Polynomial Ring Automorphisms, Rational (w, σ)-Canonical Forms, and the Assignment Problem

Dedicated to the memory of Manuel Bronstein (1963 – 2005)

S. A. Abramov

Russian Academy of Sciences
Dorodnicyn Computing Centre
Vavilova 40, 119991, Moscow GSP-1, Russia

M. Petkovšek

Faculty of Mathematics and Physics
University of Ljubljana
Jadranska 19, SI-1000 Ljubljana, Slovenia

Abstract

We investigate representations of a rational function $R \in k(x)$ where k is a field of characteristic zero, in the form $R = K \cdot \sigma S/S$. Here $K, S \in k(x)$, and σ is an automorphism of $k(x)$ which maps $k[x]$ onto $k[x]$. We show that the degrees of the numerator and denominator of K are simultaneously minimized iff $K = r/s$ where $r, s \in k[x]$ and r is coprime with $\sigma^n s$ for all $n \in \mathbb{Z}$. Assuming existence of algorithms for computing orbital decompositions of $R \in k(x)$ and semi-periods of irreducible $p \in k[x] \setminus k$, we present an algorithm for minimizing $w(\deg \mathrm{num}(S), \deg \mathrm{den}(S))$ among representations with minimal K, where w is any appropriate weight function. This algorithm is based on a reduction to the well-known assignment problem of combinatorial optimization. We show how to use these representations of rational functions to obtain succinct representations of σ-hypergeometric terms.

Key words: polynomial ring automorphisms, rational normal forms, rational canonical forms, product representation of hypergeometric terms

Preprint submitted to Elsevier *2 March 2010*

1. Introduction

Let k be a field of characteristic zero, and let x be transcendental over k. Denote by $\mathcal{E}$ the unique k-automorphism [1] of $k(x)$ which satisfies $\mathcal{E}x = x + 1$ (the *shift* operator). If $q \in k^*$, denote by $\mathcal{Q}$ the unique k-automorphism of $k(x)$ which satisfies $\mathcal{Q}x = qx$ (the *q-shift* operator).

Representations of a rational function $R \in k(x)$ in the form

$$R \;=\; K \cdot \frac{\sigma S}{S} \tag{1}$$

where σ is either the shift or the q-shift operator, and K is σ-reduced [2], play a significant rôle in various computer algebra algorithms for symbolic summation and solution of difference equations (see, e.g., (Gosper, 1978); (Zeilberger, 1991); (Petkovšek, 1992); (Pirastu and Strehl, 1995); (van der Put and Singer, 1997, Section 2.1); (Abramov and Petkovšek, 2002)). We call such a pair (K, S) a *rational σ-normal form* (RNF_σ) of R, with *kernel* K and *shell* S.

For the case $\sigma = \mathcal{E}$, it is shown in (Abramov and Petkovšek, 2001, Cor. 1) that the degrees of the numerator and denominator of K in (1) are simultaneously minimized iff K is σ-reduced. Once K has been minimized, it is also desirable to minimize S. Not surprisingly, the degrees of the numerator and denominator of S cannot, in general, be minimized simultaneously, and there is a choice of minimization criteria. In a preliminary version (Abramov, Le and Petkovšek, 2003), we used four such criteria, and called the corresponding rational normal forms (which are unique if S is monic), *rational canonical forms.*

In this paper, we generalize the theory and algorithms for computing rational normal and canonical forms in two directions. First, we allow σ to be *any automorphism* of $k(x)$ which maps $k[x]$ onto $k[x]$. In particular, we do not require that $\mathrm{Const}_\sigma(k(x)) = \mathrm{Const}_\sigma(k)$; instead, we assume that orbital decompositions [3] of rational functions in $k(x)$ and semi-periods [1] of irreducible polynomials in $k[x] \setminus k$ can be computed. Second, we show how to minimize $w(\deg \mathrm{num}(S), \deg \mathrm{den}(S))$ for *any weight function w*, by which we mean a monomorphism of the partially ordered Abelian group $\mathbb{Z}\times\mathbb{Z}$ into some computable linearly ordered Abelian group L. Typically, $L = \mathbb{Z} \times \mathbb{Z}$ ordered lexicographically. For example, if $w(n, d) = (n + d, d)$ then we minimize $\deg \mathrm{num}(S) + \deg \mathrm{den}(S)$, and in case of ties take the form with the least $\deg \mathrm{den}(S)$.

The overview of the paper is as follows: After describing our algebraic framework and notation in Section 2, we define rational σ-normal forms and state some of their basic properties in Section 3. In Section 4 we show how to use orbital decompositions with respect to σ to reduce problems about RNF_σ's of general rational functions to corresponding problems about p-orbital rational functions for an irreducible polynomial p. We give a constructive proof of existence of strict RNF_σ's in Section 5, and in Section 6

⋆ Supported in part by RFBR grant 04-01-00757 and ARRS grant P1-0294.

Email addresses: sabramov@ccas.ru (S. A. Abramov), marko.petkovsek@fmf.uni-lj.si (M. Petkovšek).

[1] see Section 2 for definitions

[2] see Definition 1 in Section 3

[3] see Definition 3 in Section 4

we show that the degrees of the numerator and denominator of K in (1) are simultaneously minimized iff (K, S) is an RNF_σ of R. The core of the paper consists of Sections 7 and 8 where we define *rational* (w, σ)*-canonical forms* ($\mathrm{RCF}_{w,\sigma}$'s), and show how to compute them. After presenting our algorithmic prerequisites in Section 8.1, we reduce in Section 8.2 computation of $\mathrm{RCF}_{w,\sigma}$'s to the *assignment problem*, a well-known combinatorial optimization problem with efficient algorithms to solve it (cf. (Papadimitriou and Steiglitz, 1982)). Two cases need to be distinguished in constructing this reduction, corresponding to p being non-periodic [4] or semi-periodic [4] w.r.t. σ. They are treated in Sections 8.3 and 8.4, respectively. In Section 9 we show that the rational (w, σ)-canonical form of $R \in k(x)$ is unique provided that each irreducible factor of R is non-periodic w.r.t. σ.

In Section 10, we present an application of rational canonical forms to the problem of obtaining succinct multiplicative representations of hypergeometric terms. Such representations are useful in simplification of hypergeometric terms and in investigation of their asymptotics. In this section we require that σ is a k-automorphism, and denote by $\tilde{n}$ the value of $\sigma^n x \in k[x]$ at $x = 1$. In particular, if $\sigma = \mathcal{E}$ then $\tilde{n} = n + 1$; if $\sigma = \mathcal{Q}$ then $\tilde{n} = q^n$. We call a sequence $t = \langle t_n \rangle_{n \geq 0}$ of elements of k a σ*-hypergeometric term* if $t_n \neq 0$ for n large enough, and there are coprime polynomials $p, q \in k[x] \setminus \{0\}$ such that

$$p(\tilde{n})t_{n+1} = q(\tilde{n})t_n \quad \text{for all } n \geq 0.$$

If there are $F, G \in k(x)$ such that $t_n = G(\tilde{n}) \prod_{i=0}^{n-1} F(\tilde{i})$ for all n, we call $\langle F, G \rangle$ a *multiplicative decomposition* of t. We show that if $t_0 \neq 0$, and (K, S) is an RNF_σ of $F \cdot \sigma G/G$ such that $S(1) \in k^*$, then $\langle K, S \cdot G(1)/S(1) \rangle$ is a multiplicative decomposition of t with minimal degrees of the numerator and denominator of its first component. Furthermore, if (K, S) is the $\mathrm{RCF}_{w,\sigma}$ of $F \cdot \sigma G/G$, then, in addition, the weight w of its second component is minimal among all such decompositions.

2. Preliminaries

We denote the set $\{1, 2, \ldots, n\}$ by $[n]$. In particular, $[0] = \emptyset$.

Throughout the paper, k is a field of characteristic zero, x is transcendental over k, and σ is a fixed automorphism of the polynomial ring $k[x]$. From $\sigma(k[x]^*) = k[x]^*$ and [5] $k[x]^* = k^*$ it follows that $\sigma(k) = k$, hence σ restricted to k is an automorphism of k. This implies that $\deg \sigma p = \deg p \cdot \deg \sigma x$ for every $p \in k[x]$, and so $\deg \sigma x = 1$ or else σ would not be surjective. Hence $\sigma x = ax + b$ for some $a \in k^*$ and $b \in k$. It follows that σ preserves degrees of polynomials, and maps irreducibles to irreducibles. The unique automorphism of the rational-function field $k(x)$ which extends σ will be denoted by σ as well. For $p, q \in k[x] \setminus \{0\}$, it is defined by $\sigma(p \cdot q^{-1}) = (\sigma p) \cdot (\sigma q)^{-1}$. Note that $(k(x), \sigma, 0)$ is a *unimonomial extension* of $(k, \sigma, 0)$ in the sense of (Bronstein, 2000). An automorphism σ of $k[x]$ or $k(x)$ is a k*-automorphism* if $\sigma\lambda = \lambda$ for all $\lambda \in k$. For any field F and automorphism σ of F we write $\mathrm{Const}_\sigma(F) := \{\lambda \in F;\ \sigma\lambda = \lambda\}$ for the *constant field* of F.

[4] see Section 2 for definitions

[5] If R is a ring with 1, we denote by R^* the group of units (i.e., invertible elements) of R.

For $p, q \in k[x]$, we write $p \perp q$ iff $\deg\gcd(p,q) = 0$. Clearly $p \perp q$ iff $\sigma p \perp \sigma q$. The leading coefficient of $p \in k[x]$ is denoted by $\mathrm{lc}\,(p)$. For $u, v \in k(x)$, we write $u \sim v$ iff $u = \lambda v$ for some $\lambda \in k^*$. For $u \in k(x)$, its numerator $\mathrm{num}(u)$ and denominator $\mathrm{den}(u)$ are uniquely determined by requiring that $\mathrm{num}(u) \in k[x]$, $\mathrm{den}(u) \in k[x] \setminus \{0\}$, $u = \mathrm{num}(u)/\mathrm{den}(u)$, $\mathrm{num}(u) \perp \mathrm{den}(u)$, and $\mathrm{lc}\,(\mathrm{den}(u)) = 1$. Obviously $\mathrm{num}(\sigma u) \sim \sigma\,\mathrm{num}(u)$ and $\mathrm{den}(\sigma u) \sim \sigma\,\mathrm{den}(u)$. We define $\mathrm{lc}\,(u) := \mathrm{lc}\,(\mathrm{num}(u))$, and call u *monic* if $\mathrm{lc}\,(u) = 1$.

Similarly as in (Abramov and Bronstein, 2000), we denote the n-th rising σ-factorial of an element $u \in k(x)^*$ by

$$u^{\sigma,n} \;=\; \prod_{i=0}^{n-1} \sigma^i u, \qquad u^{\sigma,-n} \;=\; \prod_{i=1}^{n} \sigma^{-i} u^{-1}$$

for all $n \in \mathbb{Z}$, $n \geq 0$, where an empty product equals 1. It is straightforward to see that for all $n, m \in \mathbb{Z}$ and $u, v \in k(x)^*$,

$$u^{\sigma,n+m} \;=\; u^{\sigma,n} \cdot \sigma^n(u^{\sigma,m}), \quad u^{\sigma,nm} \;=\; (u^{\sigma,n})^{\sigma^n,m},$$
$$(uv)^{\sigma,n} \;=\; u^{\sigma,n}v^{\sigma,n}, \qquad (\sigma u)^{\sigma,n} = \sigma\left(u^{\sigma,n}\right), \qquad \left(\frac{\sigma u}{u}\right)^{\sigma,n} \;=\; \frac{\sigma^n u}{u}.$$

If $p \in k[x] \setminus k$ is irreducible and n is a positive integer, then $\sigma^n p$ is irreducible and $\deg \sigma^n p = \deg p$, so either $\sigma^n p \perp p$ or $\sigma^n p \sim p$. The *semi-period* $\tilde{\pi}(p)$ of p is defined by

$$\tilde{\pi}(p) := \begin{cases} 0, & \text{if } \;\sigma^n p \perp p \;\text{ for all } n \geq 1, \\ \min\{n \geq 1;\; \sigma^n p \sim p\}, & \text{otherwise.} \end{cases}$$

We call p *non-periodic* if $\tilde{\pi}(p) = 0$, and *semi-periodic* if $\tilde{\pi}(p) > 0$. We denote

$$t(p) \;:= p^{\sigma,\tilde{\pi}(p)}, \qquad \mu(p) \;:=\; \sigma^{\tilde{\pi}(p)}p/p, \tag{2}$$

and call $t(p)$ the *total span* of p.

Proposition 1. Let $p \in k[x] \setminus k$ be irreducible. Then
(i) if p is non-periodic then $t(p) = 1$,
(ii) $\sigma t(p) = \mu(p)t(p)$ and $\sigma t(p) \sim t(p)$.

We omit the easy proof.

Let G_1 and G_2 be two partially ordered Abelian groups. A *monomorphism* of G_1 into G_2 is an injective mapping $h : G_1 \to G_2$ such that $h(a + b) = h(a) + h(b)$ and $a \leq b \Longrightarrow h(a) \leq h(b)$ for all $a, b \in G_1$.

3. Rational σ-normal forms

Definition 1. An element $R \in k(x)$ is *σ-reduced* if $\mathrm{num}(R) \perp \sigma^n\mathrm{den}(R)$ for all $n \in \mathbb{Z}$.

Definition 2. Let $R \in k(x)$. If $K \in k(x)$ and $S \in k(x)^*$ are such that
(i) $R = K \cdot \dfrac{\sigma S}{S}$,

(ii) K is σ-reduced,
then (K,S) is a *rational σ-normal form (*RNF$_\sigma$*)* of R. The set of all RNF$_\sigma$'s of R is denoted by RNF$_\sigma(R)$. We call K the *kernel* and S the *shell* of (K,S). If, in addition,
(iii) $\mathrm{num}(K) \perp \mathrm{num}(S) \cdot \mathrm{den}(\sigma S)$ and $\mathrm{den}(K) \perp \mathrm{den}(S) \cdot \mathrm{num}(\sigma S)$,
then (K,S) is a *strict* RNF$_\sigma$ of R. The set of all strict RNF$_\sigma$'s of R is denoted by sRNF$_\sigma(R)$.

Example 1. In our examples, σ is a k-automorphism of $k(x)$ unless explicitly stated otherwise. We specify it by giving $a \in k^*$ and $b \in k$ such that $\sigma x = ax + b$.

Let

$$R(x) \;=\; \frac{x^3}{(x-1)(x-2)(x-3)}.$$

1. If $\sigma x = 2x$ then $(R, 1) \in \mathrm{sRNF}_\sigma(R)$.
2. If $\sigma x = x + 1$ then $(1, (x-1)^3(x-2)^2(x-3)) \in \mathrm{sRNF}_\sigma(R)$.
3. If $\sigma x = 1 - x$ then $(-x^2/((x-2)(x-3)), 1-x) \in \mathrm{sRNF}_\sigma(R)$.

Lemma 1. Let (K,S) be an RNF$_\sigma$ of $R \in k(x)^*$. Then (K^{-1}, S^{-1}) is an RNF$_\sigma$ of R^{-1}. If (K,S) is strict then so is (K^{-1}, S^{-1}).

Proof: As σ preserves degrees, $K \in k(x)^*$ is σ-reduced iff K^{-1} is σ-reduced. $\square$

Lemma 2. Let $R \in k(x)$. If $(K,S) \in \mathrm{sRNF}_\sigma(R)$ then $\mathrm{num}(K) \,|\, \mathrm{num}(R)$ and $\mathrm{den}(K) \,|\, \mathrm{den}(R)$.

Proof: As $\mathrm{num}(R)\mathrm{den}(K)\mathrm{num}(S)\mathrm{den}(\sigma S) = \mathrm{den}(R)\mathrm{num}(K)\mathrm{den}(S)\mathrm{num}(\sigma S)$ and $\mathrm{num}(K) \perp \mathrm{den}(K)\,\mathrm{num}(S)\,\mathrm{den}(\sigma S)$, it follows that $\mathrm{num}(K) \,|\, \mathrm{num}(R)$. From $\mathrm{den}(K) \perp \mathrm{num}(K)\,\mathrm{den}(S)\,\mathrm{num}(\sigma S)$ it follows that $\mathrm{den}(K) \,|\, \mathrm{den}(R)$. $\square$

From Lemma 2 it follows immediately that if (K,S) is an sRNF$_\sigma$ of a $\lambda \in k$ then $K \in k$ as well. In fact, the same holds for any RNF$_\sigma$ of $\lambda \in k$.

Lemma 3. Let (K,S) be an RNF$_\sigma$ of $\lambda \in k$. Then $K \in k$.

Proof: If $\lambda = 0$ then $K = 0 \in k$. Now let $\lambda \neq 0$. Write $\mathrm{num}(S) = p_1 p_2 \cdots p_m$, $\mathrm{den}(S) = q_1 q_2 \cdots q_n$ where $p_i, q_j \in k[x]$ are irreducible. From $\lambda = K \cdot \sigma S / S$ it follows that $\mathrm{num}(K) \,|\, \mathrm{num}(S)\mathrm{den}(\sigma S)$ and $\mathrm{den}(K) \,|\, \mathrm{den}(S)\mathrm{num}(\sigma S)$. Let

$$\mathrm{num}(K) \sim \left(\prod_{i\in A} p_i\right)\left(\prod_{j\in B} \sigma q_j\right), \quad \mathrm{den}(K) \sim \left(\prod_{i\in C} \sigma p_i\right)\left(\prod_{j\in D} q_j\right)$$

where $A, C \subseteq [m]$ and $B, D \subseteq [n]$. Denote $\bar{A} = [m] \setminus A$, $\bar{B} = [m] \setminus B$, $\bar{C} = [n] \setminus C$, $\bar{D} = [n] \setminus D$. Then $\left(\prod_{i\in\bar{A}} p_i\right)\left(\prod_{j\in\bar{B}} \sigma q_j\right) \sim \left(\prod_{i\in\bar{C}} \sigma p_i\right)\left(\prod_{j\in\bar{D}} q_j\right)$. Since $k[x]$ is a unique factorization domain and $p_i \perp q_j$, it follows that there is a bijection $b : \bar{A} \to \bar{C}$ such that $p_i \sim \sigma p_{b(i)}$ for all $i \in \bar{A}$.

Assume that $C \neq \emptyset$, and pick an $i \in C$. As K is σ-reduced, $A \cap C = \emptyset$, so $i \in \bar{A}$ and b can be applied to i. If there is an infinite sequence over $\bar{A}$ of the form $\langle i, b(i), b^2(i), \ldots \rangle$ then

$b^n(i) = b^m(i)$ for some $n > m \geq 0$, so $b^{n-m}(i) = i \in C$. On the other hand, $b^{n-m}(i) \in b(\bar{A}) = \bar{C}$. This contradiction shows that there is an $r \geq 1$ such that $i, b(i), \ldots, b^{r-1}(i) \in \bar{A}$ while $b^r(i) \in A$. Then $p_{b^r(i)} \,|\, \mathrm{num}(K)$. From the properties of b it follows that $p_i \sim \sigma^r p_{b^r(i)}$, therefore $\sigma^{-r} p_i \,|\, \mathrm{num}(K)$. But this is impossible since $\sigma p_i \,|\, \mathrm{den}(K)$ and K is σ-reduced. Hence the assumption was false, and $C = A = \emptyset$.

By Lemma 1, (K^{-1}, S^{-1}) is an RNF_σ of λ^{-1}. Applying the above argument to (K^{-1}, S^{-1}) we see that $B = D = \emptyset$ as well. Hence $K \sim 1$, i.e., $K \in k^*$. □

4. Orbital decompositions

Definition 3. Let $p \in k[x] \setminus k$. Following (Bronstein, 2000) we say that $q \in k[x]$ is *p-orbital (with respect to σ)* if $q = u \prod_{i=0}^{n} \sigma^i p^{e_i}$ for some $u \in k$ (possibly 0) and $n, e_i \geq 0$. We say that $R \in k(x)$ is p-orbital (with respect to σ) if R can be written as the quotient of two p-orbital polynomials. An *orbital decomposition* of $R \in k(x)$ with respect to σ is a factorization $R = \prod_{i=1}^{N} R_i$ where each $R_i \in k(x)$ is p_i-orbital for some irreducible $p_i \in k[x]$ and p_i/p_j is σ-reduced for all $i, j \in [N]$. A closely related concept is called *σ-factorization* in (Karr, 1981; Schneider, 2005).

Lemma 4. Let $\prod_{i=1}^{N} R_i$ and $\prod_{i=1}^{N} R'_i$ be two orbital decompositions of $R \in k(x)^*$ where R_i and R'_i are p_i-orbital. Then $R_i \sim R'_i$ for all $i \in [N]$.

Proof: This follows from (Bronstein, 2000, Lemma 17(v)). □

Lemma 5. Let $p \in k[x]$ be irreducible. If $R \in k(x)^*$ is p-orbital and $(K, S) \in \mathrm{RNF}_\sigma(R)$, then K is p-orbital.

Proof: Let $K = \prod_{i=1}^{N} K_i$ and $S = \prod_{i=1}^{N} S_i$ be orbital decompositions of K resp. S where K_i, S_i are p_i-orbital. They exist by (Bronstein, 2000, Lemma 17(i)). W.l.g. assume that $p = p_1$. Denote $K' = K/K_1$, $S' = S/S_1$. Then

$$K' \cdot \frac{\sigma S'}{S'} = R \cdot \frac{S_1}{K_1 \sigma S_1}.$$

While the right-hand side is p_1-orbital, the left-hand side has an orbital decomposition of the form $\prod_{i=2}^{N} W_i$ where $W_i = K_i \sigma S_i / S_i$ is p_i-orbital for $i = 2, \ldots, N$. By Lemma 4, this is only possible if $K' \sigma S'/S' = R S_1/(K_1 \sigma S_1) \in k^*$. Since K is σ-reduced, K' is σ-reduced as well, and Lemma 3 implies that $K' \in k^*$. Thus $K = K' K_1$ is p-orbital. □

Note that in Lemma 5, S need not be p-orbital, even if $(K, S) \in \mathrm{sRNF}_\sigma(R)$.

Example 2. Let $\sigma x = 2x$ and $R(x) = x + 1$. Then $((x+1)/2^n, x^n) \in \mathrm{sRNF}_\sigma(R)$ for all $n \in \mathbb{Z}$. While $R(x)$ is $(x+1)$-orbital, x^n for $n \neq 0$ is not.

Corollary 1. Let $R = \prod_{i=1}^{N} R_i$ be an orbital decomposition of $R \in k(x)^*$, and $(K_i, S_i) \in \mathrm{RNF}_\sigma(R_i)$ for each $i \in [N]$. Then $(\prod_{i=1}^{N} K_i, \prod_{i=1}^{N} S_i) \in \mathrm{RNF}_\sigma(R)$.

Proof: Denote $K = \prod_{i=1}^{N} K_i, S = \prod_{i=1}^{N} S_i$. Clearly $K \cdot \sigma S/S = R$. Suppose that K is not σ-reduced. Then there are i and j such that $\mathrm{num}(K_i)/\mathrm{den}(K_j)$ is not σ-reduced. But by Lemma 5, K_i is p_i-orbital and K_j is p_j-orbital, while p_i/p_j is σ-reduced, so this is impossible. □

5. Existence of strict rational σ-normal forms

To prove existence of RNF_σ for any $R \in k(x)^*$, by Corollary 1 it suffices to do so for p-orbital rational functions of the form

$$R \;=\; \lambda \cdot \frac{\sigma^{a_1} p\, \sigma^{a_2} p\, \cdots\, \sigma^{a_m} p}{\sigma^{b_1} p\, \sigma^{b_2} p\, \cdots\, \sigma^{b_n} p}, \qquad m \leq n, \tag{3}$$

where $\lambda \in k^*$, $a_1 \leq a_2 \leq \cdots \leq a_m$ and $b_1 \leq b_2 \leq \cdots \leq b_n$ are nonnegative integers such that $a_i \neq b_j$ for all $i \in [m], j \in [n]$, and $p \in k[x]$ is irreducible. When p is semi-periodic we will assume w.l.g. that $a_i, b_j < \tilde{\pi}(p)$. If $m > n$ we consider R^{-1} and apply Lemma 1.

Existence of RNF_σ for $R \neq 0$ in a $\Pi\Sigma$-field[6] $k(x)$ over a semi-computable[7] constant field is proved constructively in (Schneider, 2005, Alg. 4.17). For R as in (3), this algorithm yields $(K, S) \in \mathrm{RNF}_\sigma(R)$ with

$$K = \lambda \cdot p^{m-n}, \quad S = \frac{\prod_{j=1}^{m} \prod_{i=0}^{a_j - 1} \sigma^i p}{\prod_{j=1}^{n} \prod_{i=0}^{b_j - 1} \sigma^i p}$$

which, in general, is not strict. In order to minimize the shell S, we need to consider the sRNF_σ's of R. Theorems 1 and 4 below describe strict RNF_σ's of R in (3) by means of injections $f : [m] \to [n]$, similar to those used in (Caruso, 2003, Chapter 4) to estimate the degree of polynomials involved in the Gosper-Form of Zeilberger's algorithm.

Theorem 1. Let R be as in (3). Let $f : [m] \to [n]$ be an injection. Define

$$K_f \;:=\; \frac{\lambda}{\prod_{j \notin f([m])} \sigma^{b_j} p}, \quad S_f \;:=\; \prod_{j=1}^{m} \frac{u_j^{(f)}}{v_j^{(f)}} \tag{4}$$

where

$$u_j^{(f)} \;=\; \begin{cases} \prod_{i=b_{f(j)}}^{a_j - 1} \sigma^i p, & a_j > b_{f(j)}, \\ 1, & \text{otherwise}, \end{cases} \quad v_j^{(f)} \;=\; \begin{cases} 1, & a_j > b_{f(j)}, \\ \prod_{i=a_j}^{b_{f(j)} - 1} \sigma^i p, & \text{otherwise}. \end{cases}$$

Then $(K_f, S_f) \in \mathrm{RNF}_\sigma(R)$. If, in addition, f is increasing (i.e., $f(1) < f(2) < \cdots < f(m)$) and such that $|\{i \in [m];\ b_{f(i)} \leq b_j\}| = |\{i \in [m];\ a_i < b_j\}|$ for each $j \in [n] \setminus f([m])$, then $(K_f, S_f) \in \mathrm{sRNF}_\sigma(R)$.

Proof: K_f is trivially σ-reduced. A simple calculation shows that $\sigma S_f / S_f = \prod_{j=1}^{m} (\sigma^{a_j} p / \sigma^{b_{f(j)}} p)$, hence that $K_f \cdot \sigma S_f / S_f = R$. The second assertion is proved in the same way as in the special case when $\sigma = \mathcal{E}$ (Abramov, Le and Petkovšek, 2003, Lemma 4.2). □

Remark 1. We call (K_f, S_f) defined in (4) the RNF_σ *induced* by f.

---

[6] see (Karr, 1981), (Karr, 1985), or (Schneider, 2001) for definitions

[7] Following (Schneider, 2005), a field F is *semi-computable* if $\mathbb{Z} \subset F$ is recognizable, there is an algorithm for factoring multivariate polynomials over F, and the *orbit problem* (given $f, g \in F^*$, decide if there is an $n \in \mathbb{Z}$ such that $f^n = g$, and if so, find one) is solvable in F.

Lemma 6. Every R of the form (3) has a strict RNF_σ with p-orbital shell.

Proof: We claim that there is an increasing injection $f : [m] \to [n]$ such that

$$|\{i \in [m];\ b_{f(i)} \le b_j\}| = |\{i \in [m];\ a_i < b_j\}| \tag{5}$$

for each $j \in [n] \setminus f([m])$. Indeed, if $m = 0$ then we take $f = \emptyset$ (the empty function). Otherwise we use induction on n.

If $n = 0$ then $m = 0$ as well.

If $n > 0$ we distinguish three cases.

(a) $m = n$: In this case we take $f = \mathrm{id}_{[m]}$.

(b) $0 < m < n$ and $a_m < b_n$: By inductive hypothesis, there exists an increasing injection $g : [m] \to [n-1]$ which satisfies $|\{i \in [m];\ b_{g(i)} \le b_j\}| = |\{i \in [m];\ a_i < b_j\}|$ for each $j \in [n-1] \setminus g([m])$. We define $f : [m] \to [n]$ by $f(i) := g(i)$ for all $i \in [m]$.

(c) $0 < m < n$ and $a_m > b_n$: By inductive hypothesis, there exists an increasing injection $g : [m-1] \to [n-1]$ which satisfies $|\{i \in [m-1];\ b_{g(i)} \le b_j\}| = |\{i \in [m-1];\ a_i < b_j\}|$ for each $j \in [n-1] \setminus g([m-1])$. We define $f : [m] \to [n]$ by $f(i) := g(i)$ for all $i \in [m-1]$ and $f(m) := n$.

In all three cases, it is easily seen that f satisfies (5).

By Theorem 1 it follows that R has a strict RNF_σ of the form (K_f, S_f) where both K_f and S_f are p-orbital. □

Corollary 2. Every $R \in k(x)$ has a strict RNF_σ.

Proof: Take an orbital decomposition $R = \prod_{i=1}^N R_i$. By Lemmas 6 and 1, for each $i \in [N]$ there is a strict RNF_σ (K_i, S_i) of R_i with p_i-orbital kernel and shell. Let $K = \prod_{i=1}^N K_i$, $S = \prod_{i=1}^N S_i$. It is easy to see that $(K, S) \in \mathrm{sRNF}_\sigma(R)$. □

6. Minimality of the kernel

It is shown in (Schneider, 2005, Thm. 4.14) for $\Pi\Sigma$-extensions $k(x)$ of k that $\deg\mathrm{num}(K)$ and $\deg\mathrm{den}(K)$ in (1) are simultaneously minimized iff K is σ-reduced. Here we show this for all unimonomial extensions $k(x)$ of k.

Lemma 7. Let $p \in k[x]$ be irreducible. If $R \in k(x)^*$ is p-orbital and (K, S), $(K', S') \in \mathrm{RNF}_\sigma(R)$, then $\deg\mathrm{num}(K) = \deg\mathrm{num}(K')$ and $\deg\mathrm{den}(K) = \deg\mathrm{den}(K')$.

Proof: From $K \cdot \sigma S/S = K' \cdot \sigma S'/S'$ it follows that

$$\deg\mathrm{num}(K) + \deg\mathrm{den}(K') = \deg\mathrm{num}(K') + \deg\mathrm{den}(K). \tag{6}$$

By Lemma 5, K and K' are p-orbital. Since they are σ-reduced, either $\deg\mathrm{num}(K) = 0$ or $\deg\mathrm{den}(K) = 0$, and either $\deg\mathrm{num}(K') = 0$ or $\deg\mathrm{den}(K') = 0$. Thus we distinguish four cases, and use (6) in each:

1. If $\deg\mathrm{num}(K) = \deg\mathrm{num}(K') = 0$ then $\deg\mathrm{den}(K) = \deg\mathrm{den}(K')$.
2. If $\deg\mathrm{num}(K) = \deg\mathrm{den}(K') = 0$ then $\deg\mathrm{num}(K') + \deg\mathrm{den}(K) = 0$, hence $\deg\mathrm{den}(K) = \deg\mathrm{num}(K') = 0$.

3. If $\deg \mathrm{den}(K) = \deg \mathrm{den}(K') = 0$ then $\deg \mathrm{num}(K) = \deg \mathrm{num}(K')$.
4. If $\deg \mathrm{den}(K) = \deg \mathrm{num}(K') = 0$ then $\deg \mathrm{num}(K) + \deg \mathrm{den}(K') = 0$, hence $\deg \mathrm{num}(K) = \deg \mathrm{den}(K') = 0$. □

Theorem 2. If (K, S) and (K', S') are two RNF_σ's of the same $R \in k(x)^*$, then $\deg \mathrm{num}(K) = \deg \mathrm{num}(K')$ and $\deg \mathrm{den}(K) = \deg \mathrm{den}(K')$.

Proof: Let $K = \prod_{i=1}^N K_i$, $S = \prod_{i=1}^N S_i$, $K' = \prod_{i=1}^N K_i'$, $S' = \prod_{i=1}^N S_i'$ be orbital decompositions of K, S, K', S', respectively, where K_i, S_i, K_i', S_i' are p_i-orbital. As K and K' are σ-reduced, so are K_i and K_i'. Denote $R_i = K_i \cdot \sigma S_i / S_i$ and $R_i' = K_i' \cdot \sigma S_i' / S_i'$. Then R_i and R_i' are p_i-orbital, $(K_i, S_i) \in \mathrm{RNF}_\sigma(R_i)$, and $(K_i', S_i') \in \mathrm{RNF}_\sigma(R_i')$, for all $i \in [N]$. As $\prod_{i=1}^N R_i = \prod_{i=1}^N R_i'$, it follows from Lemma 4 that $R_i \sim R_i'$. By Lemma 7, $\deg \mathrm{num}(K_i) = \deg \mathrm{num}(K_i')$ and $\deg \mathrm{den}(K_i) = \deg \mathrm{den}(K_i')$ for all $i \in [N]$. Hence $\deg \mathrm{num}(K) = \sum_{i=1}^N \deg \mathrm{num}(K_i) = \sum_{i=1}^N \deg \mathrm{num}(K_i') = \deg \mathrm{num}(K')$ and $\deg \mathrm{den}(K) = \sum_{i=1}^N \deg \mathrm{den}(K_i) = \sum_{i=1}^N \deg \mathrm{den}(K_i') = \deg \mathrm{den}(K')$. □

Corollary 3. Let $K, S \in k(x)^*$ and $R = K \cdot \sigma S / S$. Then $(K, S) \in \mathrm{RNF}_\sigma(R)$ iff

$$\deg \mathrm{num}(K) \le \deg \mathrm{num}(K') \quad \text{and} \quad \deg \mathrm{den}(K) \le \deg \mathrm{den}(K') \tag{7}$$

for all $K', S' \in k(x)^*$ such that $R = K' \cdot \sigma S' / S'$.

Proof: Assume that $(K, S) \in \mathrm{RNF}_\sigma(R)$, and let (L, T) be a strict RNF_σ of K' which exists by Corollary 2. Then $(L, S'T) \in \mathrm{RNF}_\sigma(R)$, and Theorem 2 implies that $\deg \mathrm{num}(K) = \deg \mathrm{num}(L)$ and $\deg \mathrm{den}(K) = \deg \mathrm{den}(L)$. By Lemma 2, $\mathrm{num}(L) \mid \mathrm{num}(K')$ and $\mathrm{den}(L) \mid \mathrm{den}(K')$, hence $\deg \mathrm{num}(K) \le \deg \mathrm{num}(K')$ and $\deg \mathrm{den}(K) \le \deg \mathrm{den}(K')$.

Conversely, assume that $(K, S) \notin \mathrm{RNF}_\sigma(R)$. Then K is not σ-reduced, hence there are $p \in k[x] \backslash k$ and $n \in \mathbb{Z} \backslash \{0\}$ such that $p \mid \mathrm{num}(K)$ and $\sigma^n p \mid \mathrm{den}(K)$. Let $K' = K \cdot \sigma^n p / p$ and $S' = S / p^{\sigma, n}$. Then $K' \cdot \sigma S' / S' = K \cdot \sigma S / S = R$, $\deg \mathrm{num}(K') = \deg \mathrm{num}(K) - \deg(p) < \deg \mathrm{num}(K)$, and $\deg \mathrm{den}(K') = \deg \mathrm{den}(K) - \deg(p) < \deg \mathrm{den}(K)$, contrary to (7). □

7. Minimization of the shell

According to Theorem 2, all RNF_σ's of the same $R \in k(x)$ have kernels of the same degrees. In contrast, the degrees of their shells can differ widely. We wish to minimize the shell with respect to one of the many possible weight functions which we define in the following way.

Definition 4. A *weight function* is a monomorphism [8] of the Abelian group $\mathbb{Z} \times \mathbb{Z}$, partially ordered by components [9], into some computable linearly ordered Abelian group L. If w is a weight function, we define the *associated weight W of a rational function $S \in k(x)^*$* by setting $W(S) := w(\deg \mathrm{num}(S), \deg \mathrm{den}(S))$.

[8] see Section 2 for definition

[9] $(a_1, b_1) \le (a_2, b_2)$ iff $a_1 \le a_2$ and $b_1 \le b_2$

Definition 5. Let w be a weight function, and $R \in k(x)$. We call $(K, S) \in \mathrm{RNF}_\sigma(R)$ a *rational* (w, σ)*-canonical form* (an $\mathrm{RCF}_{w,\sigma}$) of R if S is monic, and $W(S)$ is minimal among all RNF_σ's of R.

Proposition 2. Rational (w, σ)-canonical forms exist for all weight functions w and all $R \in k(x)$.

Proof: It follows from Corollary 2 that $\mathrm{RNF}_\sigma(R)$ is not empty. Denote $M = \{(\deg \mathrm{num}(S), \deg \mathrm{den}(S));\ (K, S) \in \mathrm{RNF}_\sigma(R)$ for some $K \in k(x)\}$. By Dickson's lemma (cf. (Cox, Little and O'Shea, 1997, Sec. 2.4)), there is a finite set $B \subseteq M$ such that for any $\alpha \in M$ there is a $\beta \in B$ such that $\beta \leq \alpha$. Let $\mathrm{BNF}_\sigma(R) = \{(K, S) \in \mathrm{RNF}_\sigma(R);\ (\deg \mathrm{num}(S), \deg \mathrm{den}(S)) \in B\}$. Since $\mathrm{BNF}_\sigma(R)$ is finite and non-empty, there exists $(K_0, S_0) \in \mathrm{BNF}_\sigma(R)$ such that $W(S_0)$ is minimal among all $W(S)$ with $(K, S) \in \mathrm{BNF}_\sigma(R)$. Now let (K, S) be any RNF_σ of R. Then by definition of B there is $(K', S') \in \mathrm{BNF}_\sigma(R)$ such that $\deg \mathrm{num}(S') \leq \deg \mathrm{num}(S)$ and $\deg \mathrm{den}(S') \leq \deg \mathrm{den}(S)$, hence that $W(S') \leq W(S)$. But $W(S_0) \leq W(S')$, so $W(S_0) \leq W(S)$. It follows that (K_0, S_0) is an RCF_σ of R. □

In Corollary 4 we will see that they are unique provided that each irreducible factor of R is non-periodic with respect to σ.

Example 3. Take $L = \mathbb{Z} \times \mathbb{Z}$, ordered lexicographically by $(a_1, b_1) \leq_{\mathrm{lex}} (a_2, b_2)$ iff $a_1 < a_2$, or $a_1 = a_2$ and $b_1 \leq b_2$. Our foremost examples are the following four weight functions:

(1) $w_1(n, d) = (d, n)$,
(2) $w_2(n, d) = (n, d)$,
(3) $w_3(n, d) = (n + d, d)$,
(4) $w_4(n, d) = (n + d, n)$.

Instead of $\mathrm{RCF}_{w_i,\sigma}$ we write $\mathrm{RCF}_{i,\sigma}$, for $i = 1, 2, 3, 4$. Thus $(K, S) \in \mathrm{RNF}_\sigma(R)$ with monic S is an

(1) $\mathrm{RCF}_{1,\sigma}$ of R iff $\deg \mathrm{den}(S)$ is minimal among all RNF_σ's of R, and under this condition, $\deg \mathrm{num}(S)$ is minimal;
(2) $\mathrm{RCF}_{2,\sigma}$ of R iff $\deg \mathrm{num}(S)$ is minimal among all RNF_σ's of R, and under this condition, $\deg \mathrm{den}(S)$ is minimal;
(3) $\mathrm{RCF}_{3,\sigma}$ of R iff $\deg \mathrm{num}(S) + \deg \mathrm{den}(S)$ is minimal among all RNF_σ's of R, and under this condition, $\deg \mathrm{den}(S)$ is minimal;
(4) $\mathrm{RCF}_{4,\sigma}$ of R iff $\deg \mathrm{num}(S) + \deg \mathrm{den}(S)$ is minimal among all RNF_σ's of R, and under this condition, $\deg \mathrm{num}(S)$ is minimal.

From these definitions and from Lemma 1 it follows that for any $R \in k(x)^*$, (K, S) is an $\mathrm{RCF}_{2,\sigma}$ of R iff (K^{-1}, S^{-1}) is an $\mathrm{RCF}_{1,\sigma}$ of R^{-1}, and (K, S) is an $\mathrm{RCF}_{4,\sigma}$ of R iff (K^{-1}, S^{-1}) is an $\mathrm{RCF}_{3,\sigma}$ of R^{-1}.

More generally, $w(n, d) = (a_1 n + b_1 d, a_2 n + b_2 d)$ is a weight function for any nonnegative integers a_1, b_1, a_2, b_2 such that $a_1 b_2 \neq a_2 b_1$. Note that it suffices to consider weight functions of the form $w'(n, d) = (a_1 n + b_1 d, n)$ and $w''(n, d) = (a_1 n + b_1 d, d)$ because $w(n, d)$ attains its minimum at the same point as $w'(n, d)$ (resp. $w''(n, d)$) when $a_1 b_2 < a_2 b_1$ (resp. $a_1 b_2 > a_2 b_1$).

Remark 2. In (Abramov, Le and Petkovšek, 2003), the forms $\mathrm{RCF}_{1,\sigma}$, $\mathrm{RCF}_{2,\sigma}$ $\mathrm{RCF}_{3,\sigma}$, and $\mathrm{RCF}_{4,\sigma}$ are denoted by RCF_1, RCF_2, RCF_1^*, and RCF_2^*, respectively, in the special case when $\sigma = \mathcal{E}$. Note that the definitions of RCF_1 and RCF_2 given in (Abramov, Le and Petkovšek, 2003) are different from those of $\mathrm{RCF}_{1,\sigma}$ and $\mathrm{RCF}_{2,\sigma}$, respectively, but are equivalent to them.

Example 4. Let σ be *any* automorphism of $k[x]$. Assume that $p \in k[x]$ is a non-periodic polynomial of degree 1, and let

$$R = \frac{p\ \sigma^3 p\ \sigma^{10} p\ \sigma^{16} p\ \sigma^{21} p}{\sigma p\ \sigma^2 p\ \sigma^6 p\ \sigma^7 p\ \sigma^{12} p\ \sigma^{13} p\ \sigma^{19} p\ \sigma^{20} p}.$$

Consider the following four strict RNF_σ's of R:

$$\begin{aligned}
K_1 &= \frac{1}{\sigma^6 p\ \sigma^{12} p\ \sigma^{19} p}, &\quad S_1 &= \frac{\sigma^2 p\ \sigma^7 p\ \sigma^8 p\ \sigma^9 p\ \sigma^{13} p\ \sigma^{14} p\ \sigma^{15} p\ \sigma^{20} p}{p};\\
K_2 &= \frac{1}{\sigma^2 p\ \sigma^7 p\ \sigma^{13} p}, &\quad S_2 &= \frac{\sigma^{20} p}{p\ \sigma^3 p\ \sigma^4 p\ \sigma^5 p\ \sigma^{10} p\ \sigma^{11} p\ \sigma^{16} p\ \sigma^{17} p\ \sigma^{18} p};\\
K_3 &= \frac{1}{\sigma^6 p\ \sigma^7 p\ \sigma^{19} p}, &\quad S_3 &= \frac{\sigma^2 p\ \sigma^{13} p\ \sigma^{14} p\ \sigma^{15} p\ \sigma^{20} p}{p\ \sigma^{10} p\ \sigma^{11} p};\\
K_4 &= \frac{1}{\sigma^6 p\ \sigma^7 p\ \sigma^{13} p}, &\quad S_4 &= \frac{\sigma^2 p\ \sigma^{20} p}{p\ \sigma^{10} p\ \sigma^{11} p\ \sigma^{16} p\ \sigma^{17} p\ \sigma^{18} p}.
\end{aligned}$$

The weights W_1, W_2, W_3, W_4 of S_1, S_2, S_3, S_4 are given in the following table:

	W_1	W_2	W_3	W_4
S_1	$(\mathbf{1},\mathbf{8})$	$(8,1)$	$(9,1)$	$(9,8)$
S_2	$(9,1)$	$(\mathbf{1},\mathbf{9})$	$(10,9)$	$(10,1)$
S_3	$(3,5)$	$(5,3)$	$(\mathbf{8},\mathbf{3})$	$(8,5)$
S_4	$(6,2)$	$(2,6)$	$(8,6)$	$(\mathbf{8},\mathbf{2})$

In each column, the lexicographically minimum weight is shown in boldface. It can be verified that $((\sigma\lambda_i/\lambda_i)K_i, S_i/\lambda_i)$ where $\lambda_i = \mathrm{lc}\,(S_i)$ is an $\mathrm{RCF}_{i,\sigma}$ of R, for $i = 1, 2, 3, 4$.

Theorem 3. Any $\mathrm{RCF}_{w,\sigma}$ of R is strict.

Proof: Let (K, S) be an RNF_σ of R which is not strict. We distinguish three cases.

a) $\deg\gcd(\mathrm{num}(K), \mathrm{num}(S)) > 0$: Write $\mathrm{num}(K) = rg$, $\mathrm{num}(S) = ug$ where $g = \gcd(\mathrm{num}(K), \mathrm{num}(S))$. We claim that

$$(K', S') := \left(\frac{r \cdot \sigma g}{\mathrm{den}(K)}, \frac{u}{\mathrm{den}(S)}\right) \in \mathrm{RNF}_\sigma(R).$$

Indeed,

$$\frac{r\cdot\sigma g}{\mathrm{den}(K)}\cdot\frac{\sigma u}{\mathrm{den}(\sigma S)}\cdot\frac{\mathrm{den}(S)}{u} \;=$$
$$= \;\frac{rg}{\mathrm{den}(K)}\cdot\frac{\sigma(ug)}{\mathrm{den}(\sigma S)}\cdot\frac{\mathrm{den}(S)}{ug} \;=\; K\cdot\frac{\sigma S}{S} \;=\; R,$$

and $r\cdot\sigma g/\mathrm{den}(K)$ is σ-reduced because $r \mid \mathrm{num}(K)$, $\sigma g \mid \mathrm{num}(\sigma K)$, and K is σ-reduced. But then (K,S) is not an $\mathrm{RCF}_{w,\sigma}$ of R because $\deg\mathrm{num}(S') < \deg\mathrm{num}(S)$ and $\deg\mathrm{den}(S') = \deg\mathrm{den}(S)$, so $W(S') < W(S)$.

b) $\deg\gcd(\mathrm{num}(K),\mathrm{den}(\sigma S)) > 0$: Write $\mathrm{num}(K) = rg$, $\mathrm{den}(\sigma S) = \sigma v\cdot g$ where $g = \gcd(\mathrm{num}(K),\mathrm{den}(\sigma S))$. Similarly as in a), we can verify that

$$(K',S') := \left(\frac{r\cdot\sigma^{-1}g}{\mathrm{den}(K)},\; \frac{\mathrm{num}(S)}{v}\right) \in \mathrm{RNF}_\sigma(R).$$

Thus, again (K,S) is not an $\mathrm{RCF}_{w,\sigma}$ of R because $\deg\mathrm{num}(S') = \deg\mathrm{num}(S)$ and $\deg\mathrm{den}(S') < \deg\mathrm{den}(S)$, hence $W(S') < W(S)$.

c) $\deg\gcd(\mathrm{den}(K),\mathrm{num}(\sigma S)\mathrm{den}(S)) > 0$: By Lemma 1, (K^{-1},S^{-1}) is a non-strict RNF_σ of R^{-1} such that $\deg\gcd(\mathrm{num}(K^{-1}),\mathrm{den}(\sigma S^{-1})\cdot\mathrm{num}(S^{-1})) > 0$. By a) and b), (K^{-1},S^{-1}) is not an $\mathrm{RCF}_{w,\sigma}$ of R^{-1}, so by Lemma 1, (K,S) is not an $\mathrm{RCF}_{w,\sigma}$ of R. □

8. Computing rational (w,σ)-canonical forms

8.1. Algorithmic prerequisites

A rational (w,σ)-canonical form for a given $R\in k(x)$ and a given weight function $w:\mathbb{Z}\times\mathbb{Z}\to L$ can be computed by the following algorithm:

Algorithm $\mathrm{RCF}_{w,\sigma}$

(1) Compute an orbital decomposition $\prod_{i=1}^N R_i$ of R.
(2) For each $i\in[N]$, compute a rational (w,σ)-canonical form (K_i,S_i) of R_i.
(3) Compute $K=\prod_{i=1}^N K_i$, $S=\prod_{i=1}^N S_i$, and $\lambda = \mathrm{lc}\,(S)$.
(4) Return $((\sigma\lambda/\lambda)K,\; S/\lambda)$.

Proof of correctness: Note that $(K,S)\in\mathrm{RNF}_\sigma(R)$ by Corollary 1, hence the same is true of $((\sigma\lambda/\lambda)\cdot K,\; S/\lambda)$. Now take any $(K',S')\in\mathrm{RNF}_\sigma(R)$, and let $K'=\prod_{i=1}^M K_i'$, $S'=\prod_{i=1}^M S_i'$ be orbital decompositions such that $M\ge N$ and K_i, S_i, K_i', S_i' are p_i-orbital for each $i\in[N]$. Suppose that K_i' is not σ-reduced for some $i\in[M]$. Since K' is σ-reduced, there exists some $j\in[M]$ such that $\deg\gcd(\mathrm{num}(K_i'),\mathrm{den}(K_j')) > 0$ or $\deg\gcd(\mathrm{den}(K_i'),\mathrm{num}(K_j')) > 0$. But this is impossible as K_i' is p_i-orbital and K_j' is p_j-orbital, while p_i/p_j is σ-reduced. Hence $(K_i',S_i')\in\mathrm{RNF}_\sigma(R_i')$ where $R_i' = K_i'\cdot\sigma S_i'/S_i'$, for all $i\in[M]$. Since $\prod_{i=1}^M R_i' = K'\cdot\sigma S'/S' = R$ is another orbital decomposition of R, Lemma 4 implies that $R_i'\sim R_i$ for all $i\in[M]$. Therefore for each $i\in[M]$ there is some $\lambda_i\in k^*$ such that $(\lambda_i K_i', S_i')\in\mathrm{RNF}_\sigma(R_i)$. Since (K_i,S_i) is an $\mathrm{RCF}_{w,\sigma}$ of R_i, it follows that $W(S_i)\le W(S_i')$ for all $i\in[M]$. By additivity of w,

$$
\begin{aligned}
\sum_{i=1}^{M} W(S_i) &= \sum_{i=1}^{M} w(\deg \operatorname{num}(S_i), \deg \operatorname{den}(S_i)) \\
&= w\left(\sum_{i=1}^{M} \deg \operatorname{num}(S_i), \sum_{i=1}^{M} \deg \operatorname{den}(S_i)\right) \\
&= w\left(\deg \prod_{i=1}^{M} \operatorname{num}(S_i), \deg \prod_{i=1}^{M} \operatorname{den}(S_i)\right) \\
&= w(\deg \operatorname{num}(S), \deg \operatorname{den}(S)) \;=\; W(S),
\end{aligned}
$$

where the fourth equality follows from the fact that S_i is p_i-orbital, S_j is p_j-orbital, and p_i/p_j is σ-reduced for all $i, j \in [M]$. In the same way we obtain

$$\sum_{i=1}^{M} W(S'_i) \;=\; w(\deg \operatorname{num}(S'), \deg \operatorname{den}(S')) \;=\; W(S').$$

Hence $W(S) \leq W(S')$ for all $(K', S') \in \mathrm{RNF}_\sigma(R)$. Together with $\mathrm{lc}\,(S/\lambda) = 1$ this implies that $((\sigma\lambda/\lambda)K,\ S/\lambda)$ is an $\mathrm{RCF}_{w,\sigma}$ of R. □

It remains to explain how to perform steps 1 and 2 of Algorithm $\mathrm{RCF}_{w,\sigma}$. In step 1, an orbital decomposition of R can be computed [10] if we have

(1) an algorithm PF for factoring polynomials in $k[x]$;
(2) an algorithm SE which, given irreducible $p, q \in k[x] \setminus k$, decides if there is an $n \in \mathbb{Z}$ such that $p \sim \sigma^n q$, and if so, computes one.

These two conditions are satisfied, e.g., when $k(x)$ is a $\Pi\Sigma$-field over a semi-computable constant field (Schneider, 2005, Thm. 2.11).

Step 2 of Algorithm $\mathrm{RCF}_{w,\sigma}$ requires the computation of an $\mathrm{RCF}_{w,\sigma}$ of a p-orbital rational function R. An algorithm for doing this via reduction to the assignment problem is the main result of the paper and is described in Sections 8.2, 8.3 and 8.4. However, this algorithm assumes that the value of $\tilde{\pi}(p)$ is known. Therefore we sketch here an algorithm which computes the semi-period of an irreducible polynomial $p \in k[x] \setminus k$, provided that we have

(1) an algorithm LDE which, given $a \in k^*$ and $b \in k$, decides if there is a $w \in k$ such that $\sigma w = aw + b$, and if so, computes one;
(2) an algorithm SR which, given $a \in k^*$, decides if a is a σ-radical [11];
(3) an algorithm HSO which, given $\alpha \in k^*$, computes a nonnegative generator of the ideal $J(\alpha) := \{n \in \mathbb{Z};\ \alpha^{\sigma,n} = 1\} \subseteq \mathbb{Z}$.

Using these algorithms, we can proceed as follows:

Run LDE on a and b where $\sigma x = ax + b$. If there is no $w \in k$ such that $\sigma w = aw + b$, Theorem 1 of (Karr, 1981) implies that there is no $q \in k[x] \setminus k$ such that $\sigma q/q \in k^*$. However, if $\tilde{\pi}(p) > 0$ then $t(p) \in k[x]\setminus k$ and Proposition 1(ii) implies that $\sigma t(p)/t(p) \in k^*$. Hence $\tilde{\pi}(p) = 0$.

[10] cf. (Bronstein, 2000, Lemma 15(i) and its proof)
[11] $a \in k$ is a *σ-radical* if $a^n = \sigma\lambda/\lambda$ for some $n \in \mathbb{Z}$, $n > 0$, and $\lambda \in k^*$

If $w \in k$ satisfies $\sigma w = aw + b$, introduce a new variable $y = x - w$. Then $\sigma y = ay$, so it suffices to consider the case $b = 0$.

Run SR on a. If a is not a σ-radical, then Theorems 2 and 9(d) of (Karr, 1981) imply that $\tilde{\pi}(p) \in \{0, 1\}$. Hence: if $\sigma p \sim p$ then $\tilde{\pi}(p) = 1$ else $\tilde{\pi}(p) = 0$.

So let $\sigma x = ax$ where a is a σ-radical. Assume that $\sigma^n p = \lambda p$ for some $n > 0$ and $\lambda \in k^*$. Write $p(x) = \sum_{i=0}^{r} c_i x^i$ where $r > 0$. If $c_0 = 0$ then $r = 1$ (since p is irreducible), hence $\tilde{\pi}(p) = 1$. Otherwise (since $\tilde{\pi}(\lambda p) = \tilde{\pi}(p)$ for any $\lambda \in k^*$) assume w.l.g. that $c_0 = 1$. Then $\sigma^n c_i \cdot (a^{\sigma,n})^i = \lambda c_i$ for all $i \in [r]$ and also for $i = 0$. This yields $\lambda = 1$ and

$$\left(a^i \frac{\sigma c_i}{c_i}\right)^{\sigma,n} = 1$$

for all $i \in [r]$ such that $c_i \neq 0$. Run HSO on $\alpha_i := a^i \cdot \sigma c_i / c_i$ for all $i \in [r]$ such that $c_i \neq 0$, and let n_i be the generators of the corresponding ideals $J(\alpha_i)$. Then, clearly, $\tilde{\pi}(p) = \mathrm{lcm}\{n_i;\ i \in [r], c_i \neq 0\}$.

Example 5. Let σ be a k-automorphism of $k(x)$ where $\sigma x = ax$ and $a \in k^*$ is a primitive m-th root of unity. Then $(a^i \cdot \sigma c_i/c_i)^{\sigma,n} = 1 \ \Leftrightarrow\ a^{in} = 1 \ \Leftrightarrow\ m \,|\, (in) \ \Leftrightarrow\ (m/\gcd(m,i)) \,|\, n$. Hence $n_i = m/\gcd(m,i)$ and

$$\tilde{\pi}(p) = \mathrm{lcm}\left\{\frac{m}{\gcd(m,i)};\ i \in [r], c_i \neq 0\right\}.$$

So we can compute $\tilde{\pi}(p)$ if we know m.

Example 6. Let σ be *any* automorphism of $k(x)$ where $\sigma x = x$ (i.e., $a = 1$ and x is an explicit new constant). Define the *period* $\pi(c)$ of $c \in k^*$ by

$$\pi(c) := \begin{cases} 0, & \text{if } \ \sigma^n c \neq c \ \text{ for all } n \geq 1, \\ \min\{n \geq 1;\ \sigma^n c = c\}, & \text{otherwise.} \end{cases}$$

Then $(a^i \cdot \sigma c_i/c_i)^{\sigma,n} = 1 \ \Leftrightarrow\ \sigma^n c_i = c_i \ \Leftrightarrow\ \pi(c_i) \,|\, n$, hence $n_i = \pi(c_i)$ and

$$\tilde{\pi}(p) = \mathrm{lcm}\left\{\pi(c_i);\ i \in [r], c_i \neq 0\right\}.$$

So we can compute $\tilde{\pi}(p)$ if we can compute $\pi(c)$ for each $c \in k^*$.

Algorithms LDE and SR exist, e.g., when k is a $\Pi\Sigma$-field over a σ-computable [12] constant field (see (Karr, 1981, Section 3); (Schneider, 2005, Thm. 3.2)). If also $k(t)$ is a $\Pi\Sigma$-extension of k then $\tilde{\pi}(p) \in \{0, 1\}$ by (Karr, 1981, Thm. 9(d)), hence algorithm HSO is not needed in this case. Furthermore, if $\tilde{\pi}(p) = 1$ then R in (3) is σ-reduced, so $(R, 1)$ is trivially an $\mathrm{RCF}_{w,\sigma}$ of R for any weight function w, and the algorithm of Section 8.4 is not needed either. Incidentally, a k-automorphism of $k[x]$ such that $\tilde{\pi}(p) \in \{0, 1\}$ for each irreducible $p \in k[x] \setminus k$ is called *aperiodic* in (Bauer and Petkovšek, 1999).

[12] Following (Schneider, 2005), a field F is *σ-computable* if it is semi-computable (see footnote 7) and the *generalized orbit problem* (given $f_1, \ldots, f_r \in F^*$, find a basis for the $\mathbb{Z}$-module $\{(n_1, \ldots, n_r);\ f_1^{n_1} \cdots f_r^{n_r} = 1\} \subseteq \mathbb{Z}^r$) is solvable in F.

8.2. The assignment problem

Let R be as in (3). Theorem 3 tells us that in order to find an $\mathrm{RCF}_{w,\sigma}$ of R, we need to minimize $W(S)$ over all $(K,S) \in \mathrm{sRNF}_\sigma(R)$. Up to a factor from k, the kernel K is determined by some increasing injection $f : [m] \to [n]$. The shell S satisfies the first-order σ-difference equation $\sigma S = (R/K) \cdot S$, so once the kernel is fixed, the shell is determined up to a factor $T \in k(x)$ such that $\sigma T \sim T$ (Theorem 4). If, in addition, (K,S) is an $\mathrm{RCF}_{w,\sigma}$ of R, then $T \sim t(p)^\xi$ where $t(p)$ is the total span of p, and $\xi \in \mathbb{Z}$ (Theorem 5).

Theorem 4. Let R be as in (3), and let $(K,S) \in \mathrm{sRNF}_\sigma(R)$. Then there is $T \in k(x)^*$ such that $\sigma T \sim T$, and an increasing injection $f : [m] \to [n]$ such that $K \sim K_f$ and $S = TS_f$, where (K_f, S_f) is the RNF_σ of R induced by f.

Proof: By Lemma 5, K is p-orbital. As it is σ-reduced, either $\mathrm{num}(K) \sim 1$ or $\mathrm{den}(K) \sim 1$. But $\deg \mathrm{num}(K) - \deg \mathrm{den}(K) = (m-n) \deg p \le 0$, hence $\mathrm{num}(K) \sim 1$ and $\deg \mathrm{den}(K) = (n-m) \deg p$. By Lemma 2, $\mathrm{den}(K) \mid \prod_{j=1}^n \sigma^{b_j} p$. Let $j_1 < \cdots < j_m$ be such that $\prod_{j=1}^n \sigma^{b_j} p / \mathrm{den}(K) \sim \prod_{i=1}^m \sigma^{b_{j_i}} p$. Define $f(i) := j_i$. Then $f : [m] \to [n]$ is an increasing injection and $\mathrm{den}(K) \sim \prod_{j \in [n] \setminus f([m])} \sigma^{b_j} p$, hence $K \sim K_f$ and $R \sim K_f \cdot \sigma S / S$. Let $T := S/S_f$. By Theorem 1, $R = K_f \cdot \sigma S_f / S_f$. Hence $\sigma T \sim T$. □

Lemma 8. Let $\prod_{i=1}^m T_i$ be an orbital decomposition of $T \in k(x)^*$. If $\sigma T \sim T$ then $\sigma T_i \sim T_i$ for all $i \in [m]$.

Proof: Clearly $\prod_{i=1}^m (\sigma T_i / T_i)$ is an orbital decomposition of some $\lambda \in k^*$, and so is $\lambda \cdot 1 \cdot 1 \cdots 1$. By Lemma 4, $\sigma T_i / T_i \sim 1$ for all $i \in [m]$. □

Lemma 9. Let $T \in k(x)$ be such that $\sigma T \sim T$. Then $\sigma \mathrm{num}(T) \sim \mathrm{num}(T)$ and $\sigma \mathrm{den}(T) \sim \mathrm{den}(T)$.

Proof: From the assumption it follows that $\sigma \mathrm{num}(T) \cdot \mathrm{den}(T) \sim \sigma \mathrm{den}(T) \cdot \mathrm{num}(T)$. Hence $\sigma \mathrm{num}(T) \mid \mathrm{num}(T)$, $\mathrm{den}(T) \mid \sigma \mathrm{den}(T)$, $\sigma \mathrm{den}(T) \mid \mathrm{den}(T)$, and $\mathrm{num}(T) \mid \sigma \mathrm{num}(T)$, proving the claim. □

Proposition 3. Let $p \in k[x]$ be irreducible, and let $P \in k[x] \setminus \{0\}$ be a p-orbital polynomial such that $\sigma P \sim P$. Then $P \sim t(p)^\xi$ for some $\xi \in \mathbb{Z}$, $\xi \ge 0$.

Proof: Assume that $\sigma^j p \mid P$ for some $j \ge 0$. Then $\sigma^{j+1} p \mid \sigma P$. From $\sigma P \sim P$ it follows that $\sigma^{j+1} p \mid P$. By induction, $\sigma^i p \mid P$ for all $i \ge j$. If $\tilde{\pi}(p) = 0$ this is impossible, so $P \in k^*$. If $\tilde{\pi}(p) > 0$ we use induction on $\deg P$. If $\deg P = 0$ then $P \sim t(p)^0$. Otherwise $P = t(p) P'$ where $P' \in k[x] \setminus \{0\}$, $\sigma P' \sim P'$, and $\deg P' < \deg P$. By inductive hypothesis, $P' \sim t(p)^{\xi'}$, hence $P \sim t(p)^{\xi'+1}$. □

Theorem 5. Let R be as in (3), and let (K,S) be an $\mathrm{RCF}_{w,\sigma}$ of R for some weight function w. Then there are an increasing injection $f : [m] \to [n]$ and $\xi \in \mathbb{Z}$ such that $K \sim K_f$ and $S \sim t(p)^\xi S_f$ where (K_f, S_f) is the RNF_σ of R induced by f.

Proof: By Theorem 3, (K,S) is strict. By Theorem 4, there are $T \in k(x)^*$ and an increasing injection $f : [m] \to [n]$ such that $\sigma T \sim T$, $K \sim K_f$, and $S = TS_f$. Let $\prod_{i=1}^j T_i$ be an orbital decomposition of T where each T_i is p_i-orbital and $p_1 = p$. Write $T' = T/T_1$. By Lemma 8, $\sigma T_1 \sim T_1$. By Lemma 9 and Proposition 3, $T_1 \sim t(p)^\xi$ for some $\xi \in \mathbb{Z}$, hence $T \sim t(p)^\xi T'$ and $S \sim t(p)^\xi T' S_f$. From $\mathrm{num}(t(p)^\xi T' S_f) = \mathrm{num}(T')\mathrm{num}(t(p)^\xi S_f)$ it follows that $\deg \mathrm{num}(S) = \deg \mathrm{num}(t(p)^\xi T' S_f) = \deg \mathrm{num}(T') + \deg \mathrm{num}(t(p)^\xi S_f) \geq \deg \mathrm{num}(t(p)^\xi S_f)$. Similarly, $\deg \mathrm{den}(S) = \deg \mathrm{den}(T') + \deg \mathrm{den}(t(p)^\xi S_f) \geq \deg \mathrm{den}(t(p)^\xi S_f)$, hence $W(S) \geq W(t(p)^\xi S_f)$. But (K, S) is an $\mathrm{RCF}_{w,\sigma}$ of R and $(K_f/\mu(p)^\xi, t(p)^\xi S_f)$ is an RNF_σ of R, so $W(S) = W(t(p)^\xi S_f)$. This implies that $\deg \mathrm{num}(S) = \deg \mathrm{num}(t(p)^\xi S_f)$ and $\deg \mathrm{den}(S) = \deg \mathrm{den}(t(p)^\xi S_f)$. Hence $\deg \mathrm{num}(T') = \deg \mathrm{den}(T') = 0$, $T' \sim 1$, and $S \sim t(p)^\xi S_f$. □

Now we will reduce the problem of finding an $\mathrm{RCF}_{w,\sigma}$ of R as in (3) to an instance of the following combinatorial optimization problem:

Assignment problem

INPUT: a computable linearly ordered Abelian group L;
a cost matrix $[c_{i,j}]_{i \in [m], j \in [n]}$ where $c_{i,j} \in L$ and $m \leq n$;
OUTPUT: an injection $f : [m] \to [n]$ such that its cost $c(f) = \sum_{i=1}^m c_{i,f(i)}$ is minimal.

The assignment problem can be solved in time polynomial in $\max\{m, n\}$ by linear programming techniques (see, e.g., (Papadimitriou and Steiglitz, 1982)), hence an $\mathrm{RCF}_{w,\sigma}$ of R can be computed efficiently for arbitrary $R \in k(x)$ from the orbital decomposition of R. In order to reduce the computation of $\mathrm{RCF}_{w,\sigma}$ to the assignment problem, we need to distinguish two cases – according to whether p is non-periodic or semi-periodic.

Remark 3. In standard specifications of the assignment problem, L is a computable subgroup (such as $\mathbb{Z}$ or $\mathbb{Q}$) of the linearly ordered additive group $\mathbb{R}$. Allowing more general groups L – as we do above – does not affect algorithms for solving the assignment problem, provided that subroutines for computing addition and comparison of elements of L are available (which is implied by computability of L). Nevertheless, if one wishes to model this more general situation in a standard setting, one can often do so quite easily. For instance, if $L = \mathbb{Z} \times \mathbb{Z}$ ordered lexicographically as in Example 3, one can replace each weight $c_{i,j} = (a_{i,j}, b_{i,j}) \in \mathbb{Z} \times \mathbb{Z}$ where $a_{i,j}, b_{i,j} \geq 0$, by the weight $a_{i,j}N + b_{i,j} \in \mathbb{Z}$ where $N = \max\left\{\sum_{i=1}^m \max_{j \in [n]} a_{i,j}, \sum_{i=1}^m \max_{j \in [n]} b_{i,j}\right\} + 1$. Since the cost of an injection $f : [m] \to [n]$ does not exceed $(N-1, N-1)$, this mapping (representing evaluation of 2-digit numbers in base N) faithfully embeds the original lexicographic order in $\mathbb{Z} \times \mathbb{Z}$ into the usual order in $\mathbb{Z}$.

8.3. The non-periodic case

In this subsection, $p \in k[x]$ is an irreducible non-periodic polynomial, hence $t(p) = 1$. We denote $\delta := \deg p$. If (K, S) is an $\mathrm{RCF}_{w,\sigma}$ of R, then by Theorem 5, $K \sim K_f$ and $S \sim S_f$ where $f : [m] \to [n]$ is an increasing injection. Thus it only remains to define a cost matrix $[c_{i,j}]_{i\in[m],j\in[n]}$ so that the solution f of the associated assignment problem will also minimize the weight of S_f.

Definition 6. Let R be as in (3), let $f:[m]\to[n]$ be an injection, and let w be a weight function. We define the *weight of* f as $w(f):=w(d_1,d_2)$ where

$$\begin{aligned} d_1 &= \delta \sum_{a_j>b_{f(j)}} (a_j - b_{f(j)}), \\ d_2 &= \delta \sum_{a_j<b_{f(j)}} (b_{f(j)} - a_j). \end{aligned}$$

Lemma 10. Let $f:[m]\to[n]$ be an injection, and let w be a weight function. Then $W(S_f)\le w(f)$. If f is increasing, then $W(S_f)=w(f)$.

Proof: From (4), $\deg\operatorname{num}(S_f)\le\sum_{j=1}^m \deg u_j^{(f)} = d_1$ and $\deg\operatorname{den}(S_f)\le\sum_{j=1}^m \deg v_j^{(f)} = d_2$, hence $W(S_f)=w(\deg\operatorname{num}(S_f),\deg\operatorname{den}(S_f))\le w(d_1,d_2)=w(f)$. If f is increasing then we claim that $u_{j_1}\perp v_{j_2}$ for all $j_1,j_2\in[m]$. To prove this, assume that $q\in k[x]$ is an irreducible common factor of u_{j_1} and v_{j_2}. By definition of $u_j^{(f)}$ and $v_j^{(f)}$ it follows that $a_{j_1}>b_{f(j_1)}$, $a_{j_2}<b_{f(j_2)}$, and there are i_1, i_2 such that $q\sim\sigma^{i_1}p$ where $b_{f(j_1)}\le i_1<a_{j_1}$ and $q\sim\sigma^{i_2}p$ where $a_{j_2}\le i_2<b_{f(j_2)}$. From $\sigma^{i_1}p\sim\sigma^{i_2}p$ we get $\sigma^{|i_1-i_2|}p\sim p$. As p is non-periodic, this implies that $i_1=i_2$. Hence $a_{j_2}<a_{j_1}$ which implies that $j_2<j_1$, and $b_{f(j_1)}<b_{f(j_2)}$ which implies that $f(j_1)<f(j_2)$. As f is increasing, it follows that $j_1<j_2$, a contradiction. Thus in this case $\deg\operatorname{num}(S_f)=\sum_{j=1}^m\deg u_j^{(f)}=d_1$ and $\deg\operatorname{den}(S_f)=\sum_{j=1}^m\deg v_j^{(f)}=d_2$, whence $W(S_f)=w(f)$. □

Theorem 6. Let R be as in (3), w a weight function, $g:[m]\to[n]$ an injection of minimum weight, and let (K_g,S_g) be the RNF_σ of R induced by g. Then $((\sigma\lambda/\lambda)K_g, S_g/\lambda)$, where $\lambda=\operatorname{lc}(S_g)$, is an $\mathrm{RCF}_{w,\sigma}$ of R.

Proof: Let (K,S) be an $\mathrm{RCF}_{w,\sigma}$ of R. By Theorem 5, there is an increasing injection $f:[m]\to[n]$ such that $K\sim K_f$ and $S\sim S_f$. Then by Lemma 10, $W(S)=W(S_f)=w(f)\ge w(g)\ge W(S_g)$. Hence $W(S_g)=W(S)$ is minimal among all RNF_σ's of R, and the assertion follows because $\operatorname{lc}(S_g/\lambda)=1$. □

Theorem 6 shows that to compute an $\mathrm{RCF}_{w,\sigma}$ of R where R is as in (3), it suffices to find an injection $f:[m]\to[n]$ of minimum weight. This can be done by solving the assignment problem with the cost matrix

$$c_{i,j} = \begin{cases} w(a_i-b_j,0), & a_i>b_j, \\ w(0,b_j-a_i), & a_i<b_j. \end{cases} \tag{8}$$

Indeed, the cost $c(f)$ of f is then given by

$$c(f) = \sum_{a_i>b_{f(i)}} w(a_i-b_{f(i)},0) + \sum_{a_i<b_{f(i)}} w(0,b_{f(i)}-a_i) = w\left(\frac{d_1}{\delta},\frac{d_2}{\delta}\right).$$

As w is additive, $\delta \cdot c(f) = w(d_1, d_2) = w(f)$, hence injections of minimum cost are also injections of minimum weight, and vice versa.

Example 7. Let $\sigma = \mathcal{Q}$ and assume that q is transcendental over $\mathbb{Q} \subseteq k$. Let

$$p_1(x) = q^{-3}\,x + q^2, \qquad p_2(x) = q^{-4}\,x + q - q^{-1}$$

and $R = R_1 R_2$ where

$$R_1 = \frac{\sigma^3 p_1\ \sigma^5 p_1}{p_1\ \sigma p_1^2\ \sigma^9 p_1}, \qquad R_2 = \frac{p_2\ \sigma p_2\ \sigma^6 p_2\ \sigma^{15} p_2}{\sigma^3 p_2\ \sigma^5 p_2}.$$

Notice that because q is transcendental over $\mathbb{Q}$, p_1 and p_2 are non-periodic, and p_1/p_2 is σ-reduced. Since p_1 and p_2 are irreducible, $R_1 R_2$ is an orbital decomposition of R. For $i = 1, 2, 3, 4$, the algorithm suggested by Theorem 6 finds that $((\sigma\lambda_i/\lambda_i)K_i, S_i/\lambda_i)$ where $\lambda_i = \mathrm{lc}\,(S_i)$ and

$$K_1 = \frac{p_2\ \sigma p_2}{p_1\ \sigma^9 p_1}, \qquad S_1 = \sigma p_1\ \sigma^2 p_1\ \sigma^5 p_2\ \textstyle\prod_{i=1}^{4} \sigma^i p_1\ \prod_{j=3}^{14} \sigma^j p_2;$$

$$K_2 = \frac{\sigma^6 p_2\ \sigma^{15} p_2}{p_1\ \sigma p_1}, \qquad S_2 = \frac{\sigma p_1\ \sigma^2 p_1}{\sigma p_2\ \sigma^2 p_2\ \prod_{i=5}^{8} \sigma^i p_1\ \prod_{j=0}^{4} \sigma^j p_2};$$

$$K_3 = \frac{p_2\ \sigma^{15} p_2}{p_1\ \sigma^9 p_1}, \qquad S_3 = \frac{\sigma p_1\ \sigma^2 p_1\ \sigma^5 p_2\ \prod_{i=1}^{4} \sigma^i p_1}{\sigma p_2\ \sigma^2 p_2};$$

$$K_4 = \frac{p_2\ \sigma^{15} p_2}{p_1\ \sigma p_1}, \qquad S_4 = \frac{\sigma p_1\ \sigma^2 p_1\ \sigma^5 p_2}{\sigma p_2\ \sigma^2 p_2\ \prod_{i=5}^{8} \sigma^i p_1};$$

is an $\mathrm{RCF}_{i,\sigma}$ of R. The weights of the shells are given in the following table:

	W_1	W_2	W_3	W_4
S_1	$(\mathbf{0}, \mathbf{19})$	$(19, 0)$	$(19, 0)$	$(19, 19)$
S_2	$(11, 2)$	$(\mathbf{2}, \mathbf{11})$	$(13, 11)$	$(13, 2)$
S_3	$(2, 7)$	$(7, 2)$	$(\mathbf{9}, \mathbf{2})$	$(9, 7)$
S_4	$(6, 3)$	$(3, 6)$	$(9, 6)$	$(\mathbf{9}, \mathbf{3})$

In each column, the lexicographically minimum weight is shown in boldface.

8.4. *The semi-periodic case*

In this subsection, $p \in k[x]$ is an irreducible semi-periodic polynomial. If R is as in (3) and $\tilde{\pi}(p) = 1$, then trivially $(R, 1)$ is an $\mathrm{RCF}_{w,\sigma}$ of R for any weight function w, hence we can assume that $\tilde{\pi}(p) > 1$. Denote $\delta := \deg p$ and $\rho := \tilde{\pi}(p)$. If (K, S) is an $\mathrm{RCF}_{w,\sigma}$ of R, then by Theorem 5, $K \sim K_f$ and $S \sim t(p)^{\xi} S_f$ where $f : [m] \to [n]$ is an increasing injection, $t(p)$ is the total span of p, and $\xi \in \mathbb{Z}$. Here it can happen that $W(t(p)^\xi S_f) < W(S_f)$ for $\xi = \pm 1$ because of cancellations, hence it is not enough to consider merely those RNF_σ's which are induced by injections. For example, if $R = \sigma^a p / \sigma^b p$ where $a < b$, then

$$S_f = \frac{1}{\prod_{i=a}^{b-1} \sigma^i p}, \qquad t(p) S_f = \prod_{i=b}^{a+\rho-1} \sigma^{i \bmod \rho} p,$$

so we choose between S_f and $t(p)S_f$, and take the one with smaller weight. Therefore instead of plain injections as in the non-periodic case, we consider *signed injections* which are pairs (f, s) where $f : [m] \to [n]$ is an injection and $s : [m] \to \{-1, +1\}$ is a sign function. We define the RNF_σ of R induced by (f, s) roughly in the following way: The kernel depends only on f and is defined in the same way as in the non-periodic case. The contribution from $\sigma^{a_i} p / \sigma^{b_{f(i)}} p$ to the shell is initially also defined in the same way as in the non-periodic case, but if $s(j) = -1$, this contribution is divided by $t(p)$ (in case it is a polynomial) or multiplied by $t(p)$ (in case it is the reciprocal of a polynomial). As it turns out, it is again possible to define an appropriate cost matrix such that an $\mathrm{RCF}_{w,\sigma}$ of R can be obtained from the solution of the associated assignment problem.

Definition 7. Let m, n be nonnegative integers such that $m \le n$. The pair (f, s) is a *signed injection* if $f : [m] \to [n]$ is an injection and $s : [m] \to \{-1, +1\}$.

Theorem 7. Let R be as in (3), and let (f, s) be a signed injection. Define

$$r(j) = \begin{cases} \rho, & s(j) = -1, \\ 0, & s(j) = +1, \end{cases}$$

and

$$K_{f,s} \ := \ \frac{\lambda \cdot \mu(p)^\tau}{\prod_{j \notin f([m])} \sigma^{b_j} p}, \quad S_{f,s} \ := \ \prod_{j=1}^{m} \frac{u_j^{(f,s)}}{v_j^{(f,s)}} \tag{9}$$

where $\mu(p)$ is defined in (2),

$$\tau \ = \ |\{j \in s^{-1}(-1);\ a_j > b_{f(j)}\}| - |\{j \in s^{-1}(-1);\ a_j < b_{f(j)}\}|,$$

$$u_j^{(f,s)} \ = \ \begin{cases} \prod_{i=b_{f(j)}}^{a_j + r(j) - 1} \sigma^{i \bmod \rho} p, & s(j) \cdot (a_j - b_{f(j)}) > 0, \\ 1, & \text{otherwise}, \end{cases}$$

$$v_j^{(f,s)} \ = \ \begin{cases} 1, & s(j) \cdot (a_j - b_{f(j)}) > 0, \\ \prod_{i=a_j}^{b_{f(j)} + r(j) - 1} \sigma^{i \bmod \rho} p, & \text{otherwise}. \end{cases}$$

Then $(K_{f,s}, S_{f,s}) \in \mathrm{RNF}_\sigma(R)$.

Proof: $K_{f,s}$ is trivially σ-reduced.

Assume that $s(j) \cdot (a_j - b_{f(j)}) > 0$. If $r(j) = 0$ then $u_j^{(f,s)} = \prod_{i=b_{f(j)}}^{a_j-1} \sigma^i p$, and

$$\frac{\sigma u_j^{(f,s)}}{u_j^{(f,s)}} = \frac{\sigma^{a_j} p}{\sigma^{b_{f(j)}} p}.$$

If $r(j) = \rho$ then $u_j^{(f,s)} = \prod_{i=b_{f(j)}}^{\rho-1} \sigma^i p \cdot \prod_{i=0}^{a_j-1} \sigma^i p$, and

$$\frac{\sigma u_j^{(f,s)}}{u_j^{(f,s)}} = \frac{\sigma^{\rho} p}{\sigma^{b_{f(j)}} p} \cdot \frac{\sigma^{a_j} p}{p} = \frac{\sigma^{a_j} p}{\sigma^{b_{f(j)}} p} \cdot \mu(p).$$

Hence

$$\frac{\sigma u_j^{(f,s)}}{u_j^{(f,s)}} = \begin{cases} \frac{\sigma^{a_j} p}{\sigma^{b_{f(j)}} p} \cdot \mu(p)^{r(j)/\rho}, & s(j) \cdot (a_j - b_{f(j)}) > 0 \\ 1, & \text{otherwise.} \end{cases}$$

Similarly we compute

$$\frac{v_j^{(f,s)}}{\sigma v_j^{(f,s)}} = \begin{cases} 1, & s(j) \cdot (a_j - b_{f(j)}) > 0 \\ \frac{\sigma^{a_j} p}{\sigma^{b_{f(j)}} p} \cdot \mu(p)^{-r(j)/\rho}, & \text{otherwise.} \end{cases}$$

Therefore

$$\frac{\sigma S_{f,s}}{S_{f,s}} = \prod_{j=1}^{m} \frac{\sigma u_j^{(f,s)}}{u_j^{(f,s)}} \cdot \frac{v_j^{(f,s)}}{\sigma v_j^{(f,s)}} = \prod_{j=1}^{m} \frac{\sigma^{a_j} p}{\sigma^{b_{f(j)}} p} \cdot \mu(p)^{-\tau},$$

hence $K_{f,s} \cdot \sigma S_{f,s} / S_{f,s} = R$. □

Remark 4. We call $(K_{f,s}, S_{f,s})$ defined in (9) the RNF$_\sigma$ *induced* by (f, s).

Definition 8. Let R be as in (3), let (f, s) be a signed injection, and let w be a weight function. We define the *weight of* (f, s) as $w(f, s) := w(d_1, d_2)$ where

$$\begin{aligned} d_1 &= \delta \sum_{s(j)\cdot(a_j - b_{f(j)})>0} (a_j + r(j) - b_{f(j)}), \\ d_2 &= \delta \sum_{s(j)\cdot(a_j - b_{f(j)})<0} (b_{f(j)} + r(j) - a_j), \end{aligned}$$

and $r(j)$ is defined in Theorem 7.

Lemma 11. Let (f, s) be a signed injection, and let w be a weight function. Then $W(S_{f,s}) \leq w(f, s)$.

Proof: From (9), $\deg \operatorname{num}(S_{f,s}) \leq \sum_{j=1}^{m} \deg u_j^{(f,s)} = d_1$ and $\deg \operatorname{den}(S_{f,s}) \leq \sum_{j=1}^{m} \deg v_j^{(f,s)} = d_2$, hence $W(S_{f,s}) = w(\deg \operatorname{num}(S_{f,s}), \deg \operatorname{den}(S_{f,s})) \leq w(d_1, d_2) = w(f,s)$. □

Definition 9. A signed injection (f,s) is *non-crossing* if $W(S_{f,s}) = w(f,s)$.

Lemma 12. Let (f,s) be a signed injection. Then there is a non-crossing signed injection (f',s') which induces the same RNF_σ as (f,s).

Proof: If $\prod_{j=1}^{m} u_j^{(f,s)} \perp \prod_{l=1}^{m} v_l^{(f,s)}$ then (f,s) is non-crossing and we can take $f' = f, s' = s$. Otherwise there are $j \neq l \in [m]$ such that $u_j^{(f,s)}$ and $v_l^{(f,s)}$ share a nontrivial common factor. This means that $s(j) \cdot (a_j - b_{f(j)}) > 0$, $s(l) \cdot (a_l - b_{f(l)}) < 0$, and

$$Q(j,l) \;:=\; \frac{u_j^{(f,s)}}{v_j^{(f,s)}} \cdot \frac{u_l^{(f,s)}}{v_l^{(f,s)}} \;=\; \frac{\prod_{i=b_{f(j)}}^{a_j+r(j)-1} \sigma^{i \bmod \rho} p}{\prod_{i=a_l}^{b_{f(l)}+r(l)-1} \sigma^{i \bmod \rho} p}.$$

There are four ways in which the intervals $I := [b_{f(j)}, a_j + r(j) - 1] \cap \mathbb{Z}$ and $J := [a_l, b_{f(l)} + r(l) - 1] \cap \mathbb{Z}$ can intersect when projected into $\mathbb{Z}/\rho\mathbb{Z}$:

(a) one of I, J is contained in the other,
(b) I and J partially overlap,
(c) $I \cap J = \emptyset$ but when projected into $\mathbb{Z}/\rho\mathbb{Z}$ one is contained in the other,
(d) $I \cap J = \emptyset$ but when projected into $\mathbb{Z}/\rho\mathbb{Z}$ they partially overlap.

In each of these cases there are two subcases as to the rôles played by I and J. Hence altogether we distinguish eight subcases:

(a1) $b_{f(j)} < a_l < b_{f(l)} + r(l) < a_j + r(j)$:
This is only possible if $r(l) = 0$, or $r(j) = r(l) = \rho$. Then

$$Q(j,l) \;=\; \prod_{i=b_{f(j)}}^{a_l-1} \sigma^{i \bmod \rho} p \cdot \prod_{i=b_{f(l)}+r(l)}^{a_j+r(j)-1} \sigma^{i \bmod \rho} p.$$

(a2) $a_l < b_{f(j)} < a_j + r(j) < b_{f(l)} + r(l)$:
This is only possible if $r(j) = 0$, or $r(j) = r(l) = \rho$. Then

$$Q(j,l) \;=\; \frac{1}{\prod_{i=a_l}^{b_{f(j)}-1} \sigma^{i \bmod \rho} p \cdot \prod_{i=a_j+r(j)}^{b_{f(l)}+r(l)-1} \sigma^{i \bmod \rho} p}.$$

(b1) $b_{f(j)} < a_l < a_j + r(j) < b_{f(l)} + r(l)$:
This is only possible if $r(j) = 0$, or $r(j) = r(l) = \rho$. Then

$$Q(j,l) \;=\; \frac{\prod_{i=b_{f(j)}}^{a_l-1} \sigma^{i \bmod \rho} p}{\prod_{i=a_j+r(j)}^{b_{f(l)}+r(l)-1} \sigma^{i \bmod \rho} p}.$$

(b2) $a_l < b_{f(j)} < b_{f(l)} + r(l) < a_j + r(j)$:

This is only possible if $r(l) = 0$, or $r(j) = r(l) = \rho$. Then

$$Q(j,l) \;=\; \frac{\prod_{i=b_{f(l)}+r(l)}^{a_j+r(j)-1} \sigma^{i \bmod \rho} p}{\prod_{i=a_l}^{b_{f(j)}-1} \sigma^{i \bmod \rho} p}.$$

In subcases (c1) and (d1) we have $b_{f(j)} < a_j + r(j) < a_l < b_{f(l)} + r(l)$ and $b_{f(j)} + \rho < b_{f(l)} + r(l)$. This is only possible if $r(j) = 0$ and $r(l) = \rho$, hence $a_l > b_{f(l)} > b_{f(j)}$.
(c1) If $a_j < b_{f(l)}$ then

$$Q(j,l) \;=\; \frac{1}{\prod_{i=a_l}^{b_{f(j)}+\rho-1} \sigma^{i \bmod \rho} p \cdot \prod_{i=a_j}^{b_{f(l)}-1} \sigma^{i \bmod \rho} p}.$$

(d1) If $a_j > b_{f(l)}$ then

$$Q(j,l) \;=\; \frac{\prod_{i=b_{f(l)}}^{a_j-1} \sigma^{i \bmod \rho} p}{\prod_{i=a_l}^{b_{f(j)}+\rho-1} \sigma^{i \bmod \rho} p}.$$

In subcases (c2) and (d2) we have $a_l < b_{f(l)} + r(l) < b_{f(j)} < a_j + r(j)$ and $a_l + \rho < a_j + r(j)$. This is only possible if $r(j) = \rho$ and $r(l) = 0$, hence $a_l < a_j < b_{f(j)}$.
(c2) If $a_j > b_{f(l)}$ then

$$Q(j,l) \;=\; \prod_{i=b_{f(j)}}^{a_l+\rho-1} \sigma^{i \bmod \rho} p \cdot \prod_{i=b_{f(l)}}^{a_j-1} \sigma^{i \bmod \rho} p.$$

(d2) If $a_j < b_{f(l)}$ then

$$Q(j,l) \;=\; \frac{\prod_{i=b_{f(j)}}^{a_l+\rho-1} \sigma^{i \bmod \rho} p}{\prod_{i=a_j}^{b_{f(l)}-1} \sigma^{i \bmod \rho} p}.$$

Define $f_1 : [m] \to [n]$ by $f_1(x) = f(x)$ for $x \neq j, l$, $f_1(j) = f(l)$, $f_1(l) = f(j)$. Define $s_1 : [m] \to \{-1, +1\}$ by $s_1(x) = s(x)$ for $x \neq j, l$, and

- in cases (a), (b):

$$\begin{aligned} s_1(j) &= \begin{cases} +1, & s(j) = s(l), \\ -1, & \text{otherwise}, \end{cases} \\ s_1(l) &= +1; \end{aligned}$$

- in cases (c), (d):

$$\begin{aligned} s_1(j) &= +1, \\ s_1(l) &= -1. \end{aligned}$$

Then it is straightforward to check that (f_1, s_1) is a signed injection which induces the same RNF_σ as (f, s), and that $\deg\gcd\left(\prod_{j=1}^m u_j^{(f_1,s_1)}, \prod_{l=1}^m v_l^{(f_1,s_1)}\right) < \deg\gcd\left(\prod_{j=1}^m u_j^{(f,s)}, \prod_{l=1}^m v_l^{(f,s)}\right)$. Iterating this procedure, we eventually arrive at a signed injection (f', s') which induces the same RNF_σ as (f, s), and is such that $\prod_{j=1}^m u_j^{(f',s')} \perp \prod_{l=1}^m v_l^{(f',s')}$. Hence (f', s') is non-crossing. $\square$

Lemma 13. Let R be as in (3), and let (K, S) be an $\mathrm{RCF}_{w,\sigma}$ of R. Then there is a non-crossing signed injection (f, s) such that $W(S) = w(f, s)$.

Proof: By Theorem 5, there are an increasing injection $f : [m] \to [n]$ and $\xi \in \mathbb{Z}$ such that $K \sim K_f$ and $S \sim t(p)^\xi S_f$. Let $S_f = \prod_{j=1}^m u_j^{(f)}/v_j^{(f)}$ as in (4), and assume that $\xi \geq 0$ (if $\xi < 0$ the proof is analogous). Denote $J = \{j \in [m]; a_j < b_{f(j)}\}$ and $N = |J|$. We distinguish two cases:

a) $\xi > N$: In this case, $t(p)^\xi S_f$ equals $t(p)P$ for some polynomial $P \in k[x]$. Then $(\eta K_f, P) \in \mathrm{RNF}_\sigma(R)$ where $\eta = (K/K_f)\sigma(S/P)/(S/P)$. Since $\deg P < \deg(t(p)P) = \deg\mathrm{num}(S)$, we have $W(P) = w(\deg P, 0) < w(\deg\mathrm{num}(S), \deg\mathrm{den}(S)) = W(S)$. So this case is impossible.
b) $\xi \leq N$: W.l.g. assume that $a_j < b_{f(j)}$ for $j \in [N]$. Then

$$
\begin{aligned}
t(p)^\xi S_f &= \prod_{j=1}^{\xi} \frac{t(p)}{v_j^{(f)}} \cdot \prod_{j=\xi+1}^{m} \frac{u_j^{(f)}}{v_j^{(f)}} = \prod_{j=1}^{\xi} \frac{\prod_{i=0}^{\rho-1} \sigma^i p}{\prod_{i=a_j}^{b_{f(j)}-1} \sigma^i p} \cdot \prod_{j=\xi+1}^{m} \frac{u_j^{(f)}}{v_j^{(f)}} \\
&= \prod_{j=1}^{\xi} \prod_{i=b_{f(j)}}^{a_j+\rho-1} \sigma^{i \bmod \rho} p \cdot \prod_{j=\xi+1}^{m} \frac{u_j^{(f)}}{v_j^{(f)}} = S_{f,s}
\end{aligned}
$$

where

$$
s(j) = \begin{cases} -1, & 1 \leq j \leq \xi, \\ +1, & \xi+1 \leq j \leq m. \end{cases}
$$

By Lemma 12, there is a non-crossing signed injection (f', s') which induces the same RNF_σ as (f, s). Hence $W(S) = W(t(p)^\xi S_f) = W(S_{f,s}) = W(S_{f',s'}) = w(f', s')$. $\square$

Theorem 8. Let R be as in (3), let w be a weight function, let (g, z) be a signed injection of minimum weight, and let $(K_{g,z}, S_{g,z})$ be the RNF_σ of R induced by (g, z). Then $((\sigma\lambda/\lambda)K_{g,z}, S_{g,z}/\lambda)$ where $\lambda = \mathrm{lc}\,(S_{g,z})$ is an $\mathrm{RCF}_{w,\sigma}$ of R.

Proof: Let (K, S) be an $\mathrm{RCF}_{w,\sigma}$ of R. By Lemma 13, there is a signed injection (f, s) such that $W(S) = w(f, s)$. By minimality of (g, z), we have $w(f, s) \geq w(g, z)$, and by Lemma 11, $w(g, z) \geq W(S_{g,z})$, so $W(S) \geq W(S_{g,z})$. Hence $W(S_{g,z}) = W(S)$ is minimal among all RNF_σ's of R, and the assertion follows because $\mathrm{lc}\,(S_{g,z}/\lambda) = 1$. $\square$

Theorem 8 shows that to compute an $\mathrm{RCF}_{w,\sigma}$ of R where R is as in (3), it suffices to find a signed injection of minimum weight. By additivity of w, we have

$$
\begin{aligned}
\min_{(f,s)} w(f,s) &= \min_{(f,s)} w(d_1,d_2) = \min_{(f,s)} \delta \cdot w\left(\sum_{i=1}^m \alpha_i,\ \sum_{i=1}^m \beta_i\right) \\
&= \delta \cdot \min_{(f,s)} \sum_{i=1}^m w(\alpha_i,\beta_i) = \delta \cdot \min_f \min_s \sum_{i=1}^m w(\alpha_i,\beta_i)
\end{aligned}
$$

where

$$
(\alpha_i,\beta_i) = \begin{cases} (a_i + r(i) - b_{f(i)}, 0), & s(i)\cdot(a_i - b_{f(i)}) > 0, \\ (0, b_{f(i)} + r(i) - a_i), & \text{otherwise.} \end{cases}
$$

The values of s can be chosen independently of each other, therefore

$$
\min_s \sum_{i=1}^m w(\alpha_i,\beta_i) = \sum_{i=1}^m \min_s w(\alpha_i,\beta_i) = \sum_{i=1}^m \min(\xi_i,\eta_i)
$$

where

$$
\begin{aligned}
(\xi_i,\eta_i) &= \big(w(\alpha_i,\beta_i)|_{s(i)=+1}, w(\alpha_i,\beta_i)|_{s(i)=-1}\big) \\
&= \begin{cases} \big(w(a_i - b_{f(i)},0), w(0,b_{f(i)}+\rho-a_i)\big),\ a_i > b_{f(i)}, \\ \big(w(0,b_{f(i)}-a_i), w(a_i+\rho-b_{f(i)},0)\big),\ a_i < b_{f(i)}. \end{cases}
\end{aligned}
$$

Thus $\min_{(f,s)} w(f,s) = \delta \cdot \min_f \sum_{i=1}^m c_{i,f(i)}$ where

$$
c_{i,j} = \begin{cases} \min\left(w(a_i - b_j, 0), w(0, b_j + \rho - a_i)\right),\ a_i > b_j, \\ \min\left(w(0, b_j - a_i), w(a_i + \rho - b_j, 0)\right),\ a_i < b_j. \end{cases} \tag{10}
$$

Consequently, a signed injection (f,s) of minimum weight can be found in the following way. By solving the assignment problem with cost matrix (10) we obtain f, and s is determined by f: if $a_i > b_{f(i)}$ and $w(0, b_{f(i)} + \rho - a_i) < w(a_i - b_{f(i)}, 0)$, or if $a_i < b_{f(i)}$ and $w(a_i + \rho - b_{f(i)}, 0) < w(0, b_{f(i)} - a_i)$, then $s(i) = -1$. Otherwise $s(i) = +1$.

Example 8. Let $p(x) = x$ and $\sigma x = \omega x + 1$ where ω is a primitive 22nd root of unity. Then $\sigma^{22} p = p$, and p is semi-periodic with semi-period $\rho = \tilde{\pi}(p) = 22$.

Let R be as in Example 4. Then $((\sigma\lambda_i/\lambda_i)K_i, S_i/\lambda_i)$ where $\lambda_i = \mathrm{lc}\,(S_i)$ and

$$\begin{aligned}
K_1 &= \frac{1}{p\ \sigma^6 p\ \sigma^{12} p}, & S_1 &= \sigma^2 p\ \textstyle\prod_{i=7}^{9} \sigma^i p\ \prod_{i=13}^{15} \sigma^i p\ \sigma^{19} p\ \left(\sigma^{20} p\right)^2 \sigma^{21} p;\\
K_2 &= \frac{1}{\sigma^7 p\ \sigma^{13} p\ \sigma^{20} p}, & S_2 &= \frac{1}{p^2\ \sigma p\ \prod_{i=3}^{5} \sigma^i p\ \prod_{i=10}^{11} \sigma^i p\ \prod_{i=16}^{18} \sigma^i p\ \sigma^{21} p};\\
K_3 &= \frac{1}{\sigma^6 p\ \sigma^7 p\ \sigma^{19} p}, & S_3 &= \frac{\sigma^2 p\ \sigma^{13} p\ \sigma^{14} p\ \sigma^{15} p\ \sigma^{20} p}{p\ \sigma^{10} p\ \sigma^{11} p};\\
K_4 &= \frac{1}{\sigma^6 p\ \sigma^7 p\ \sigma^{13} p}, & S_4 &= \frac{\sigma^2 p\ \sigma^{20} p}{p\ \sigma^{10} p\ \sigma^{11} p\ \sigma^{16} p\ \sigma^{17} p\ \sigma^{18} p};
\end{aligned}$$

is an $\mathrm{RCF}_{i,\sigma}$ of R, for $i = 1, 2, 3, 4$. The weights W_1, W_2, W_3, W_4 of S_1, S_2, S_3, S_4 are given in the following table:

	W_1	W_2	W_3	W_4
S_1	$(\mathbf{0}, \mathbf{11})$	$(11, 0)$	$(11, 0)$	$(11, 11)$
S_2	$(12, 0)$	$(\mathbf{0}, \mathbf{12})$	$(12, 12)$	$(12, 0)$
S_3	$(3, 5)$	$(5, 3)$	$(\mathbf{8}, \mathbf{3})$	$(8, 5)$
S_4	$(6, 2)$	$(2, 6)$	$(8, 6)$	$(\mathbf{8}, \mathbf{2})$

In each column, the lexicographically minimum weight is shown in boldface. It is instructive to compare this table with the one in Example 4.

Proposition 4. Let $p \in k[x]$ be irreducible semi-periodic, let $R \in k(x)$ be p-orbital, and let (K_1, S_1) resp. (K_2, S_2) be an $\mathrm{RCF}_{1,\sigma}$ resp. an $\mathrm{RCF}_{2,\sigma}$ of R. Then S_1 and $1/S_2$ are polynomials.

Proof: In the case of $\mathrm{RCF}_{1,\sigma}$, the cost matrix (10) is

$$c_{i,j} \;=\; \begin{cases} (0, a_i - b_j), & a_i > b_j,\\ (0, a_i + \rho - b_j), & a_i < b_j, \end{cases}$$

hence $W(S_1) = (\deg \mathrm{den}(S_1), \deg \mathrm{num}(S_1))$ is of the form $(0, u)$ for some $u \in \mathbb{Z}$, $u \geq 0$. – Similarly, in the case of $\mathrm{RCF}_{2,\sigma}$, the cost matrix (10) is

$$c_{i,j} \;=\; \begin{cases} (0, b_j + \rho - a_i), & a_i > b_j,\\ (0, b_j - a_i), & a_i < b_j, \end{cases}$$

hence $W(S_2) = (\deg \mathrm{num}(S_2), \deg \mathrm{den}(S_2))$ is of the form $(0, v)$ for some $v \in \mathbb{Z}$, $v \geq 0$. □

9. Uniqueness of rational (w,σ)-canonical forms

In this section we show that the rational (w,σ)-canonical form of $R \in k(x)$ is unique provided that each irreducible factor of R is non-periodic w.r.t. σ.

Definition 10. Let $f_1, f_2 : [m] \to [n]$ be two increasing injections, and $s \geq 1$. A sequence of integers $\langle i_1, i_2, \ldots, i_s\rangle$, $1 \leq i_1 < i_2 < \cdots < i_s \leq m$, is an (f_1, f_2)-*chain* if
(1) $f_1(i_j) < f_2(i_j)$, for $1 \leq j \leq s$,
(2) $f_1(i_{j+1}) = f_2(i_j)$, for $1 \leq j \leq s-1$.
Such a chain is *maximal* if $f_1(i_1) \notin f_2([m])$ and $f_2(i_s) \notin f_1([m])$.

Lemma 14. If there is an $i \in [m]$ such that $f_1(i) < f_2(i)$ then $[m]$ contains a maximal (f_1, f_2)-chain.

Proof: Let $\langle i_1, i_2, \ldots, i_s\rangle$ be an (f_1, f_2)-chain. If it is not maximal then either there is $i_0 < i_1$ such that $f_2(i_0) = f_1(i_1)$ or $i_{s+1} > i_s$ such that $f_1(i_{s+1}) = f_2(i_s)$. In the former case, $f_1(i_0) < f_1(i_1) = f_2(i_0)$, so $\langle i_0, i_1, \ldots, i_s\rangle$ is a larger (f_1, f_2)-chain. In the latter case, $f_1(i_{s+1}) = f_2(i_s) < f_2(i_{s+1})$, so $\langle i_1, \ldots, i_s, i_{s+1}\rangle$ is a larger (f_1, f_2)-chain. Thus every chain which is not maximal can be extended to a maximal chain. In particular, if $f_1(i) < f_2(i)$ then $\langle i\rangle$ is an (f_1, f_2)-chain which is contained in some maximal chain. □

Proposition 5. Let $f_1, f_2 : [m] \to [n]$, $f_1 \neq f_2$, be two increasing injections such that $c(f_1) = c(f_2)$ where c is the cost matrix (8). Then there is an injection $f : [m] \to [n]$ such that $c(f) < c(f_1)$.

Proof: Let $i \in [m]$ be such that $f_1(i) \neq f_2(i)$. W.l.g. assume that $f_1(i) < f_2(i)$ (otherwise interchange the rôles of f_1 and f_2). By Lemma 14, $[m]$ contains a maximal (f_1, f_2)-chain $\langle i_1, i_2, \ldots, i_s\rangle$. Define $g, h : [m] \to [n]$ by

$$g(x) = \begin{cases} f_1(x), & x \neq i_1, i_2, \ldots, i_s, \\ f_2(x), & \text{otherwise}, \end{cases}$$

$$h(x) = \begin{cases} f_2(x), & x \neq i_1, i_2, \ldots, i_s, \\ f_1(x), & \text{otherwise}. \end{cases}$$

We claim that g and h are injective. Indeed, if g is not injective then $f_1(x) = f_2(i_j)$ for some $x \neq i_1, \ldots, i_s$ and $j \in [s]$. Since $f_2(i_j) = f_1(i_{j+1})$ for $1 \leq j \leq s-1$, this is only possible if $j = s$. But then $f_2(i_s) = f_1(x) \in f_1([m])$, contrary to the maximality of $\langle i_1, i_2, \ldots, i_s\rangle$. – In an analogous way we can see that h is injective.

The cost of g respectively h is

$$c(g) = \gamma - \alpha, \quad c(h) = \gamma + \alpha,$$

where $\gamma = c(f_1) = c(f_2)$ and

$$\alpha = \sum_{j=1}^{s} (c_{i_j, f_1(i_j)} - c_{i_j, f_2(i_j)}).$$

We wish to show that $\alpha \neq 0$. By (8), we can write $c_{i_j,f_1(i_j)} - c_{i_j,f_2(i_j)} = w(u_j, v_j)$ for some $u_j, v_j \in \mathbb{Z}$. Then $\alpha = \sum_{j=1}^{s} w(u_j, v_j) = w(u, v)$ where $u = \sum_{j=1}^{s} u_j$ and $v = \sum_{j=1}^{s} v_j$. Since $b_{f_1(i_j)} < b_{f_2(i_j)}$, it suffices to distinguish three cases:

(1) If $a_{i_j} < b_{f_1(i_j)} < b_{f_2(i_j)}$ then, by (8), $u_j = 0$ and $v_j = b_{f_1(i_j)} - b_{f_2(i_j)} < 0$.
(2) If $b_{f_1(i_j)} < a_{i_j} < b_{f_2(i_j)}$ then, by (8), $u_j = a_{i_j} - b_{f_1(i_j)} > 0$ and $v_j = a_{i_j} - b_{f_2(i_j)} < 0$.
(3) If $b_{f_1(i_j)} < b_{f_2(i_j)} < a_{i_j}$ then, by (8), $u_j = b_{f_2(i_j)} - b_{f_1(i_j)} > 0$ and $v_j = 0$.

Hence $u = \sum_{j=1}^{s} u_j \geq 0$, $v = \sum_{j=1}^{s} v_j \leq 0$, and at least one of these inequalities is strict. As w is injective, it follows that $\alpha = w(u, v) \neq w(0, 0) = 0$.

Now define

$$f = \begin{cases} g, & \alpha > 0, \\ h, & \alpha < 0. \end{cases}$$

Then $c(f) = \gamma - |\alpha| < \gamma$. □

Corollary 4. Let $R \in k(x)$ be as in (3) where $p \in k[x]$ is non-periodic. Then R has a unique $\mathrm{RCF}_{w,\sigma}$ for any weight function w.

Proof: Existence of $\mathrm{RCF}_{w,\sigma}$ has already been established in Proposition 2.

To prove uniqueness, assume that (K_1, S_1) and (K_2, S_2) are two distinct $\mathrm{RCF}_{w,\sigma}$'s of R. By Theorem 5, (K_1, S_1) and (K_2, S_2) arise from increasing injections $f_1, f_2 : [m] \to [n]$, respectively. By Lemma 10, $w(f_1) = W(S_1) = W(S_2) = w(f_2)$, hence $c(f_1) = c(f_2)$ where c is the cost matrix (8). By Proposition 5, there is an injection $f : [m] \to [n]$ such that $c(f) < c(f_1)$. But then $w(f) < w(f_1)$, which is impossible. □

10. An application: Succinct representation of σ-hypergeometric terms

In this section we assume that σ is a k-automorphism[13] of $k(x)$, which implies that $\sigma R(x) = R(\sigma x)$ for all $R \in k(x)$. In addition, we assume that the mapping $\tilde{\ } : \mathbb{Z} \to k$ defined by $\tilde{n} = (\sigma^n x)\,|_{x=1}$, is injective.

Definition 11. A sequence $t = \langle t_n \rangle_{n \geq 0}$ of elements of k is a *σ-hypergeometric term* if $t_n \neq 0$ for all large enough n, and there are polynomials $p, q \in k[x] \setminus \{0\}$, $p \perp q$, such that

$$p(\tilde{n}) t_{n+1} = q(\tilde{n}) t_n \quad \text{for all } n \geq 0,$$

where $\tilde{n} = (\sigma^n x)\,|_{x=1}$. The quotient $q/p \in k(x)^*$ is called the *certificate* of t.

A sequence $\langle s_n \rangle_{n \geq n_0}$ with $n_0 \in \mathbb{Z} \setminus \{0\}$ is also called a *σ-hypergeometric term* if the sequence $t = \langle t_n \rangle_{n \geq 0}$ where $t_n = s_{n+n_0}$ satisfies Definition 11.

Proposition 6. The certificate of a σ-hypergeometric term is unique.

---

[13] In this case, we could also restrict our attention to the two special cases $\sigma x = x + b$ and $\sigma x = ax$, for if $\sigma x = ax + b$ and $a \neq 1$, the new variable $y = x + b/(a - 1)$ satisfies $\sigma y = ay$.

Proof: By the assumptions on t and $\tilde{}$, both t_n and $p(\tilde{n})$ are nonzero for all large enough n, hence $q(\tilde{n})/p(\tilde{n}) = t_{n+1}/t_n$ for such n. Thus any two certificates of t agree infinitely often, and hence are equal. □

Theorem 9. Let $F, G \in k(x)^*$ be rational functions. For each $n \geq 0$, let

$$T_n = \sigma^n G \cdot \prod_{i=0}^{n-1} \sigma^i F. \tag{11}$$

If $\mathrm{den}(T_n)(1) \neq 0$ for all $n \geq 0$ and $\mathrm{num}(T_n)(1) \neq 0$ for all large enough n, then the sequence $t = \langle t_n \rangle_{n \geq 0}$ defined by

$$t_n = T_n(1)$$

is a σ-hypergeometric term with certificate $H = F \cdot \sigma G/G$.

Proof: Denote $p = \mathrm{den}(H)$, $q = \mathrm{num}(H)$, and $h_i = \sigma^i H$. Then

$$\frac{T_{n+1}}{T_n} = \frac{\sigma^{n+1} G}{\sigma^n G} \cdot \sigma^n F = \sigma^n H = h_n,$$

therefore $\mathrm{den}(h_n)T_{n+1} = \mathrm{num}(h_n)T_n$. As $\mathrm{den}(h_n)(1) = \mathrm{den}(\sigma^n H(x))|_{x=1} = \mathrm{den}(H(\sigma^n x))|_{x=1} = \mathrm{den}(H)(\sigma^n x)|_{x=1} = p(\sigma^n x)|_{x=1} = p((\sigma^n x)|_{x=1}) = p(\tilde{n})$, and similarly $\mathrm{num}(h_n)(1) = q(\tilde{n})$, it follows that $p(\tilde{n})t_{n+1} = q(\tilde{n})t_n$. □

Definition 12. Let F, G and t be as in Theorem 9. Then we call $\langle F, G \rangle$ a *multiplicative decomposition* of t. If $\deg \mathrm{num}(F) \leq \deg \mathrm{num}(F')$ and $\deg \mathrm{den}(F) \leq \deg \mathrm{den}(F')$ for all multiplicative decompositions $\langle F', G' \rangle$ of t, then $\langle F, G \rangle$ is a *minimal multiplicative decomposition* of t.

Example 9. Let $\sigma x = x + 1$. Then $\tilde{n} = (x + n)|_{x=1} = n + 1$. Let $p \in k[x] \setminus \{0\}$ be a polynomial such that $p(0) \neq 0$, and let the sequence $t = \langle t_n \rangle_{n \geq 0}$ be defined by $t_n = p(n)$. Then $p(\tilde{n}-1)t_{n+1} = p(\tilde{n})t_n$ for all $n \geq 0$, so t is a σ-hypergeometric term. Since $(\sigma^n p(x-1) \cdot \prod_{i=0}^{n-1} \sigma^i 1)|_{x=1} = p(x+n-1)|_{x=1} = p(n)$ and $(\sigma^n p(0) \cdot \prod_{i=0}^{n-1} \sigma^i (p(x)/p(x-1)))|_{x=1} = (p(0) \cdot \prod_{i=0}^{n-1} (p(x+i)/p(x+i-1)))|_{x=1} = (p(0) \cdot p(x+n-1)/p(x-1))|_{x=1} = p(n)$, both $(1, p(x-1))$ and $(p(x)/p(x-1), p(0))$ are multiplicative decompositions of t. Note that in the latter case, some of the factors in $\prod_{i=0}^{n-1} (p(x+i)/p(x+i-1))$ may well be undefined at $x = 1$, but this represents no obstacle since the product itself is defined at $x = 1$.

Definition 13. Let w be a weight function, and let $\langle F, G \rangle$ be a minimal multiplicative decomposition of t. If $W(G) \leq W(G')$ for all minimal multiplicative decompositions $\langle F', G' \rangle$ of t, then $\langle F, G \rangle$ is a *w-minimal multiplicative decomposition* of t.

Theorem 10. Let $t = \langle t_n \rangle_{n \geq 0}$ be a σ-hypergeometric term such that $t_0 \neq 0$, with multiplicative decomposition $\langle F, G \rangle$ and certificate $H = F \cdot \sigma G/G$. If $(K, S) \in \mathrm{RNF}_\sigma(H)$ is such that $S(1) \in k^*$, and if $S' = S \cdot G(1)/S(1)$, then

(i) $\langle K, S' \rangle$ is a minimal multiplicative decomposition of t;

(ii) if, in addition, (K,S) is an $\mathrm{RCF}_{w,\sigma}$ of H for some weight function w, then $\langle K,S'\rangle$ is a w-minimal multiplicative decomposition of t.

Proof: We have

$$
\begin{aligned}
T_n &= \sigma^n G \cdot \prod_{i=0}^{n-1} \sigma^i F \;=\; G \cdot \prod_{i=0}^{n-1} \sigma^i \left(F \cdot \frac{\sigma G}{G}\right) \\
&= G \cdot \prod_{i=0}^{n-1} \sigma^i \left(K \cdot \frac{\sigma S}{S}\right) = \frac{G}{S} \cdot \sigma^n S \cdot \prod_{i=0}^{n-1} \sigma^i K.
\end{aligned}
$$

By assumption, $G(1) = t_0 \in k^*$ and $S(1) \in k^*$. Therefore

$$
t_n = T_n(1) = \frac{G(1)}{S(1)} \cdot \left(\sigma^n S \cdot \prod_{i=0}^{n-1} \sigma^i K\right)(1) = \left(\sigma^n S' \cdot \prod_{i=0}^{n-1} \sigma^i K\right)(1),
$$

hence $\langle K,S'\rangle$ is a multiplicative decomposition of t.

(i) Let $\langle F',G'\rangle$ be any multiplicative decomposition of t. Then by Theorem 9 and Proposition 6, $H = F' \cdot \sigma G'/G'$. As $(K,S) \in \mathrm{RNF}_\sigma(H)$, Corollary 3 implies that $\deg \mathrm{num}(K) \le \deg \mathrm{num}(F')$ and $\deg \mathrm{den}(K) \le \deg \mathrm{den}(F')$. Hence $\langle K,S'\rangle$ is a minimal multiplicative decomposition of t.

(ii) Let $\langle F',G'\rangle$ be any minimal multiplicative decomposition of t. By (i), $\langle K,S'\rangle$ is a minimal multiplicative decomposition of t as well, therefore $\deg \mathrm{num}(F') = \deg \mathrm{num}(K)$ and $\deg \mathrm{den}(F') = \deg \mathrm{den}(K)$. As $(K,S) \in \mathrm{RNF}_\sigma(H)$, Corollary 3 implies that $\deg \mathrm{num}(F') \le \deg \mathrm{num}(F'')$ and $\deg \mathrm{den}(F') \le \deg \mathrm{den}(F'')$ for all $F'', G'' \in k^*$ such that $H = F'' \cdot \sigma G''/G''$. Hence, by Corollary 3, $(F',G') \in \mathrm{RNF}_\sigma(H)$. Since (K,S) is an $\mathrm{RCF}_{w,\sigma}$ of H, it follows that $W(S') = W(S) \le W(G')$, and so $\langle K,S'\rangle$ is a w-minimal multiplicative decomposition of t. □

Example 10. Let $\sigma x = qx$ where $q \in k^*$ is transcendental over $\mathbb{Q} \subseteq k$. In this case, $\tilde{n} = (\sigma^n x)|_{x=1} = q^n$. Let t be a σ-hypergeometric term (called *q-hypergeometric* in this case) with multiplicative decomposition $\langle F,G\rangle$. By factoring F into linear factors over $\bar{k}$, we may be able to avoid the explicit use of the product operator in (11), and instead express t entirely by means of the *q-Pochhammer symbol* $(z;q)_n$ defined for $z \in k$ and $n \in \mathbb{Z}$, $n \ge 0$, by

$$
(z;q)_n = \prod_{i=0}^{n-1} (1 - zq^i).
$$

Consider the q-hypergeometric term t with multiplicative decomposition $\langle R,1\rangle$ where R is given in Example 7. Then

$$
\begin{aligned}
t_n = T_n(1) \;&=\; \prod_{j=0}^{n-1} \sigma^j R(x)|_{x=1} \;=\; \prod_{j=0}^{n-1} R(\sigma^j x|_{x=1}) \;=\; \prod_{j=0}^{n-1} R(q^j) \\
&= \prod_{j=0}^{n-1} \frac{(q^j{+}q^2)(q^j{+}1)(q^j{+}q^5{-}q^3)(q^j{+}q^4{-}q^2)(q^3q^j{+}q^2{-}1)(q^{12}q^j{+}q^2{-}1)}{(q^j{+}q^5)(q^j{+}q^4)^2(q^4q^j{+}1)(q^j{+}q^2{-}1)(q^2q^j{+}q^2{-}1)},
\end{aligned}
$$

which can be expressed in terms of q-Pochhammer symbols as

$$t_n \;=\; \alpha^n \cdot \frac{\left(-\frac{1}{q^2};q\right)_n (-1;q)_n \left(\frac{1}{q^3-q^5};q\right)_n \left(\frac{1}{q^2-q^4};q\right)_n \left(\frac{q^3}{1-q^2};q\right)_n \left(\frac{q^{12}}{1-q^2};q\right)_n}{\left(-\frac{1}{q^5};q\right)_n \left(-\frac{1}{q^4};q\right)_n^2 (-q^4;q)_n \left(\frac{1}{1-q^2};q\right)_n \left(\frac{q^2}{1-q^2};q\right)_n}$$

where $\alpha = (q^2-1)^2/q^6 \in k^*$.

Note that the number of q-Pochhammer symbols appearing in the above expression (counted with multiplicities) is $\deg\operatorname{num}(R) + \deg\operatorname{den}(R) = 12$. By replacing decomposition $\langle R, 1\rangle$ with some decomposition $\langle K, S\rangle$ where $(K, S) \in \mathrm{RNF}_\sigma(R)$ and $S(1) = 1$, we can reduce the number of q-Pochhammer symbols to its minimal possible value $\deg\operatorname{num}(K)+\deg\operatorname{den}(K) = 4$, at the reasonable price of introducing the rational-function factor $S(q^n)$. Furthermore, if (K, S) is an $\mathrm{RCF}_{w,\sigma}$ of R for some weight function w, then, in addition, $W(S)$ will be minimal among all such representations of t.

Thus for the term t given above, and for the weight functions w_1, w_2, w_3, w_4 from Example 3, we obtain the following succinct representations of t:

$$\begin{aligned}
t_n &= \frac{\alpha^n}{S_1(1)} \cdot S_1(q^n) \cdot \frac{\left(\frac{1}{q^3-q^5};q\right)_n \left(\frac{1}{q^2-q^4};q\right)_n}{\left(-\frac{1}{q^5};q\right)_n (-q^4;q)_n} \\
&= \frac{\alpha^n}{S_2(1)} \cdot S_2(q^n) \cdot \frac{\left(\frac{q^3}{1-q^2};q\right)_n \left(\frac{q^{12}}{1-q^2};q\right)_n}{\left(-\frac{1}{q^5};q\right)_n \left(-\frac{1}{q^4};q\right)_n} \\
&= \frac{\alpha^n}{S_3(1)} \cdot S_3(q^n) \cdot \frac{\left(\frac{q^{12}}{1-q^2};q\right)_n \left(\frac{1}{q^3-q^5};q\right)_n}{\left(-\frac{1}{q^5};q\right)_n (-q^4;q)_n} \\
&= \frac{\alpha^n}{S_4(1)} \cdot S_4(q^n) \cdot \frac{\left(\frac{1}{q^3-q^5};q\right)_n \left(\frac{q^{12}}{1-q^2};q\right)_n}{\left(-\frac{1}{q^5};q\right)_n \left(-\frac{1}{q^4};q\right)_n},
\end{aligned}$$

where the rational functions S_i, for $i = 1, 2, 3, 4$, are given in Example 7. Note that in each of the above representations, the number of q-Pochhammer symbols is four (which is the least possible), and the weight $W_i(S_i)$ is minimal among all representations of t containing no more than four q-Pochhammer symbols, for $i = 1, 2, 3, 4$.

11. Questions for further research

(1) Is $\mathrm{RCF}_{w,\sigma}(R)$ unique even if R contains irreducible factors which are semi-periodic with respect to σ?

(2) Our approach to the computation of $\mathrm{RCF}_{w,\sigma}$'s is based on orbital decomposition which requires polynomial facorization. In special cases (such as computing $\mathrm{RCF}_{1,\sigma}$ and $\mathrm{RCF}_{2,\sigma}$ when $\sigma = \mathcal{E}$) algorithms are known which require only gcd and resultant computations (Abramov, Le and Petkovšek, 2003, Section 4.5). Is there an algorithm for computing $\mathrm{RCF}_{w,\sigma}$, based perhaps on a suitable generalization of the greatest factorial factorization of (Paule, 1995), which avoids polynomial factorization?

(3) The problem solved by the (hypothetical) algorithm HSO of Section 8.1 is the homogeneous case ($\beta = 1$) of the *σ-orbit problem*[14] of (Abramov and Bronstein, 2000). In an analogous way, an algorithm for solving the σ-orbit problem can also be used to construct algorithm SE of Section 8.1 in the case $\sigma x = ax$. Karr (1981, Thms. 4 and 5) reduced the σ-orbit problem in a general $\Pi\Sigma$-field to the *orbit problem*[15] in its constant field. Together with (Kannan and Lipton, 1986) and (Abramov and Bronstein, 2000), this gives an algorithm for solving the σ-orbit problem in towers of $\Pi\Sigma$-extensions over certain commonly occurring base fields. In which other fields is this important problem solvable?

Acknowledgements

The authors wish to express their thanks to the referees whose reports inspired a thorough revision of the initial submission and helped clear up the algorithmic aspects in the revised version, as well as to Prof. Peter Paule for his encouragement and great patience while waiting for the revised version. The second author thanks Ha Q. Le for his valuable contributions. We are especially indebted to our late friend and colleague Manuel Bronstein whose scholarly work in (Bronstein, 2000) paved the way for our investigations.

References

S. A. Abramov and M. Bronstein. Hypergeometric dispersion and the orbit problem. *Proc. Int. Symp. on Symbolic and Algebraic Computation (ISSAC 2000)*, St. Andrews, ACM Press, New York, 2000, 8–13.

S. A. Abramov, H. Q. Le, and M. Petkovšek. Rational canonical forms and efficient representations of hypergeometric terms. *Proc. Int. Symp. on Symbolic and Algebraic Computation (ISSAC 2003)*, Philadelphia, ACM Press, New York, 2003, 7–14.

S. A. Abramov and M. Petkovšek. Canonical representations of hypergeometric terms. *Proc. Formal Power Series and Algebraic Combinatorics (FPSAC 2001)*, Arizona, U.S.A., 2001, 1–10.

S. A. Abramov and M. Petkovšek. Rational normal forms and minimal decompositions of hypergeometric terms. *J. Symb. Comput.* **33**, 521–543, 2002.

A. Bauer and M. Petkovšek. Multibasic and mixed hypergeometric Gosper-type algorithms. *J. Symb. Comput.* **28**, 711–736, 1999.

M. Bronstein. On solutions of linear ordinary difference equations in their coefficient field. *J. Symb. Comput.* **29**, 841–877, 2000.

F. Caruso. *Polynomial arithmetic and linear systems in symbolic summation*, Ph.D. Thesis. RISC-Linz (Austria), 2003.

D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*, 2nd ed. Springer-Verlag, New York, 1997.

R. W. Gosper, Jr. Decision procedure for indefinite hypergeometric summation. *Proc. Natl. Acad. Sci. U.S.A.* **75**, 40–42, 1978.

[14] Given $\alpha, \beta \in k^*$, decide if the affine set $A(\alpha, \beta) := \{n \in \mathbb{Z};\ \alpha^{\sigma,n} = \beta\}$ is empty, and if not, find $m, n \in \mathbb{Z}$ such that $A(\alpha, \beta) = m + n\mathbb{Z}$.

[15] Given $\alpha, \beta \in k^*$, decide if the affine set $A(\alpha, \beta) := \{n \in \mathbb{Z};\ \alpha^n = \beta\}$ is empty, and if not, find $m, n \in \mathbb{Z}$ such that $A(\alpha, \beta) = m + n\mathbb{Z}$.

R. Kannan and R. J. Lipton. Polynomial time algorithm for the orbit problem. *J. ACM* **33**, 808–821, 1986.

M. Karr. Summation in finite terms. *J. ACM* **28**, 305–350, 1981.

M. Karr. Theory of summation in finite terms. *J. Symb. Comput.* **1**, 303–315, 1985.

C. H. Papadimitriou and K. Steiglitz. *Combinatorial Optimization: Algorithms and Complexity.* Prentice-Hall Inc., Englewood Cliffs, New Jersey, 1982.

P. Paule. Greatest factorial factorization and symbolic summation. *J. Symb. Comput.* **20**, 235–268, 1995.

M. Petkovšek. Hypergeometric solutions of linear recurrences with polynomial coefficients. *J. Symb. Comput.* **14**, 243–264, 1992.

R. Pirastu and V. Strehl. Rational summation and Gosper-Petkovšek representation. *J. Symb. Comput.* **20**, 617–635, 1995.

M. van der Put and M. F. Singer. *Galois Theory of Difference Equations.* Springer-Verlag, Berlin Heidelberg, 1997.

C. Schneider. *Symbolic summation in difference fields*, Ph.D. Thesis. RISC-Linz (Austria), 2001.

C. Schneider. Product representations in ΠΣ-fields. *Ann. Comb.* **9**, 75–99, 2005.

D. Zeilberger. The method of creative telescoping. *J. Symb. Comput.* **11**, 195–204, 1991.