}} \mid a$, hence that $\phi^{i_{s'}}(p)^{e_{i_{s'}} - \mu} \mid a'$, so $\phi^{i_{s'}}(p)^{f_{i_{s'}} - f_{i_{s'}+1}} \mid a'$, and a' is a right–bound for q'. A similar argument shows that b' is a left–bound for q', hence that q' is bounded by (a', b').
Suppose now that $a, b, q \in R[X]$, where q has no irreducible factor in $R[X]^{\phi^*}$ and write the orbital decompositions of a, b and q as $a = \prod_{p \in \mathcal{P}} a_p$, $b = \prod_{p \in \mathcal{P}} b_p$ and $q = \prod_{p \in \mathcal{P}} q_p$ where each p is irreducible, $\mathrm{Spr}_\phi(p, p')$ is empty for $p \neq p'$ and a_p, b_p and q_p are p–orbital (some of those components are allowed to be in R). Let $m = \mathrm{Dis}_\phi(a,b)$ be finite and nonnegative. Since each $\mathcal{O}_p^\phi$ is closed under ϕ and any two nonzero elements of $\mathcal{O}_p^\phi$ and $\mathcal{O}_{p'}^\phi$ have an empty spread, hence are coprime, by Lemma 17 whenever $p \neq p'$, we have $d = \prod_{p \in \mathcal{P}} d_p$ where $d_p = \gcd(a_p, \phi^m b_p)$, which implies that the orbital decompositions of a' and b' are

$$a' = \prod_{p \in \mathcal{P}} a'_p = \prod_{p \in \mathcal{P}} \frac{a_p}{d_p} \quad \text{and} \quad b' = \prod_{p \in \mathcal{P}} b'_p = \prod_{p \in \mathcal{P}} \frac{a_p}{\phi^{-m} d_p} .$$

Furthermore, $c = \prod_{p\in\mathcal{P}} c_p$ where $c_p = \prod_{j=0}^{m} \phi^{-j} d_p$, so the orbital decomposition of q' is $q' = \prod_{p\in\mathcal{P}} q'_p = \prod_{p\in\mathcal{P}} (q_p/\gcd(c_p, q_p))$. Since $\mathrm{Dis}_\phi(a,b)$ is finite, $\mathrm{Dis}_\phi(a_p,b_p)$ is finite for each p, and $m \geq \mathrm{Dis}_\phi(a_p,b_p)$, so either $m > \mathrm{Dis}_\phi(a_p,b_p)$, in which case $d_p = 1$, which implies that $a'_p = a_p$, $b'_p = b_p$ and $q'_p = q_p$, hence that q'_p is bounded by (a'_p, b'_p), or $m = \mathrm{Dis}_\phi(a_p,b_p)$, in which case the above proof shows that q'_p is bounded by (a'_p, b'_p). Thus, q'_p is bounded by (a'_p, b'_p), hence by (a', b') in any case, so q' is bounded by (a', b'). □

We can now generalize the algorithm of [5] for computing a common multiple of primitive polynomials bounded by a given pair.

Theorem 8 *Let $R[X]$ be a polynomial ring over a unique factorization domain R, ϕ be an automorphism of $R[X]$ mapping R onto R and $a, b \in R[X]$ be such that $Spr_\phi(a,b)$ is finite. Write*

$$Spr_\phi(a,b) = \{m_1 > m_2 > \ldots > m_s \geq 0\}$$

and let (g_i), (a_i), (b_i) and (u_i) be the sequences given by $a_1 = a$, $b_1 = b$, $u_1 = 1$, g_i is the primitive part of $\gcd(a_i, \phi^{m_i} b_i)$ and

$$a_{i+1} = \frac{a_i}{g_i}, b_{i+1} = \frac{b_i}{\phi^{-m_i} g_i}, u_{i+1} = u_i \prod_{j=0}^{m_i} \phi^{-j} g_i \quad \textit{for } 1 \leq i \leq s\,.$$

Let $d \in R[X] \setminus \{0\}$ be primitive and have no irreducible factor in $R[X]^{\phi^*}$, and suppose that d is bounded by (a,b). Then, $d \mid u_{s+1}$.

Proof. We first show by induction on i that $\mathrm{Spr}_\phi(a_i,b_i) \subseteq \{m_i > \ldots > m_s\}$. This holds by hypothesis for $i = 1$, so suppose that it holds for some $i \geq 1$. Let $m \in \mathrm{Spr}_\phi(a_{i+1}, b_{i+1})$ and $p \in R[X]$ be an irreducible factor of $\gcd(a_{i+1}, \phi^m b_{i+1})$. Since $a_{i+1} \mid a_i$ and $b_{i+1} \mid b_i$, $p \mid \gcd(a_i, \phi^m b_i)$, which implies that $m \in \mathrm{Spr}_\phi(a_i,b_i)$, hence that $\mathrm{Spr}_\phi(a_{i+1}, b_{i+1}) \subseteq \{m_i > \ldots > m_s\}$. Let now $h \in R[X]$ be any divisor of $\gcd(a_{i+1}, \phi^{m_i} b_{i+1})$. Then, $h \mid a_i/g_i$ and $h \mid \phi^{m_i}(b_i/\phi^{-m_i} g_i) = \phi^{m_i}(b_i)/g_i$. But $\gcd(a_i/g_i, \phi^{m_i}(b_i)/g_i) \in R$, which implies that $h \in R$, hence that $m_i \notin \mathrm{Spr}_\phi(a_{i+1}, b_{i+1})$ so $\mathrm{Spr}_\phi(a_{i+1}, b_{i+1}) \subseteq \{m_{i+1} > \ldots > m_s\}$. As a consequence, $\mathrm{Spr}_\phi(a_{s+1}, b_{s+1})$ must be empty. Consider now the sequence (d_i) given by $d_1 = d$ and $d_{i+1} = d_i/\gcd(d_i, u_{i+1}/u_i)$ for $1 \leq i \leq s$. Multiplying the definition of d_{i+1} by u_{i+1}/u_i, we see that $d_i \mid d_{i+1} u_{i+1}/u_i$, so $u_i d_i \mid u_{i+1} d_{i+1}$. Since $d = u_1 d_1$, it follows that $d \mid u_i d_i$ for $1 \leq i \leq s+1$, hence that $d \mid u_{s+1} d_{s+1}$. Since $d_{i+1} \mid d_i$ for $1 \leq i \leq s$ and d_1 has no irreducible factor in $R[X]^{\phi^*}$, it follows that d_i has no irreducible factor in $R[X]^{\phi^*}$ for $1 \leq i \leq s$. We now show by induction on i that d_i is bounded by (a_i, b_i). This holds by hypothesis for $i = 1$, so suppose that it holds for some $i \geq 1$. Since $m_i \geq \mathrm{Dis}_\phi(a_i,b_i)$ and $u_{i+1}/u_i = \prod_{j=0}^{m_i} \phi^{-j}(\gcd(a_i, \phi^{m_i} b_i))$, Lemma 19 implies that d_{i+1} is bounded by (a_{i+1}, b_{i+1}). Therefore, d_{s+1} is bounded by (a_{s+1}, b_{s+1}). But $\mathrm{Spr}_\phi(a_{s+1}, b_{s+1})$ is empty, so $\mathrm{Dis}_\phi(d_{s+1}) = -1$ by Lemma 18, which implies that $d_{s+1} \in R \setminus \{0\}$. Since $d \mid d_{s+1} u_{s+1}$, taking the primitive parts on both sides we get that d divides the primitive part of u_{s+1}, hence that $d \mid u_{s+1}$. □

We conclude by remarking that the orbital decomposition is a different concept than the greatest factorial factorization of [20], since we allow gaps in the factorials. The empty–spread hypothesis of Lemma 15 does not hold in general for greatest factorial factorizations.

On the other hand, we do not know how to compute orbital decompositions using only gcd computations (unless an *a priori* bound on the dispersion is known), while this is possible for greatest factorial factorizations. Greatest factorial factorizations and the algorithm to compute them can be generalized to the finite parts of splitting factorization whenever ϕ is an automorphism of $R[X]$ mapping R onto R.

6 Rational solutions

We consider in this section the problem of finding the denominators of the solutions in $k(t)$ of linear functional equations. The main result is that the dispersion of the finite part of such denominators can be bounded, and this allows the finite part to be computed.

Theorem 9 *Let (k,σ,δ) be a σ–differential field, t be a unimonomial over k, $a_0,\ldots,a_n$ in $k[t]$ be such that $a_0 \neq 0 \neq a_n$ and let $a_0 = a_{0\infty}\overline{a_0}$ be a splitting factorization of a_0 with respect to σ. Then, $Dis_\sigma(a_n,\overline{a_0})$ is finite and any $y \in k(t)$ satisfying*

$$\sum_{i=0}^{n} a_i \sigma^i y \in k[t]\,, \tag{15}$$

can be written as $y = a/d$ with $a,d \in k[t]$ and d has a splitting factorization $d = d_\infty \overline{d}$ where

$$Dis_\sigma(\overline{d}) \leq \max\left(-1, Dis_\sigma(a_n,\overline{a_0}) - n\right).$$

Proof. Since $\overline{a_0}$ has no nontrivial factor in $k[t]^{\sigma^*}$, Theorem 6 implies that $\mathrm{Dis}_\sigma(a_n,\overline{a_0})$ is finite. Let $y \in k(t)$ satisfy (15). If $y = 0$, then we can take $a = 0$ and $d = \overline{d} = 1$, so $\mathrm{Dis}_\sigma(\overline{d}) = -1$, which satisfies the theorem, so suppose that $y \neq 0$ and write $y = a/d$ where $a,d \in k[t]\setminus\{0\}$, d is monic and $\gcd(a,d) = 1$. Let $d = d_\infty\overline{d}$ be a splitting factorization of d where both d_∞ and $\overline{d}$ are monic and $m = \mathrm{Dis}_\sigma(\overline{d})$. If $m = -1$, then the theorem is satisfied, so suppose that $m \geq 0$ and let $p \in k[t]$ be an irreducible common factor of $\overline{d}$ and $\sigma^m\overline{d}$. Then, $q = \sigma^{-m}p$ is irreducible, $q \mid \overline{d}$ and $\sigma^m q \mid \overline{d}$. Furthermore, $\sigma^{-j}q \not| \overline{d}$ for any $j > 0$, otherwise we would have $p \mid \sigma^{m+j}\overline{d}$ and $m + j \in \mathrm{Spr}_\sigma(\overline{d})$. This implies that $\sigma^{i-j}q \not| \sigma^i\overline{d}$ for any $i \geq 0$ and $j > 0$, hence in particular that $q \not| \sigma^i\overline{d}$ for any $i > 0$. Every irreducible factor of d_∞ must be in $k[t]^{\sigma^*}$ by Theorem 6. Since σ maps irreducibles to irreducibles and $k[t]^{\sigma^*}$ is closed under σ by Lemma 3, it follows that every irreducible factor of $\sigma^i d_\infty$ is in $k[t]^{\sigma^*}$, hence that $q \not| \sigma^i d_\infty$ for any $i \geq 0$. Therefore, $q \not| \sigma^i d$ for any $i > 0$. Since $q \mid d$ and y satisfies (15), it follows that $q \mid a_0$, hence that $q \mid \overline{a_0}$ since $q \notin k[t]^{\sigma^*}$. In a similar fashion, $\sigma^{m+i+j}q \not| \sigma^i\overline{d}$ for any $i \geq 0$ and $j > 0$, otherwise we would have $\sigma^j p \mid \overline{d}$ and $m + j \in \mathrm{Spr}_\sigma(\overline{d})$. This implies in particular that $\sigma^{m+n}q \not| \sigma^i\overline{d}$ for $0 \leq i < n$. As above, $\sigma^{m+n}q \not| \sigma^i d_\infty$ for any $i \geq 0$, so $\sigma^{m+n}q \not| \sigma^i d$ for $0 \leq i < n$. Since $\sigma^{m+n}q \mid \sigma^n d$ and $\gcd(\sigma^n a, \sigma^n d) = \gcd(a,d) = 1$, it follows that $\sigma^{m+n}q \mid a_n$. Therefore, $\sigma^{m+n}q \mid \gcd(a_n, \sigma^{m+n}\overline{a_0})$, which implies that $m + n \in \mathrm{Spr}_\sigma(a_n,\overline{a_0})$ and the theorem follows. □

Recall that the notions of being in $k[t]^{\sigma^*}$ or having all its irreducible factors in $k[t]^{\sigma^*}$ are equivalent (Lemma 3).

Corollary 3 *With the hypotheses and notations of Theorem 9, if* $Dis_\sigma(a_n, \overline{a_0}) < n$, *then any* $y \in k(t)$ *satisfying (15) can be written as* $y = a/d$ *where* $a \in k[t]$ *and* $d \in k[t]^{\sigma^*}$.

Proof. This follows immediately from Theorems 6 and 9. □

Note that the hypothesis of Corollary 3 is satisfied when either $\overline{a}_0 \in k^*$ or $a_n \in k^*$, as in the following example.

Example 11 *Consider the recurrence equation (10) from Example 2. Since its leading coefficient is* 1, *Corollary 3 implies that any solution* $y \in \mathbb{Q}(n, n!)$ *must be in fact in* $\mathbb{Q}(n)[n!, n!^{-1}]$.

Once we have a bound on the dispersion of the finite part of the denominator, the algorithm of [3] can be generalized to arbitrary unimonomial extensions as follows: with the hypotheses and notations as in Theorem 9, let $L = a_n E^n + \ldots + a_0$ be a difference operator in $\mathcal{R} = k(t)[E; \sigma, 0]$, $V = \mathcal{R}/\mathcal{R}L$ and $\pi_L : \mathcal{R} \to V$ be the right–remainder by L. Let $h > 0$ be an integer and $z_i = \pi_L(E^{ih})$ for $i \geq 0$. Since V is a finite–dimensional vector space over $k(t)$, the family $(z_i)_{i \geq 0}$ is linearly dependent over $k(t)$, so let $b_0 z_0 + \ldots + b_s z_s = 0$ be a linear dependence relation over $k(t)$ with $b_s \neq 0$ (such a relation can be computed by Gaussian elimination) and $L_h = b_s E^{hs} + \ldots + b_0 \in \mathcal{R}$. Since $\pi_L(L_h) = 0$, $L_h = RL$ for some $R \in \mathcal{R}$, which can be computed by Euclidean division in $\mathcal{R}$. It follows that $L_h y = Rb$ for any $b \in k[t]$ and any solution $y \in k(t)$ of $Ly = b$. Clearing denominators, we get that every solution $y \in k(t)$ of $Ly = b$ satisfies an equation of the form

$$c_s \sigma^{hs} y + \ldots + c_1 \sigma^h y + c_0 y = b_h \tag{16}$$

where $c_0, \ldots, c_s, b_h \in k[t]$ and $c_s \neq 0$. Suppose now that h was chosen so that the denominator of y has a splitting factorization of the form $d = d_\infty \overline{d}$ where $\mathrm{Dis}_\sigma(\overline{d}) < h$ (such a bound can be obtained by Theorem 9) and let $p \in k[t]$ be an irreducible factor of $\overline{d}$ and $e_p > 0$ be such that $p^{e_p} \mid \overline{d}$ and $p^{e_p+1} \not| \overline{d}$. Then, $(\sigma^{ih} p)^{e_p} \mid \sigma^{ih} \overline{d}$ for any $i \geq 0$. But $\sigma^{ih} p \not| \sigma^{jh} \overline{d}$ for any $i, j \geq 0$ and $i \neq j$, otherwise we would have $|i - j| h \in \mathrm{Spr}_\sigma(\overline{d})$. As in the proof of Theorem 9, every factor of $\sigma^{ih} d_\infty$ is in $k[t]^{\sigma^*}$, which implies that $\sigma^{ih} p \not| \sigma^{jh} d_\infty$ for any $i, j \geq 0$. Therefore, $(\sigma^{ih} p)^{e_p} \mid \sigma^{ih} d$ for any $i \geq 0$ and $\sigma^{ih} p \not| \sigma^{jh} d$ whenever $i \neq j$. Since y is a solution of (16), it follows that $(\sigma^{ih} p)^{e_p} \mid c_i$, hence that $p^{e_p} \mid \sigma^{-ih} c_i$ for $0 \leq i \leq s$. Since this holds for every irreducible factor of $\overline{d}$, we get that

$$\overline{d} \mid \gcd_{0 \leq i \leq s} \left(\sigma^{-ih} c_i \right),$$

which allows us to compute a multiple of $\overline{d}$. We note that the above algorithm can be used in order to compute the denominators of solutions with bounded dispersions, even when no algorithm to compute the dispersion is available. A dispersion algorithm is however necessary in order to compute a bound by Theorem 9. Combining Karr's computation of the specification of equivalence [17] with Theorem 7, this yields an algorithm for computing the finite part of denominators of solutions in $\Pi\Sigma$–extensions. Also, since a rational algorithm for computing the dispersion exists for q–difference equations with polynomial coefficients,

this yields the following alternative to [4, 5] for computing the rational solutions of such equations: let C be a field and $q \in C$ be such that q is not a root of unity and C is q-suitable in the sense of [6],*i.e.* there is an algorithm for finding the roots of the form q^m with $m \in \mathbb{Z}$ and $m \geq 0$ of univariate algebraic equations over C. For example, any finitely generated extension of $F(q)$ is q–suitable where F is a finitely generated extension of $\mathbb{Q}$ and q is either transcendental over F or algebraic over $\mathbb{Q}$ with complex norm not equal to 1 [4]. Let x be an indeterminate over C and σ be the automorphism of $F(x)$ given by $\sigma x = qx$ and $\sigma a = a$ for any $a \in F$. Since $\sigma x/x = q$ is not a root of unity, $\sigma a \neq q^n a$ for any $a \in F^*$ and integer $n > 0$, so q is not a σ–radical over F. Corollary 2 then implies that x is a unimonomial over F, $\mathrm{Const}_{\sigma,0}(F(x)) = F$ and

$$F[x]^{\sigma^*} = F[x]^{\sigma} = F \cup \{ax^m \text{ such that } a \in F, m \geq 0\}\,.$$

Therefore a splitting factorization of $p \in F[x]$ is simply $p = x^m \overline{p}$ where $m \geq 0$ and $\overline{p}(0) \neq 0$. Since C is q–suitable, spreads and dispersions with respect to σ can be computed via resultants [4, 6]. Given a q–difference equation $\sum_{i=0}^{n} a_i \sigma^i y = b$ where $a_0, \ldots, a_n, b \in F[x]$ and $a_0 \neq 0 \neq a_n$, the above algorithm for the denominator reduces the problem of computing its solutions in $F(x)$ to computing its solutions in $F[x, x^{-1}]$. A bound for the power of x that can appear in the denominator is obtained by solving the indicial equation of [4], thereby reducing the problem to computing its solutions in $F[x]$. The recurrence of [1] gives an upper bound for the degree of those solutions, and we conclude by applying the algorithm of Section 3, specializing the equation at $x = 0$.

Example 12 *[4] Consider the q–difference equation*

$$q^3(qx+1)y(q^2x) - 2q^2(x+1)y(qx) + (x+q)y(x) = 0 \tag{17}$$

whose coefficients are in $(k(x), \sigma, \delta)$ where $k = \mathbb{Q}(q)$, q is transcendental over $\mathbb{Q}$, x is an indeterminate over k, $\delta = 0$, and σ is the automorphism of $k(x)$ over k that maps x to qx. We have $\overline{a_0} = x + q$, $a_2 = q^3(qx+1)$ and

$$res_x(q^3(qx+1), \sigma^m(x+q)) = res_x(q^3(qx+1), q^m x + q) = q^3(q^2 - q^m)\,,$$

which implies that $Dis_\sigma(a_2, \overline{a_0}) = 2$, hence that any solution of (17) has a denominator of the form $x^n \overline{d}$ where $Dis_\sigma(\overline{d}) \leq 0$. Using the bound $h = 1$, we get $L_h = L$ and

$$\overline{d} \mid \gcd(x+q, \sigma^{-1}(q^2(x+1)), \sigma^{-2}(q^3(qx+1))) = \gcd(x+q, q(x+q), q^2(x+q)) = x+q\,.$$

Therefore, any rational solution of (17) can be written as $y = p/(x^n(x+q))$ where $n \geq 0$ and $p \in k[x]$. The indicial equation at $x = 0$ is [4]:

$$qZ^2 - 2q^2 Z + q^3 = 0\,.$$

Its only solution of the form $Z = q^m$ is for $m = 1$, which implies that any rational solution of (17) can be written as $y = p/(x(x+q))$. Replacing y by this form in (17) we get

$$p(q^2x) - 2p(qx) + p(x) = 0\,. \tag{18}$$

The indicial equation for the degree of the polynomial solutions is [1]:

$$Z^2 - 2Z + 1 = 0\,.$$

Its only solution of the form $Z = q^m$ is for $m = 0$, which implies that any polynomial solution of (18) must be of the form $p_0 \in k$. The equation (18) now becomes $p_0 - 2p_0 + p_0 = 0$, whose solution space is k. This implies that the general rational solution of (17) is

$$y = \frac{C}{x(x+q)} \qquad \textit{for any } C \in \mathbb{Q}(q)\,.$$

We now generalize Abramov's second algorithm for the denominator [4, 5] to unimonomial extensions. The following Lemma first reduces the problem to bounding p–orbital denominators.

Lemma 20 *Let (k, σ, δ) be a σ–differential field, t be a unimonomial over k, $a_0, \ldots, a_n$ in $k[t]$ and $y \in k(t)$ be such that $\sum_{i=0}^{n} a_i \sigma^i y \in k[t]$. Write $y = a/d$ where $a, d \in k[t]$, $d \neq 0$, $\gcd(a, d) = 1$, let $d = d_\infty \overline{d}$ be a splitting factorization of d, $\overline{d} = d_1 \ldots d_m$ be an orbital decomposition of $\overline{d}$ with respect to σ and*

$$y = \frac{b_\infty}{d_\infty} + \sum_{j=1}^{m} \frac{b_j}{d_j}$$

be a partial fraction decomposition of y where $b_\infty, b_1, \ldots, b_m \in k[t]$ and $\gcd(b_\infty, d_\infty) = \gcd(b_j, d_j) = 1$ for $1 \leq j \leq m$. We then have

$$\sum_{i=0}^{n} a_i \sigma^i \left(\frac{b_\infty}{d_\infty}\right) \in k[t] \qquad \textit{and} \qquad \sum_{i=0}^{n} a_i \sigma^i \left(\frac{b_j}{d_j}\right) \in k[t] \textit{ for } 1 \leq j \leq m\,.$$

Proof. Write $L = \sum_{i=0}^{n} a_i \sigma^i$. Then,

$$Ly = L\frac{b_\infty}{d_\infty} + \sum_{j=1}^{m} L\frac{b_j}{d_j} \in k[t]\,.$$

Let $p_1, \ldots, p_m \in R[X]$ be irreducibles such that $q_j \in \mathcal{O}_{p_j}^{\sigma}$ for $1 \leq j \leq m$. Since $\mathcal{O}_{p_j}^{\sigma}$ is closed under σ as well as under taking factors by Lemma 17, we have $L(b_j/d_j) = c_j/h_j$ where $c_j \in k[t]$ and $h_j \in \mathcal{O}_{p_j}^{\sigma}$ for each j. Since $\mathrm{Spr}_\sigma(p_i, p_j)$ is empty for $i \neq j$ in an orbital decomposition, Lemma 17 also implies that $\mathrm{Spr}_\sigma(h_i, h_j)$ is empty, hence that $\gcd(h_i, h_j) = 1$, for $i \neq j$. In addition, $d_\infty \in k[t]^{\sigma^*}$, which is closed under σ and under taking factors by Lemma 3, so $L(b_\infty/d_\infty) = c_\infty/h_\infty$ where $c_\infty \in k[t]$ and $h_\infty \in k[t]^{\sigma^*}$, which implies that $\gcd(h_\infty, h_j) = 1$ for $1 \leq j \leq m$ since $p_j \notin k[t]^{\sigma^*}$ implies that $\sigma^m p_j \notin k[t]^{\sigma^*}$ for any $m \geq 0$. We now have

$$Ly = \frac{c_\infty}{h_\infty} + \sum_{j=1}^{m} \frac{c_j}{h_j} \in k[t]$$

where the denominators are two by two coprime, which implies that each term in the above sum must be in $k[t]$. □

We can now show that the denominator of a solution of a linear functional equation is bounded by its leading and trailing coefficients.

Theorem 10 *Let (k,σ,δ) be a σ–differential field, t be a unimonomial over k, $a_0,\ldots,a_n$ in $k[t]$ be such that $a_0 \neq 0 \neq a_n$ and let $a_0 = a_{0\infty}\overline{a_0}$ be a splitting factorization of a_0 with respect to σ. Let $y \in k(t)$ be such that $\sum_{i=0}^{n} a_i\sigma^i y \in k[t]$, write $y = a/d$ where $a,d \in k[t]$, $d \neq 0$, $\gcd(a,d) = 1$, and let $d = d_\infty\overline{d}$ be a splitting factorization of d. Then, $\overline{d}$ is bounded by $(\sigma^{-n}a_n, \overline{a_0})$.*

Proof. Let $\overline{d} = d_1 \ldots d_m$ be an orbital decomposition of $\overline{d}$ with respect to σ and

$$y = \frac{b_\infty}{d_\infty} + \sum_{j=1}^{m} \frac{b_j}{d_j}$$

be a partial fraction decomposition of y where $b_\infty, b_1, \ldots, b_m \in k[t]$ and $\gcd(b_\infty, d_\infty) = \gcd(b_j, d_j) = 1$ for $1 \leq j \leq m$. Since $\sum_{i=0}^{n} a_i\sigma^i(b_j/d_j) \in k[t]$ for each j by Lemma 20, we can replace y by b_j/d_j and assume that its denominator d is p–orbital for some irreducible $p \in k[t]$ such that $p \notin k[t]^{\sigma^*}$. If $d \in k$, then $B^-(d)$ and $B^+(d)$ are empty and the theorem holds, so assume that $d \notin k$ and let $B^-(d) = \{j_1 < \ldots < j_r\}$ where $r \geq 1$, w be an integer between 1 and r and $p_w = \sigma^{j_w}p$. Then, $p_w \in k[t]$ is irreducible and $p_w^{e_{j_w}} \mid d$. Suppose that $p_w^e \mid \sigma^m d$ for some integers $m > 0$ and $e > 0$. Then, $\sigma^{j_w - m}(p)^e \mid d$, which implies that $m \leq j_w$ and that $e < e_{j_w}$ since $j_w \in B^-(d)$. By definition of B^-, $e_j < e_{j_w}$ for $j < j_w$ and $e_j < e_{j_{w-1}}$ for $j < j_{w-1}$. Let $\mu = \max_{j_{w-1}<j<j_w}(e_j)$ and v be minimal among the indices such that $j_{w-1} < v < j_w$ and $e_v = \mu$. Since $v \notin B^-(d)$, we must have $\mu \leq e_{j_{w-1}}$, which implies that $e_j \leq e_{j_{w-1}}$ for $j_{w-1} < j < j_w$, hence that $e_j \leq e_{j_{w-1}}$ for $j < j_w$. Taking $j = j_w - m < j_w$, we get that $e \leq e_{j_{w-1}}$, hence that the largest power of p_w that can divide the denominator of $\sigma^m y$ for $m > 0$ is $p_w^{e_{j_{w-1}}}$. Since $\sum_{i=0}^{n} a_i\sigma^i y \in k[t]$ and $a_0 \neq 0$, it follows that $p_w^{e_{j_w} - e_{j_{w-1}}} \mid a_0$. Since $p \notin k[t]^{\sigma^*}$, $p_w \notin k[t]^{\sigma^*}$, so $p_w^{e_{j_w} - e_{j_{w-1}}} \mid \overline{a_0}$ and $\overline{a_0}$ is a left–bound for d. Let now $B^+(d) = \{i_1 < \ldots < i_s\}$ where $s \geq 1$, w be an integer between 1 and s and $p_w = \sigma^{i_w+n}p$. Then, $p_w \in k[t]$ is irreducible and $p_w^{e_{i_w}} \mid \sigma^n d$. Suppose that $p_w^e \mid \sigma^m d$ for some integers $0 \leq m < n$ and $e > 0$. Then, $\sigma^{i_w+n-m}(p)^e \mid d$, which implies that $e < e_{i_w}$ since $i_w \in B^+(d)$. As above, the definition of B^+ implies that $e_i \leq e_{i_w+1}$ for $i > i_w$. Taking $i = i_w + n - m > i_w$, we get that $e \leq e_{i_w+1}$, hence that the largest power of p_w that can divide the denominator of $\sigma^m y$ for $0 \leq m < n$ is $p_w^{e_{i_w+1}}$. Since $\sum_{i=0}^{n} a_i\sigma^i y \in k[t]$ and $a_n \neq 0$, it follows that $p_w^{e_{i_w} - e_{i_w+1}} \mid a_n$, hence that $\sigma^{i_w}(p)^{e_{i_w} - e_{i_w+1}} \mid \sigma^{-n}a_n$, implying that $\sigma^{-n}a_n$ is a right–bound for d. □

Our generalization of Abramov's second algorithm now follows from Theorems 8 and 10: let $h_0,\ldots,h_n,h \in k[t]$ be such that $h_0 \neq 0 \neq h_n$ and let $h_0 = h_{0\infty}\overline{h_0}$ be a splitting factorization of h_0 with respect to σ. Then, $\mathrm{Spr}_\sigma(\sigma^{-n}h_n, \overline{h_0})$ is finite by Theorem 6, so let u_{s+1} be the result of the iteration of Theorem 8 with $a = \sigma^{-n}h_n$ and $b = \overline{h_0}$. Then, if $y \in k(t)$ is a solution of $\sum_{i=0}^{n} h_i\sigma^i y = h$, the denominator of $u_{s+1}y$ must be in $k[t]^{\sigma^*}$.

Example 13 *Consider again the q–difference equation (17) of Example 12. As in that example, we have* $\overline{h_0} = x + q$ *and* $h_2 = q^3(qx+1)$*, so* $\sigma^{-2}h_2 = q^2(x+q)$ *and*

$$res_x(q^2(x+q), \sigma^m(x+q)) = res_x(q^2(x+q), q^m x + q) = q^3(1-q^m)\,,$$

which implies that $Spr_\sigma(\sigma^{-2}h_2, \overline{h_0}) = \{0\}$*. The iteration is then* $a_1 = q^2(x+q)$*,* $b_1 = x+q$*,* $u_1 = 1$*,* $g_1 = \gcd(a_1, b_1) = x+q$*, and* $u_2 = g_1 = x+q$*, so we find again that any rational solution of (17) can be written as* $y = a/(x^n(x+q))$ *where* $n \geq 0$ *and* $a \in \mathbb{Q}(q)[x]$*. Continuing as in Example 12 yields the general rational solution* $y = C/(x(x+q))$ *for* $C \in \mathbb{Q}(q)$*.*

We remark that Theorem 9 can be obtained as a corollary of Theorem 10: since $\overline{d}$ is bounded by $(\sigma^{-n}a_n, \overline{a}_0)$, Lemma 18 implies that $\mathrm{Dis}_\sigma(\overline{d}) \leq \mathrm{Dis}_\sigma(\sigma^{-n}a_n, \overline{a}_0)$. Since Lemma 16 implies that $\mathrm{Dis}_\sigma(\sigma^{-n}a_n, \overline{a}_0) = \max(-1, \mathrm{Dis}_\sigma(a_n, \overline{a}_0) - n)$, Theorem 9 follows.

Another consequence of Theorem 9 is useful in the context of symbolic summation: we see from Example 9 that $\mathrm{Dis}_{d/dX}(q)$ is a measure of the multiplicities of the factors of q, and that applying d/dx to a fraction increases the dispersion of its denominator (w.r.t. d/dx). This property is fundamental for integration methods, such as the Hermite reduction [10, 14], which can be seen as a processus for gradually decreasing the dispersion of the denominator of an integrand. A similar property for finite differences was given in [2] and has been used in summation algorithms. Its generalization to unimonomial extensions follows from Theorem 9.

Corollary 4 *Let* (k, σ, δ) *be a* σ*–differential field,* t *be a unimonomial over* k *and* $a, b, c, d \in k[t]$ *be such that* $b \neq 0 \neq d$*,* $\gcd(a, b) = \gcd(c, d) = 1$ *and*

$$\sigma\frac{a}{b} - \frac{a}{b} = \frac{c}{d}\,.$$

Let $b = b_\infty \overline{b}$ *and* $d = d_\infty \overline{d}$ *be splitting factorizations of* b *and* d*. If* $\overline{d} \notin k$*, then*

$$Dis_\sigma(\overline{d}) = 1 + Dis_\sigma(\overline{b})\,.$$

Proof. Suppose that $\overline{d} \notin k$. Applying Theorem 9 to $(d\sigma - d)(a/b) = c \in k[t]$, we get

$$\mathrm{Dis}_\sigma(\overline{b}) \leq \max(-1, \mathrm{Dis}_\sigma(d, \overline{d}) - 1)\,.$$

Since $k[t]^{\sigma^*}$ is closed under σ^{-1} by Lemma 3, $\sigma^m(\overline{d})$ has no irreducible factor in $k[t]^{\sigma^*}$, which implies that $\mathrm{Dis}_\sigma(d, \overline{d}) = \mathrm{Dis}_\sigma(\overline{d}) \geq 0$, hence that $\mathrm{Dis}_\sigma(\overline{b}) \leq \mathrm{Dis}_\sigma(\overline{d}) - 1$. Conversely, using (2) with $\delta = \sigma - 1$ shows that $d \mid b\sigma b$, hence that $\overline{d} \mid \overline{b}\sigma\overline{b}$. Let $m = \mathrm{Dis}_\sigma(\overline{d}) \geq 0$ and p be an irreducible common factor of $\overline{d}$ and $\sigma^m\overline{d}$. Then $p \mid \overline{b}\sigma\overline{b}$ so either $p \mid \overline{b}$ or $p \mid \sigma\overline{b}$. Similarly, $p \mid \sigma^m(\overline{b}\sigma\overline{b})$ so either $p \mid \sigma^m\overline{b}$ or $p \mid \sigma^{m+1}\overline{b}$. Therefore, one of $m-1$,m or $m+1$ is in $\mathrm{Spr}_\sigma(\overline{b})$, which implies that $\mathrm{Dis}_\sigma(\overline{b}) \geq m - 1$ and the corollary follows. □

References

[1] Sergei Abramov, Manuel Bronstein, and Marko Petkovšek. On polynomial solutions of linear operator equations. In *Proceedings of ISSAC'95*, pages 290–296. ACM Press, 1995.

[2] Sergei A. Abramov. On the summation of rational functions. *Journal of Computational Mathematics and Mathematical Physics*, 11:324–330, 1971.

[3] Sergei A. Abramov. Rational solutions of linear differential and difference equations with polynomial coefficients. *Journal of Computational Mathematics and Mathematical Physics*, 29:1611–1620, 1989.

[4] Sergei A. Abramov. Rational solutions of linear difference and q–difference equations with polynomial coefficients. In A.H.M. Levelt, editor, *Proceedings of ISSAC'95*, pages 285–289. ACM Press, 1995.

[5] Sergei A. Abramov. Rational solutions of linear difference and q–difference equations with polynomial coefficients. *Programming and Computer Software*, 21:273–278, 1995.

[6] Sergei A. Abramov, Peter Paule, and Marko Petkovšek. q-hypergeometric solutions of q-difference equations. *Discrete Mathematics*, 180:3–22, 1998.

[7] Raphaël Bomboy. Réductibilité des opérateurs aux différences finies: une approche galois–théorique. Rapport de Recherche RR–3735, INRIA, 1999.

[8] Manuel Bronstein. A unification of Liouvillian extensions. *Applicable Algebra in Engineering, Communication and Computing*, 1(1):5–24, 1990.

[9] Manuel Bronstein. On solutions of linear ordinary differential equations in their coefficient field. *Journal of Symbolic Computation*, 13(4):413–440, April 1992.

[10] Manuel Bronstein. *Symbolic Integration I – Transcendental Functions.* Springer, Heidelberg, 1997.

[11] Manuel Bronstein and Anne Fredet. Solving linear ordinary differential equations over $C(x, e^{\int f(x)dx})$. In Sam Dooley, editor, *Proceedings of ISSAC'99*, pages 173–179. ACM Press, 1999.

[12] Manuel Bronstein and Marko Petkovšek. An introduction to pseudo–linear algebra. *Theoretical Computer Science*, 157:3–33, 1996.

[13] P.A. Hendriks and M.F. Singer. Solving difference equations in finite terms. *J. Symbolic Computation*, 27(3):239–260, March 1999.

[14] E. Hermite. Sur l'intégration des fractions rationelles. *Nouvelles Annales de Mathématiques (2^{eme} série)*, 11:145–148, 1872.

[15] R. Kannan and R.J. Lipton. Polynomial–time algorithm for the orbit problem. *Journal of the ACM*, 33(4):808–821, October 1986.

[16] M. Karr. Theory of Summation in Finite Terms. *J. Symbolic Computation*, 1(3):303–316, September 1985.

[17] Michael Karr. Summation in finite terms. *Journal of the ACM*, 28:305–350, April 1981.

[18] Y.-K. Man. On computing closed forms for indefinite summations. *J. Symbolic Computation*, 16(4):355–376, October 1993.

[19] Oysten Ore. Theory of non-commutative polynomials. *Annals of Mathematics*, 34:480–508, 1933.

[20] P. Paule. Greatest factorial factorization and symbolic summation. *J. Symbolic Computation*, 20(3):235–268, September 1995.

[21] M.F. Singer. Liouvillian solution of linear differential equations with Liouvillian coefficients. *J. Symbolic Computation*, 11(3):251–274, March 1991.

Contents

Unité de recherche INRIA Sophia Antipolis
2004, route des Lucioles - B.P. 93 - 06902 Sophia Antipolis Cedex (France)

Unité de recherche INRIA Lorraine : Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - B.P. 101 - 54602 Villers lès Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38330 Montbonnot St Martin (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 Le Chesnay Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, B.P. 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399