# Symbolic Summation with Radical Expressions

Manuel Kauers*
RISC-Linz
Johannes Kepler Universität
A-4040 Linz, Austria
mkauers@risc.uni-linz.ac.at

Carsten Schneider*
RISC-Linz
Johannes Kepler Universität
A-4040 Linz, Austria
cschneid@risc.uni-linz.ac.at

## ABSTRACT

An extension of Karr's summation algorithm is presented by which symbolic sums involving radical expressions can be simplified. We discuss the construction of appropriate difference fields as well as algorithms for solving difference equations in these fields. The paper is concluded by a list of identities found with an implementation of our techniques.

## Categories and Subject Descriptors

I.1.2 [**Computing Methodologies**]: Symbolic and Algebraic Manipulation—*Algorithms*; G.2.1 [**Discrete Mathematics**]: Combinatorics—*Recurrences and difference equations*

## General Terms

Algorithms

## Keywords

Symbolic Summation, Difference Fields

## 1. INTRODUCTION

The algorithm of Karr [6] has often been called the summation analogue to Risch's integration algorithm [10]. Both algorithms are applicable only to expressions composed from building blocks that are algebraically independent. For the integration case, Bronstein [2] was able to remove this restriction by giving a generalized integration algorithm that can handle elementary functions with arbitrary algebraic relations among them.

No summation analogue to this algorithm is known. Even worse, while algebraic functions naturally belong to the elementary functions, it is not clear what the most natural class of sequences is that a summation algorithm allowing algebraic relations should target on. In this paper, we consider the most literal analogue: we provide a simplifier for symbolic sums that allows radical expressions to appear in the summand. A simple example for such a sum is

$$\sum_{k=0}^{n}(k-\sqrt{k}+1)\sqrt{k!}.$$

Continuing earlier work [13, 11, 8, 7] on extending Karr's algorithm, we have obtained algorithms for handling telescoping, creative telescoping [9] and recurrence solving for nested sums and products involving radical expressions.

Our algorithms are correct and complete as long as the difference fields by which the radical expressions are represented are properly constructed. In the construction of the difference field for a given expression, we need to assume a very deep algebraic property of the sequences corresponding to the expression. We do believe that this assumption is justified for most algebraic sequences, but we are not able to show it even for the simple sequence $\sqrt{n}$.

It is therefore important to note that on expressions for which the assumption is wrong (or undecided), our algorithms remain correct, but completeness may be lost: every identity found by the algorithm is true, but identities may be overlooked or the algorithms may inadvertently run into a division by zero. We have implemented our algorithms as a supplement to the summation package Sigma [14], and while experimenting with this implementation, we have never observed any failure due to a violated assumption. A collection of identities found with our implementation is given in Section 7. As summation identities involving radical expressions appear only very sparsely in the literature, this collection is likely to contain previously unpublished identities.

## 2. PRELIMINARIES

Let $(\mathbb{F},\sigma)$ be a difference field, i.e., a field[1] $\mathbb{F}$ together with a field automorphism $\sigma:\mathbb{F}\to\mathbb{F}$. Then indefinite summation can be formulated as follows: Given $f\in\mathbb{F}$, find $g\in\mathbb{F}$ with

$$\sigma(g)-g=f. \tag{1}$$

Namely, if we can model a sequence $f'(k)$ with $f\in\mathbb{F}$ by the shift $f'(k+1)\equiv\sigma(f)$, then we solve the telescoping problem. More generally, we are interested in solving parameterized linear difference equations. Here we need the set of constants

$$\text{const}_\sigma\mathbb{F}:=\{c\in\mathbb{F}|\sigma(c)=c\}.$$

*Both authors were supported by the Austrian science foundation FWF, grants P16613-N12 and SFB F1305.

[1]All fields are commutative, contain $\mathbb{Q}$, and are computable.

Note that $\text{const}_\sigma \mathbb{F}$ is a subfield of $\mathbb{F}$. In particular, it follows that $\mathbb{Q}$ is a subfield of $\text{const}_\sigma \mathbb{F}$.

**Parameterized linear difference equations (PLDE):** *Given* $(\mathbb{F}, \sigma)$ with $\mathbb{K} := \text{const}_\sigma \mathbb{F}$, $a_0, \dots, a_r \in \mathbb{F}$ (not all zero) and $f_1, \dots, f_m \in \mathbb{F}$. *Find* all $g \in \mathbb{F}$, $c_0, \dots, c_m \in \mathbb{K}$ such that

$$a_0 g + a_1 \sigma(g) + \dots + a_r \sigma^r(g) = c_1 f_1 + \dots + c_m f_m. \quad (2)$$

Note that $\mathbb{V} := \{(c_1, \dots, c_m, g) \in \mathbb{K}^m \times \mathbb{F} | c_i, g \text{ is a solution of (2)}\}$ is a vector space of $\mathbb{K}$ which has dimension $\leq m+r$. Hence problem PLDE is solved by finding a basis of $\mathbb{V}$.

The following prominent summation problems [9] are covered by the PLDE-problem; for further details see [14]:

1. Telescoping (1) can be obtained by restricting to $r = m = 1$ with $a_0 = -1$ and $a_1 = 1$.
2. Zeilberger's creative telescoping can be formulated by restricting to $r = 1$ with $a_0 = -1$ and $a_1 = 1$ and setting $f_i \equiv f'(n + i - 1, k)$ for a parameter $n$ which occurs in the constant field $\mathbb{K}$.
3. Solving linear difference equations (recurrences) can be handled by setting $m = 1$.
4. PLDEs are the backbone to treat the telescoping and creative telescoping problem for rather general classes of holonomic and $\partial$-finite sequences, see, e.g., [12].

Problem PLDE can be solved for the rational case $\mathbb{F} = \mathbb{K}(k)$ with $\sigma(k) = k+1$ and the $q$-rational case $\mathbb{F} = \mathbb{K}'(q)(k)$ where $q$ is transcendental over $\mathbb{K}'$ and $\sigma(k) = q\,k$; for the corresponding literature we refer to [13, p 801].

More generally, algorithms and methods exist for $\Pi\Sigma^*$-extensions which allow to model nested sums and products. Those difference fields are defined by difference field extensions. A difference field $(\mathbb{E}, \sigma)$ is a difference field extension of a difference field $(\mathbb{F}, \sigma')$ if $\mathbb{F}$ is a subfield of $\mathbb{E}$ and $\sigma' = \sigma|_{\mathbb{F}}$; usually we do not distinguish $\sigma$ and $\sigma'$.

*Definition 1.* A $\Pi\Sigma^*$*-extension* $(\mathbb{F}(t), \sigma)$ of $(\mathbb{F}, \sigma)$ is a difference field extension where $\sigma(t) = t + a$ or $\sigma(t) = a\,t$ for some $a \in \mathbb{F}^*$ and $\text{const}_\sigma \mathbb{F}(t) = \text{const}_\sigma \mathbb{F}$. More generally, a tower of such $\Pi\Sigma^*$-extensions is called a $\Pi\Sigma^*$-extension.

Karr [6] presented algorithms that solve problem PLDE with $r = 1$ for the so-called $\Pi\Sigma^*$-fields: these are $\Pi\Sigma^*$-extensions $(\mathbb{E}, \sigma)$ of $(\mathbb{G}, \sigma)$ where $\text{const}_\sigma \mathbb{G} = \mathbb{G}$. Analyzing Karr's machinery [6], it turns out that one can lift various algorithmic properties from the ground field $(\mathbb{G}, \sigma)$ (not necessarily the constant field) to the field $(\mathbb{E}, \sigma)$. E.g., we obtain the following result [8].

THEOREM 1. *Let* $(\mathbb{E}, \sigma)$ *be a* $\Pi\Sigma^*$*-extension of* $(\mathbb{G}, \sigma)$*. If* $(\mathbb{G}, \sigma)$ *is* $\sigma^*$*-computable (see Definition 2 below) and one can solve PLDEs with* $r = 1$ *for* $(\mathbb{G}, \sigma)$*, then* $(\mathbb{E}, \sigma)$ *is* $\sigma^*$*-computable and one can solve PLDEs with* $r = 1$ *for* $(\mathbb{E}, \sigma)$*.*

Moreover, we get the following result; see [11, 8].

THEOREM 2. *Let* $(\mathbb{E}, \sigma)$ *be a* $\Pi\Sigma^*$*-extension of* $(\mathbb{G}, \sigma)$*. If* $(\mathbb{G}, \sigma)$ *is* $\sigma^*$*-computable and one can solve PLDEs with* $r = 1$ *for* $(\mathbb{G}, \sigma)$*, there is an algorithm for problem DOS*[2]*.*

[2]Note that the $\Pi\Sigma^*$-extension $(\mathbb{E}, \sigma)$ of $(\mathbb{G}, \sigma)$ itself must be constructed in a refined form. Again, if $(\mathbb{G}, \sigma)$ is $\sigma^*$-computable, this task can be accomplished.

**Depth optimal summation (DOS):** *Given* a $\Pi\Sigma^*$-extension $(\mathbb{E}, \sigma)$ of $(\mathbb{G}, \sigma)$ and $f \in \mathbb{E}$. *Find*, if possible, a $\Pi\Sigma^*$-extension $(\mathbb{D}, \sigma)$ of $(\mathbb{E}, \sigma)$ such that $g \in \mathbb{D}$ with (1) and such that the additional sums and products introduced by the extension $\mathbb{D}$ are not more nested than the already given sums and products occurring in $f$.

Furthermore, by Theorem 5.7 in [13] we obtain the following result if one can solve problem PLDE in the ground field $(\mathbb{G}, \sigma)$ by a recursive enumeration procedure; i.e. there is a method that produces after finitely many solve-attempts all solutions.

THEOREM 3. *Let* $(\mathbb{E}, \sigma)$ *be a* $\Pi\Sigma^*$*- extension of* $(\mathbb{G}, \sigma)$*. If* $(\mathbb{G}, \sigma)$ *is* $\sigma^*$*-computable and one can solve PLDEs for* $(\mathbb{G}, \sigma)$ *by an enumerative procedure, then one can solve PLDEs for* $(\mathbb{E}, \sigma)$ *by an enumerative procedure.*

**SUMMARY.** For a $\Pi\Sigma^*$-extension $(\mathbb{E}, \sigma)$ of $(\mathbb{G}, \sigma)$ where $(\mathbb{G}, \sigma)$ is $\sigma^*$-computable we can produce in a systematic fashion all solutions of a given PLDE (Theorem 3). Moreover, if one can solve all first order PLDEs in $(\mathbb{G}, \sigma)$, then one can solve all first order PLDEs in $(\mathbb{E}, \sigma)$ (Theorem 1); in particular, there are algorithms for DOS (Theorem 2).

So far it has been shown that the following two difference fields $(\mathbb{G}, \sigma)$ satisfy these properties:

1. $(\mathbb{G}, \sigma)$ with $\text{const}_\sigma \mathbb{G} = \mathbb{G}$; see [6, 8].
2. $(\mathbb{G}, \sigma)$ is a tower of free difference field extensions over the constant field; see [8, 7].

In this article we show that those properties hold also for what we call radical extensions (see Definition 4 below). In combination with Theorem 1 we obtain completely new input classes of difference fields for our algorithms.

Finally, we define $\sigma^*$-computability. Here we need the following notions.

Let $(\mathbb{F}, \sigma)$ be a difference field. For $f \in \mathbb{F}^*$ we define

$$f_{(k,\sigma)} := \begin{cases} f\sigma(f)\dots\sigma^{k-1}(f) & \text{if } k > 0 \\ \frac{1}{\sigma^{-1}(f)\dots\sigma^{-k}(f)} & \text{if } k < 0 \end{cases},$$

$f_{(0,\sigma)} := 1$, and

$$f_{\{k,\sigma\}} := \begin{cases} f_{(0,\sigma)} + f_{(1,\sigma)} + \dots + f_{(k-1,\sigma)} & \text{if } k > 0 \\ -(f_{(-1,\sigma)} + \dots + f_{(k,\sigma)}) & \text{if } k < 0, \end{cases}$$

$f_{(0,k)} := 0$. If it is clear from the context we also write $f_{(k)} := f_{(k,\sigma)}$ and $f_{\{k\}} := f_{\{k,\sigma\}}$.

We call $(\mathbb{F}, \sigma)$ torsion-free, if for all $k \in \mathbb{Z} \setminus \{0\}$ and all $g \in \mathbb{F}^*$ the equality $\left(\frac{\sigma(g)}{g}\right)^k = 1$ implies $\frac{\sigma(g)}{g} = 1$.

*Definition 2.* A difference field $(\mathbb{F}, \sigma)$ is $\sigma^*$-computable if the following holds.

1. There is an algorithm that factors multivariate polynomials over $\mathbb{F}$.
2. $(\mathbb{F}, \sigma^k)$ is torsion free for all $k \in \mathbb{Z}$.
3. $\Pi$**-Regularity.** Given $f, g \in \mathbb{F}$ with $f$ not a root of unity, there is at most one $n \in \mathbb{Z}$ such that $f_{(n,\sigma)} = g$. There is an algorithm that finds, if possible, this $n$.

4. **$\Sigma$-Regularity.** Given $k \in \mathbb{Z} \setminus \{0\}$ and $f, g \in \mathbb{F}$ with $f = 1$ or $f$ not a root of unity, there is at most one $n \in \mathbb{Z}$ such that $f_{\{n,\sigma^k\}} = g$. There is an algorithm that finds, if possible, this $n$.

5. **Orbit-Problem.** There is an algorithm that solves the orbit problem: Given $(\mathbb{F}, \sigma)$ and $f_1, \dots, f_m \in \mathbb{F}^*$, find a basis of the following $\mathbb{Z}$-module:

$$M(f_1, \dots, f_m; \mathbb{F}) := \{ (e_1, \dots, e_m) \in \mathbb{Z}^m \mid \exists g \in \mathbb{F}^* : f_1^{e_1} \cdots f_m^{e_m} = \tfrac{\sigma(g)}{g} \}. \quad (3)$$

# 3. RADICAL EXTENSIONS

Given a field $\mathbb{G}$, $\mathbb{G}\{x\}$ denotes the ring

$$\mathbb{G}\{x\} := \mathbb{G}[\dots, x_{-2}, x_{-1}, x_0, x_1, x_2, \dots]$$

with infinitely many variables $x_i$, $i \in \mathbb{Z}$. Note that for any $f \in \mathbb{G}\{x\}$ we can take a polynomial ring $\mathbb{G}[x_l, \dots, x_r]$ which contains $f$. Obviously, $\mathbb{G}\{x\}$ is an integral domain.

A difference ring $(\mathbb{A}, \sigma)$ is a ring $\mathbb{A}$ with a ring automorphism $\sigma$; $(\mathbb{A}, \sigma)$ is a difference ring extension of $(\mathbb{B}, \sigma')$ if $\mathbb{B}$ is a subring of $\mathbb{A}$ and $\sigma' = \sigma|_{\mathbb{B}}$.

*Definition 3.* A difference ring extension $(\mathbb{F}, \sigma)$ of $(\mathbb{G}, \sigma)$ is *free* if $\mathbb{F} = \mathbb{G}\{x\}$ and $\sigma(x_i) := x_{i+1}$ for $i \in \mathbb{Z}$.

Let $(\mathbb{G}\{x\}, \sigma)$ be a free difference ring extension of $(\mathbb{G}, \sigma)$ and let $I$ be a difference ideal of $\mathbb{G}\{x\}$, i.e., $I$ is an ideal of $\mathbb{G}\{x\}$ which is closed under $\sigma$. Moreover let $\mathbb{G}\{x\}/I$ be the quotient ring of the integral domain $\mathbb{G}\{x\}$ modulo the ideal $I$. Since the elements $\mathbb{G}$ can be naturally embedded in $\mathbb{G}\{x\}/I$, we consider $\mathbb{G}\{x\}/I$ as a ring extension of $\mathbb{G}$. Moreover, $\mathbb{G}\{x\}/I$ is a field iff $I$ is a maximal ideal.
Finally, we consider the map $\sigma' : \mathbb{G}\{x\}/I \to \mathbb{G}\{x\}/I$ with

$$\sigma'(a + I) := \sigma(a) + I;$$

note that $\sigma'|_{\mathbb{G}} = \sigma$. Since $I$ is a difference ideal, it is easy to see that $\sigma'$ is a ring automorphism.

Summarizing, given a difference ideal $I$, we obtain the difference ring extension $(\mathbb{G}\{x\}/I, \sigma')$ of $(\mathbb{G}, \sigma)$. In particular we get a difference field extension if and only if the ideal $I$ is maximal. We identify $\sigma$ and $\sigma'$ from now on.

In this article, we are interested in difference ideals $I = \langle\!\langle p \rangle\!\rangle$ which are generated by a polynomial $p \in \mathbb{G}[x_0]$, i.e., the ideal is given by

$$\langle\!\langle p \rangle\!\rangle := \langle \dots, \sigma^{-2}(p), \sigma^{-1}(p), p, \sigma(p), \sigma^2(p), \dots \rangle. \quad (4)$$

Clearly, if $\deg(p) > 0$, $\langle\!\langle p \rangle\!\rangle \neq \mathbb{G}\{x\}$. In order to turn the difference ring $(\mathbb{G}\{x\}/\langle\!\langle p \rangle\!\rangle, \sigma)$ to a field, we need in addition the property that $\langle\!\langle p \rangle\!\rangle$ is maximal. This leads to the following definition.

*Definition 4.* A difference field extension $(\mathbb{G}\{x\}/\langle\!\langle p \rangle\!\rangle, \sigma)$ of $(\mathbb{G}, \sigma)$ is called a *simple algebraic extension* if $p \in \mathbb{G}[x_0]$, $d := \deg(p) > 1$, and the difference ideal $\langle\!\langle p \rangle\!\rangle$ is maximal. A simple algebraic extension is called *radical extension* if $p = x_0^d - h$ for some $d > 1$ and $h \in \mathbb{G}$.

It seems to be rather difficult to show for a particular $p$ that $\langle\!\langle p \rangle\!\rangle$ is maximal.

*Example 1.* It has been shown [5, Thm. 7] by non-trivial arguments that the sequence $x_n := \sqrt{n}$ is not holonomic. Namely, if $\mathbb{K}$ is a subfield of the complex numbers, then there is no relation of the form

$$p_0(n)x_n + \dots + p_d(n)x_{n+d} = 0, \ \forall n \geq 0$$

for polynomials $p_i(n) \in \mathbb{K}[n]$. To show that there is no polynomial $p(y_0, \dots, x_r) \in \mathbb{K}[n][y_0, \dots, y_r]$ with

$$p(x_n, \dots, x_{n+r}) = 0, \ \forall n \geq 0 \quad (5)$$

and $\deg_{y_i}(p) < 2$ is even more challenging. But this is exactly what we need to model $\sqrt{n}$ in a radical extension. More precisely, let $(\mathbb{K}(n), \sigma)$ with $\sigma(n) = n + 1$ be the ground field and consider the free difference field extension $(\mathbb{K}(n)\{x\}, \sigma)$ of $(\mathbb{K}(n), \sigma)$. Then we could identify $x_i$ with $\sqrt{n+i}$ in $\mathbb{K}(n)\{x\}/\langle\!\langle x_0^2 - n \rangle\!\rangle$ if $\langle\!\langle x_0^2 + n \rangle\!\rangle$ is maximal, i.e., no relations of the form (5) exist.

Motivated by all our computations, see Sections 7, we strongly believe that $I := \langle\!\langle x_0^d - n \rangle\!\rangle$ for $d > 1$ is maximal in $\mathbb{K}(n)\{x\}$ with $\sigma(n) = n + 1$. I.e., we conjecture that $(\mathbb{K}(n)\{x\}/I, \sigma)$ is a radical extension of $(\mathbb{K}(n), \sigma)$. The following question is immediate.

QUESTION 1. *Let $(\mathbb{G}(t), \sigma)$ be a $\Pi\Sigma^*$-extension of $(\mathbb{G}, \sigma)$ and $d > 0$. For which $h \in \mathbb{G}(t)$ is the difference ideal $I := \langle\!\langle x_0^d - h \rangle\!\rangle$ in $\mathbb{G}(t)\{x\}$ maximal? Even stronger, are there decision procedures?*

Subsequently, we collect some basic properties of a simple algebraic extension $(\mathbb{G}\{x\}/\langle\!\langle p \rangle\!\rangle, \sigma)$ of $(\mathbb{G}, \sigma)$.
Consider the maximal ideal

$$\langle\!\langle p \rangle\!\rangle_{l,r} := \langle \sigma^l(p), \sigma^{l+1}(p), \dots, \sigma^r(p) \rangle \quad (6)$$

in $\mathbb{G}[x_l, \dots, x_r]$ which is contained in $\langle\!\langle p \rangle\!\rangle$. Notice that $\langle\!\langle p \rangle\!\rangle_{l,r}$ is not a difference ideal. If $\langle\!\langle p \rangle\!\rangle_{l,r}$ is maximal, then also $\langle\!\langle p \rangle\!\rangle_{l+i,r+i}$ is maximal in $\mathbb{G}[x_{l+i}, \dots, x_{r+i}]$ for all $i \in \mathbb{Z}$; this follows by applying the automorphism $\sigma$. Moreover, all $\langle\!\langle p \rangle\!\rangle_{\lambda,\rho}$ with $l \leq \lambda \leq \rho \leq r$ are also maximal ideals in $\mathbb{G}[x_\lambda, \dots, x_\rho]$. Summarizing, we can assume that $\mathbb{G}[x_{\lambda+i}, \dots, x_{\rho+i}]/\langle\!\langle p \rangle\!\rangle_{\lambda+i,\rho+i}$ is a subfield of $\mathbb{G}\{x\}/\langle\!\langle p \rangle\!\rangle$ for all $l \leq \lambda \leq \rho \leq r$ and all $i \in \mathbb{Z}$.

LEMMA 1. *Let $(\mathbb{G}\{x\}, \sigma)$ be a free difference ring extension of the difference field $(\mathbb{G}, \sigma)$ and let $p \in \mathbb{G}[x_0]$ with degree $d > 0$. Let $\langle\!\langle p \rangle\!\rangle_{l,r}$ be a maximal ideal with $l < r$. Then the following holds.*

1. *The elements of $\mathbb{E} := \mathbb{G}[x_l, \dots, x_r]/\langle\!\langle p \rangle\!\rangle_{l,r}$ are uniquely represented in*
$$R_d := \{ f \in \mathbb{G}[x_l, \dots, x_r] \mid \deg_{x_i}(f) < d \text{ for } l \leq i \leq r \}.$$
2. *For $l \leq k < r$, $\sigma^k(p) \in (\mathbb{G}[x_l, \dots, x_k]/\langle\!\langle p \rangle\!\rangle_{l,k-1})[x_k]$ is irreducible.*
3. *The elements in $\mathbb{G}[x_l, \dots, x_r]/\langle\!\langle p \rangle\!\rangle_{l,r}$ can be inverted by the extended Euclidean algorithm.*

PROOF. **(1)** By (6) the elements from $\mathbb{E}$ can be written in the form $a + \langle\!\langle p \rangle\!\rangle_{l,r}$ where $a \in R_d$. Now let $a, b \in R_d$ with $a \neq b$ and $a + \langle\!\langle p \rangle\!\rangle_{l,r} = b + \langle\!\langle p \rangle\!\rangle_{l,r}$. Then $a - b \in \langle\!\langle p \rangle\!\rangle_{l,r}$. Since $a - b \in R_d$, $a - b = 0$. This proves uniqueness.
**(2)** Suppose $\sigma^k(p)$ is not irreducible. Then there are $a, b \in$

$\mathbb{G}[x_l,\ldots,x_{k-1}]/\langle\!\langle p\rangle\!\rangle_{l,k-1}[x_k]$ with $d > \deg(a),\deg(b) > 0$ and $a\,b = \sigma^k(p)$. Hence we get zero-divisors in the field $\mathbb{E}$, a contradiction.
**(3)** Let $a \in \mathbb{E}^*$. If $a \in \mathbb{G}$, we can compute $a^{-1}$ by assumption. Otherwise, suppose we can invert elements from the field $\mathbb{F} := \mathbb{G}[x_l,\ldots,x_r]/\langle\!\langle p\rangle\!\rangle_{l,r-1}$. If $a \in \mathbb{F}$, we are done. Otherwise, $a \in \mathbb{F}[x_r]/\langle\sigma^r(p)\rangle(=\mathbb{E})$. By part (2) there exist $\alpha,\beta \in \mathbb{F}[x_r]$ such that $\alpha\,a + \beta\,\sigma^r(p) = 1$. Such $\alpha,\beta$ can be computed by the extended Euclidean algorithm. Consequently, $\alpha$ is the inverse element of $f$. □

If we write $a+\langle\!\langle p\rangle\!\rangle_{l,r} \in \mathbb{G}\{x\}/\langle\!\langle p\rangle\!\rangle_{l,r}$ or $a+\langle\!\langle p\rangle\!\rangle \in \mathbb{G}\{x\}/\langle\!\langle p\rangle\!\rangle$ we assume that $a$ is in normal form, i.e., $a \in R_d$. In particular, if we say that $x_i$ occurs in $a \in \mathbb{G}\{x\}$, then we mean that $x_i$ occurs in the normal form of $a$.

*Remark 1.* Let $(\mathbb{G},\sigma)$ be $\sigma^*$-computable, this means we can factorize polynomials over $\mathbb{G}$. Then Lemma 1.2 tells us how we can check algorithmically if $\langle\!\langle p\rangle\!\rangle_{l,r}$ is maximal:
Namely, suppose that we have checked already that $\langle\!\langle p\rangle\!\rangle_{l,i-1}$ is maximal in $\mathbb{G}[x_l,\ldots,x_{i-1}]$. Moreover, suppose that we have constructed an irreducible polynomial $q \in \mathbb{G}[y]$ such that $\mathbb{F} := \mathbb{G}[y]/\langle q\rangle = \mathbb{G}[x_l,\ldots,x_{i-1}]/\langle\!\langle p\rangle\!\rangle_{l,i-1}$. Then with the algorithms presented in [15] we can check if $\sigma^i(p) \in \mathbb{F}[x_i]$ is irreducible. If $\sigma^i(p)$ is reducible, $\langle\!\langle p\rangle\!\rangle_{l,i}$ and therefore $\langle\!\langle p\rangle\!\rangle_{l,r}$ are not maximal. Otherwise, if $\sigma^i(p)$ is irreducible, $\langle\!\langle p\rangle\!\rangle_{l,i}$ is maximal. In particular, we can construct a new irreducible polynomial $q' \in \mathbb{G}[y]$ such that $\mathbb{F}' := \mathbb{G}[y]/\langle q'\rangle \simeq \mathbb{G}[x_l,\ldots,x_i]/\langle\!\langle p\rangle\!\rangle_{l,i}$. Iterating this procedure for $i = 1,\ldots,r$ completes the job.

LEMMA 2. *Let $(\mathbb{F},\sigma)$ with $\mathbb{F} = \mathbb{G}\{x\}/\langle\!\langle p\rangle\!\rangle$ be a simple algebraic extension of $(\mathbb{G},\sigma)$ and $k \in \mathbb{Z}\setminus\{0\}$. Then:*

1. *If $g \in \mathbb{F}\setminus\mathbb{G}$, then $\frac{\sigma^k(g)}{g} \notin \mathbb{G}$.*
2. *If $f \in \mathbb{F}\setminus\mathbb{G}$, then for any $n \in \mathbb{Z}\setminus\{0\}$ we have $f^n \neq 1$, $f_{(n,\sigma^k)} \in \mathbb{F}\setminus\mathbb{G}$, and $f_{\{n,\sigma^k\}} \in \mathbb{F}\setminus\mathbb{G}$.*
3. *$\mathrm{const}_\sigma\mathbb{F} = \mathrm{const}_\sigma\mathbb{G}$.*

PROOF. **(1)** Assume $g \in \mathbb{F}\setminus\mathbb{G}$ where $f := \frac{\sigma(g)}{g} \in \mathbb{G}$. Let $r$ be maximal such that $g$ depends on $x_r$. Then $\sigma^k(g)$ depends on $x_{r+k}$, a contradiction to $\sigma(g) = f\,g$.
**(2)** Let $n \in \mathbb{Z}\setminus\{0\}$ and $f \in \mathbb{F}\setminus\mathbb{G}$; let $r \in \mathbb{Z}$ be maximal and $l$ be minimal such that $f$ depends on $x_r$, $x_l$, respectively.
The property $f^n = 1$ for some $n$ will lead to a contradiction. Note that we can assume that $n > 0$ (If $n < 0$, take $1/f$ instead of $f$). Since $1 = \sigma^i(f^n) = (\sigma^i(f))^n$, the polynomial $Y^n - 1$ has the roots $\sigma^i(f)$ for $i \geq 0$. Note that $i + r$ is maximal such that $x_{i+r}$ occurs in $\sigma^i(f)$. Hence all the roots $\sigma^i(f)$ are different. But $Y^n - 1$ can have at most $n$ roots, a contradiction. Hence $f^n \neq 1$ for any $n \in \mathbb{Z}\setminus\{0\}$.
Note that $x_{(n-1)\,k+r}$ occurs in $f_{(n,\sigma^k)}$ and in $f_{\{n,\sigma^k\}}$ if $n > 0$ and $k > 0$. Similar arguments (using also the minimal index $l$) for the cases $(n > 0, k < 0)$, $(n < 0, k > 0)$, $(n < 0, k < 0)$ show that $f_{(n,\sigma^k)}, f_{\{n,\sigma^k\}} \notin \mathbb{G}$ for all $k, n \notin \mathbb{Z}\setminus\{0\}$.
**(3)** Let $\mathbb{K} := \mathrm{const}_\sigma\mathbb{G}$, $\mathbb{K}' := \mathrm{const}_\sigma\mathbb{F}$. Clearly, $\mathbb{K} \subseteq \mathbb{K}'$. Now let $g \in \mathbb{K}'$. With $\sigma(g) = g$ and part (1), $g \in \mathbb{G}$. Hence $g \in \mathbb{K}$. □

# 4. $\sigma^*$-COMPUTABILITY

We show in this section that certain radical extensions are compatible with $\Pi\Sigma$-extensions: radical extensions of $\sigma^*$-computable fields are again $\sigma^*$-computable.

THEOREM 4. *Let $(\mathbb{G},\sigma)$ be a $\sigma^*$-computable field, $\mathbb{G}(t)$ be a $\Pi\Sigma$-extension of $\mathbb{G}$ and let $\mathbb{F} := \mathbb{G}(t)\{x\}/\langle\!\langle P\rangle\!\rangle$ be a radical extension of $\mathbb{G}(t)$, where $P = x_0^d - h(t)$ for some irreducible polynomial $h \in \mathbb{G}[t]$. Then $(\mathbb{F},\sigma)$ is $\sigma^*$-computable.*

In order to prove that $\mathbb{F}$ is $\sigma^*$-computable, we need to show that this difference field satisfies the conditions listed in Definition 2. Condition 1 is clear under the assumption that the subfield $\mathbb{G}$ is $\sigma^*$-computable. Conditions 2–4 are settled by the following proposition.

PROPOSITION 1. *Let $(\mathbb{F},\sigma)$ with $\mathbb{F} = \mathbb{G}\{x\}/\langle\!\langle p\rangle\!\rangle$ be a simple algebraic extension of $(\mathbb{G},\sigma)$ where $(\mathbb{G},\sigma)$ is $\sigma^*$-computable. Let $f,g \in \mathbb{F}$ and $k \in \mathbb{Z}\setminus\{0\}$.*

1. *$(\mathbb{F},\sigma^k)$ is torsion-free.*
2. *($\Pi$-Regularity) If $f$ is not a root of unity, there is at most one $n \in \mathbb{Z}$ such that $f_{(n,\sigma)} = g$. If $n$ exists, it can be computed.*
3. *($\Sigma$-Regularity) If $f = 1$ or $f$ is not a root of unity, there is at most one $n \in \mathbb{Z}$ such that $f_{\{n,\sigma^k\}} = g$. If $n$ exists, it can be computed.*

PROOF. **(1)** Let $g \in \mathbb{F}^*$ and set $f := \sigma^k(g)/g \in \mathbb{F}^*$. Suppose that $f^n = 1$ for some $n \in \mathbb{Z}\setminus\{0\}$. By Lemma 2.2 it follows that $f \in \mathbb{G}$. Then also $g \in \mathbb{G}$ by Lemma 2.1. Since $(\mathbb{G},\sigma)$ is torsion-free, $f = 1$.
**(2)** Algorithms for deciding $\Pi$ regularity can be obtained as follows. Let $f,g \in \mathbb{F}$ where $f$ is not a root of unity.
First suppose that $f \in \mathbb{G}$. Then $f_{(n,\sigma)} \in \mathbb{G}$. Hence, if $g \notin \mathbb{G}$, there is no solution $n$. If also $g \in \mathbb{G}$, there is at most one $n$ such that $f_{(n,\sigma)} = g$ by assumption. In particular, there is an algorithm to compute $n$, if it exists.
Next, suppose $f \notin \mathbb{G}$. Then $f_{(n,\sigma)} \notin \mathbb{G}$ by Lemma 2.2. If $g \in \mathbb{G}$, the only choice is $n = 0$; check this candidate.
Finally, consider the case $f,g \in \mathbb{F}\setminus\mathbb{G}$. Here the solution $n = 0$ is not possible. Let $r_f, r_g$ be the maximum index $i$ such that $x_i$ occurs in $f,g$, respectively. Similarly, let $l_f, l_g$ be the minimum index. If for the possible $n$ we have $n > 0$, the maximum index $i$ for which $x_i$ occurs in $f_{(n,\sigma)}$ is $n - 1 + r_f$. Therefore, $g = f_{(n,\sigma)}$ can only occur if $n = r_g - r_f + 1$. Hence there is at most one solution $n > 0$ and it suffices to check this candidate. Notice that a solution $n > 0$ implies that $l_g = l_f$. Similarly, if $n < 0$, then we get the constraint $n = l_g - l_f$. Again, we can conclude that there is at most one negative solution, and, in case of existence, it can be computed. Moreover, if there is such a solution, it follows that $r_g = r_f$. This proves in addition that there is either a positive or a negative solution. Summarizing, there is at most one solution $n \in \mathbb{Z}$.
**(3)** $\Sigma$-regularity can be shown along the lines of **(2)**. □

It only remains to provide an algorithm for solving the OHG problem. In the remainder of this section, we describe an algorithm for reducing the OHG problem in $\mathbb{F}$ to OHG problems in the ground field $\mathbb{G}$. We use terminology from the theory of algebraic functions [3], similar reasoning is used in Bronstein's integration algorithm for algebraic functions [2]. In particular, for $f \in \mathbb{F}$ and a place $p$, we write $\nu_p(f)$ for the order of $f$ at $p$.

By $P = x_0^d - h(t)$ with $h$ irreducible, it follows that every $x_i$ is singular at precisely one finite place $p_i$, and we have $\nu_p(f) = 1/d$. We call these the critical places, and write $\Sigma := \{p_i : i \in \mathbb{Z}\}$ for the set of critical places.

*Example 2.* Let $\mathbb{F} := \mathbb{Q}(n)\{x\}/\langle\langle x_0^2 - n\rangle\rangle$ with $\sigma(n) = n+1$. Here, $x_i$ corresponds to $\sqrt{n+i}$ ($i \in \mathbb{Z}$) and has its singular place $p_i$ over $n = -i$. We have $\nu_{p_i}(x_i) = 1/2$ and $\nu_p(x_i) = 0$ for all other finite places.

Let $f_1, \ldots, f_m \in \mathbb{F}^*$ be given. We seek a basis for the $\mathbb{Z}$-module $M(f_1, \ldots, f_m; \mathbb{F})$.

Karr [6] solves the OHG problem in transcendental extensions by factoring numerators and denominators of the $f_i$, grouping shift equivalent factors and determining exponent vectors that cancel disturbing factors. In the algebraic case, factorization has no meaning. We will mimic Karr's OHG algorithm by considering singularities of the $f_i$ instead of irreducible factors. To make this work, we need the following observations.

LEMMA 3. *We have*

$$\nu_p(f) \in \begin{cases} \mathbb{Z} & \text{if } p \notin \Sigma \\ \frac{1}{\deg P}\mathbb{Z} & \text{if } p \in \Sigma \end{cases}$$

*for all $f \in \mathbb{F}^*$ and for all finite places $p$.*

PROOF. For $p \notin \Sigma$ there is nothing to prove. If $p \in \Sigma$, then, by assumption on $\mathbb{F}$, there is exactly one index $i$ such that $p$ is a singular place of $x_i$. Write $f = \sum_e a_e x_l^{e_l} \cdots x_r^{e_r}$ for appropriate $l, r \in \mathbb{Z}$ and $e = (e_l, \ldots, e_r) \in \mathbb{Z}^{r-l+1}$. Then

$$\nu_p(f) = \max_e \Big( \underbrace{\nu_p(a_e)}_{\in\mathbb{Z}} + \sum_{j\neq i} \underbrace{e_j \nu_p(x_j)}_{\in\mathbb{Z}} + \underbrace{e_i \nu_p(x_i)}_{\in \frac{1}{\deg P}\mathbb{Z}} \Big)$$

and the claim follows. □

LEMMA 4. *Let $p \in \Sigma$ and $\nu \in \frac{1}{\deg P}\mathbb{Z}$. Then there exists $g \in \mathbb{F}$ such that $\nu_p(g) = \nu$ and $\nu_q(g) = 0$ for all $q \neq p$.*

PROOF. If $i$ is such that $p$ is the branch place of $x_i$, then $g := x_i^{\nu \deg P}$ does the job. □

LEMMA 5. *Let $p_l, \ldots, p_r$ be the branch places of $x_l, \ldots, x_r$ and let $\nu_l, \ldots, \nu_r \in \frac{1}{\deg P}\mathbb{Z}$ be such that $\sum_i \nu_i = 0$. Then there exists $g \in \mathbb{F}$ such that*

$$\nu_{p_i}(\sigma(g)/g) = \nu_i \quad (i = l, \ldots, r)$$

*and $\nu_p(\sigma(g)/g) = 0$ for $p \notin \{p_l, \ldots, p_r\}$.*

PROOF. By Lemma 4, for each $i = l, \ldots, r$ we can find elements $g_i \in \mathbb{F}$ with $\nu_{p_i}(g_i) = -\sum_{j=l}^{i} \nu_j$ and $\nu_p(g_i) = 0$ for $p \neq p_i$. Set $g := \prod_{i=l}^{r} g_i$. Then

$$\nu_{p_l}(\sigma(g)/g) = \nu_{p_l}(\sigma(g)) - \nu_{p_l}(g) = 0 - (-\nu_l) = \nu_l$$

and for $i = l+1, \ldots, r$ we have

$$\begin{aligned} \nu_{p_i}(\sigma(g)/g) &= \nu_{p_i}(\sigma(g)) - \nu_{p_i}(g) = \nu_{p_{i-1}}(g) - \nu_{p_i}(g) \\ &= -\sum_{j=l}^{i-1} \nu_j - \Big(-\sum_{j=l}^{i} \nu_j\Big) = \nu_i. \end{aligned}$$

Furthermore,

$$\begin{aligned} \nu_{p_{r+1}}(\sigma(g)/g) &= \nu_{p_{r+1}}(\sigma(g)) - \nu_{p_{r+1}}(g) \\ &= \nu_{p_r}(g) - \nu_{p_{r+1}}(g) = -\sum_{j=l}^{r} \nu_j - 0 = 0 \end{aligned}$$

and obviously $\nu_p(\sigma(g)/g) = 0$ for $p \notin \{p_l, \ldots, p_{r+1}\}$. □

The automorphism $\sigma$ on $\mathbb{F}$ naturally induces a bijection on the set of finite places, which we also denote by $\sigma$. Let $p$ be a finite place. If $p \in \Sigma$, say $p = p_i$, then we define $\sigma(p_i) = p_{i+1}$. If $p \notin \Sigma$, then $p$ is the vanishing place of some irreducible polynomial $Q \in \mathbb{G}[t]$, and we define $\sigma(p)$ to be the vanishing place of the irreducible polynomial $\sigma(Q)$. With this definition, we say that two finite places $p, q$ are shift equivalent if $p = \sigma^k(q)$ for some $k \in \mathbb{Z}$.

We can now determine exponent vectors $(e_1, \ldots, e_m)$ for which appropriate cancellations among the singularities happen. This is the main step in reducing the OHG problem in $\mathbb{F}$ to OHG problems in $\mathbb{G}$.

LEMMA 6. *Let $f_1, \ldots, f_m \in \mathbb{F}^*$. Denote by $p_1^{\text{fin}}, p_2^{\text{fin}}, \ldots$ finite places, pairwise not shift equivalent, such that all finite singular places of the $f_i$ can be written as $\sigma^k(p_j^{\text{fin}})$ for appropriate $k$ and $j$. Write $p_1^\infty, p_2^\infty, \ldots$ for the singular places of the $f_i$ over infinity.*

*Let*

$$M := \{\, (e_1, \ldots, e_m) \in \mathbb{Z}^m \mid \exists g \in \mathbb{F}^* : f_1^{e_1} \cdots f_m^{e_m} \frac{g}{\sigma(g)} \in \mathbb{G} \,\}$$

*and define*

$$M_{\text{fin}} := \{\, (e_1, \ldots, e_m) \in \mathbb{Z}^m \mid \forall i : \sum_{j,k} e_j \nu_{\sigma^k(p_i^{\text{fin}})}(f_j) = 0 \,\},$$

$$M_\infty := \{\, (e_1, \ldots, e_m) \in \mathbb{Z}^m \mid \forall i : \sum_{j} e_j \nu_{p_i^\infty}(f_j) = 0 \,\}.$$

*Then $M = M_{\text{fin}} \cap M_\infty$.*

PROOF. "$\subseteq$" Let $e = (e_1, \ldots, e_m) \in M$. Then there are $g \in \mathbb{F}^*$ and $c \in \mathbb{G}^*$ with $f_1^{e_1} \cdots f_m^{e_m} = c\sigma(g)/g$.

Consider an arbitrary place $p_i^{\text{fin}}$. Then for each $k \in \mathbb{Z}$,

$$\begin{aligned} &e_1 \nu_{\sigma^k(p_i^{\text{fin}})}(f_1) + \cdots + e_m \nu_{\sigma^k(p_i^{\text{fin}})}(f_m) \\ &= \nu_{\sigma^k(p_i^{\text{fin}})}(f_1^{e_1} \cdots f_m^{e_m}) = \nu_{\sigma^k(p_i^{\text{fin}})}(c\sigma(g)/g) \\ &= \nu_{\sigma^k(p_i^{\text{fin}})}(c) + \nu_{\sigma^k(p_i^{\text{fin}})}(\sigma(g)) - \nu_{\sigma^k(p_i^{\text{fin}})}(g) \\ &= 0 + \nu_{\sigma^{k-1}(p_i^{\text{fin}})}(g) - \nu_{\sigma^k(p_i^{\text{fin}})}(g). \end{aligned}$$

As $\nu_{\sigma^k(p_i^{\text{fin}})}(g) \neq 0$ only for finitely many $k$, summing over all $k$ gives $\sum_{j,k} e_j \nu_{\sigma^k(p_i^{\text{fin}})}(f_j) = 0$. Since $i$ was arbitrary, it follows that $e \in M_{\text{fin}}$.

Consider an arbitrary place $p_i^\infty$. Then

$$\begin{aligned} &e_1 \nu_{p_i^\infty}(f_1) + \cdots + e_m \nu_{p_i^\infty}(f_m) = \nu_{p_i^\infty}(f_1^{e_1} \cdots f_m^{e_m}) \\ &= \nu_{p_i^\infty}(c\sigma(g)/g) = \nu_{p_i^\infty}(c) + \nu_{p_i^\infty}(\sigma(g)) - \nu_{p_i^\infty}(g) = 0, \end{aligned}$$

because $\nu_p(\sigma(g)) = \nu_p(g)$ for every $g \in \mathbb{F}^*$ when $p$ is a place over infinity. Since $i$ was arbitrary, it follows that $e \in M_\infty$.

"$\supseteq$" Now let $e \in M_{\text{fin}} \cap M_\infty$.

Consider an arbitrary place $p_i^{\text{fin}}$. Let $l, r \in \mathbb{Z}$ be the minimum and maximum index such that $\sigma^l(p_i^{\text{fin}})$ and $\sigma^r(p_i^{\text{fin}})$ are singular for at least one of the $f_i$. Since $e \in M_{\text{fin}}$, we have

$$\sum_k \sum_j e_j \nu_{\sigma^k(p_i^{\text{fin}})}(f_j) = 0.$$

Therefore there exists an element $g_i \in \mathbb{F}^*$ with

$$\nu_{\sigma^k(p_i^{\text{fin}})}(\sigma(g_i)/g_i) = \sum_j e_j \nu_{\sigma^k(p_i^{\text{fin}})}(f_j)$$

and $\nu_p(\sigma(g)/g) = 0$ for all other places. (For $p_i^{\text{fin}} \in \Sigma$ the existence follows from Lemma 5, for $p_i^{\text{fin}} \notin \Sigma$ the existence follows like in Karr's original theorem.)

Hence for $g := \prod_i g_i$ we have

$$\nu_p(f_1^{e_1} \cdots f_m^{e_m}) = \nu_p(\sigma(g)/g)$$

for all finite places $p$. Furthermore, since also $e \in M_\infty$ and $\nu_p(\sigma(g)/g) = 0$ for all places $p$ over infinity, we have

$$\nu_p(f_1^{e_1} \cdots f_m^{e_m}) = \nu_p(\sigma(g)/g)$$

for all places. Therefore $f_1^{e_1} \cdots f_m^{e_m}$ and $\sigma(g)/g$ agree up to a multiplicative factor from the ground field, and therefore $f_1^{e_1} \cdots f_m^{e_m} g/\sigma(g) \in \mathbb{G}$, so $(e_1, \ldots, e_m) \in M$. □

The above lemma is constructive in the sense that not only can we compute a module basis for $M \subseteq \mathbb{Z}^m$, but also we can explicitly compute for every $(e_1, \ldots, e_m) \in M$ a witness $g \in \mathbb{F}$ with $f_1^{e_1} \cdots f_m^{e_m} \sigma(g)/g \in \mathbb{G}$, by just constructing the element $g$ as described in the proof.

We are now able to prove the following structure theorems, which, together with the above lemma, correspond to Theorem 8 in [6]. These theorems complete the reduction to OHG problems in the ground field $\mathbb{G}$.

THEOREM 5. *Suppose that $\mathbb{G}(t)$ is a $\Sigma$-extension of $\mathbb{G}$. Let $f_1, \ldots, f_m \in \mathbb{F}^*$, and let $M \subseteq \mathbb{Z}^m$ be as in Lemma 6. Let $B = ((e_{j,i})) \in \mathbb{Z}^{\bar{m} \times m}$ be such that the rows of $B$ form a basis of $M$, and let $g_j \in \mathbb{G}$ $(j = 1, \ldots, \bar{m})$ be such that*

$$\bar{f}_j := f_1^{e_{j,1}} \cdots f_m^{e_{j,m}} g_j/\sigma(g_j) \in \mathbb{G}.$$

*Let $\bar{M} := M(\bar{f}_1, \ldots, \bar{f}_{\bar{m}}; \mathbb{G})$ and let $\bar{B} = ((\bar{e}_{k,j})) \in \mathbb{Z}^{\bar{m} \times \bar{m}}$ be such that the rows of $\bar{B}$ form a basis of $\bar{M}$. Then the rows of $\bar{B} \cdot B$ form a basis of $M(f_1, \ldots, f_m; \mathbb{F})$.*

PROOF. "$\subseteq$" We show that every row in $\bar{B} \cdot B$ belongs to $M(f_1, \ldots, f_m; \mathbb{F})$. If $(e_1, \ldots, e_m)$ is the $k$th row, then

$$e_i = \sum_{j=1}^{\bar{m}} \bar{e}_{k,j} e_{j,i} \quad (i = 1, \ldots, m).$$

We have

$$\prod_i f_i^{e_i} = \prod_i (f_i)^{\sum_j \bar{e}_{k,j} e_{j,i}} = \prod_j \Big( \prod_i f_i^{e_{j,i}} \Big)^{\bar{e}_{k,j}}$$
$$= \prod_j \Big( \frac{\bar{f}_j}{g_j/\sigma(g_j)} \Big)^{\bar{e}_{k,j}} = \prod_j \bar{f}_j^{\bar{e}_{k,j}} \prod_j \Big( \frac{\sigma(g_j)}{g_j} \Big)^{\bar{e}_{k,j}}.$$

Since $(\bar{e}_{k,1}, \ldots, \bar{e}_{k,\bar{m}}) \in M(\bar{f}_1, \ldots, \bar{f}_{\bar{m}}; \mathbb{G})$, there exists $\bar{g}_k \in \mathbb{G}$ such that $\prod_j \bar{f}_j^{\bar{e}_{k,j}} = \sigma(\bar{g}_k)/\bar{g}_k$, altogether

$$\prod_i f_i^{e_i} = \frac{\sigma(\bar{g}_k)}{\bar{g}_k} \prod_j \Big( \frac{\sigma(g_j)}{g_j} \Big)^{\bar{e}_{k,j}} = \frac{\sigma\big(\bar{g}_k \prod_j g_j^{\bar{e}_{k,j}}\big)}{\bar{g}_k \prod_j g_j^{\bar{e}_{k,j}}},$$

and therefore $(e_1, \ldots, e_m) \in M(f_1, \ldots, f_m; \mathbb{F})$.

"$\supseteq$" We show that every $(e_1, \ldots, e_m) \in M(f_1, \ldots, f_m; \mathbb{F})$ is a $\mathbb{Z}$-linear combination of the rows of $\bar{B} \cdot B$. Let $g \in \mathbb{F}^*$ be such that

$$f_1^{e_1} \cdots f_m^{e_m} = \sigma(g)/g.$$

Then clearly $\nu_p(f_1^{e_1} \cdots f_m^{e_m} g/\sigma(g)) = 0$ for all places $p$. Consequently, $(e_1, \ldots, e_m) \in \bar{M}$, say

$$(e_1, \ldots, e_m) = (\bar{e}_1, \ldots, \bar{e}_{\bar{m}}) \cdot B.$$

To complete the proof, it suffices to show that $(\bar{e}_1, \ldots, \bar{e}_{\bar{m}}) \in \bar{M}$. Indeed,

$$\sigma(g)/g = \prod_i f_i^{e_i} = \prod_j \Big( \frac{\bar{f}_j}{g_j/\sigma(g_j)} \Big)^{\bar{e}_j},$$

therefore

$$\prod_j \bar{f}_j^{\bar{e}_j} = \frac{\sigma(g/\prod_j g_j)}{g/\prod_j g_j}.$$

Since the left side belongs to $\mathbb{G}$, so does the right hand side. It follows that $(\bar{e}_1, \ldots, \bar{e}_{\bar{m}}) \in \bar{M}$, as desired.

As it is easy to see that the rows of of $\bar{B} \cdot B$ are linearly independent if the rows of $\bar{B}$ and $B$ are, the proof is complete. □

If $\mathbb{G}(t)$ is a $\Pi$-extension, we also have to take into account that $\sigma(t)/t \in \mathbb{G}$, while in a $\Sigma$-extension we have $\sigma(f)/f \in \mathbb{G}^*$ only if $f \in \mathbb{G}^*$; see [6, Thm. 4]. But since the proof is otherwise similar, we skip the details.

THEOREM 6. *Suppose that $\mathbb{G}(t)$ is a $\Pi$-extension of $\mathbb{G}$. Let $f_1, \ldots, f_m \in \mathbb{F}^*$, and let $M \subseteq \mathbb{Z}^m$ be as in Lemma 6 and $B \in \mathbb{Z}^{\bar{m} \times m}$ and $\bar{f}_j$ $(j = 1, \ldots, \bar{m})$ be as in Theorem 5. Let*

$$\bar{M} := \pi(M(\bar{f}_1, \ldots, f_{\bar{m}}, t/\sigma(t); \mathbb{G})),$$

*where $\pi \colon \mathbb{Z}^{\bar{m}+1} \to \mathbb{Z}^{\bar{m}}$ is the projection that drops the last component, and let $\bar{B} \in \mathbb{Z}^{\bar{m} \times \bar{m}}$ be such that the rows of $\bar{B}$ form a basis of $\bar{M}$. Then the rows of $\bar{B} \cdot B$ form a basis of $M(f_1, \ldots, f_m; \mathbb{F})$.*

Theorems 5 and 6 directly give rise to an algorithm for solving the OHG problem in $\mathbb{F}$. This algorithm differs from Karr's original algorithm for the transcendental case in that Karr's algorithm avoids the explicit computation of the elements $g$ on the right hand side. However, if our algorithm is applied in the transcendental case, it is often faster than Karr's, because we often have $\bar{m} < m$ so the problem size may decrease during recursion whereas in Karr's algorithm the problem size never decreases during recursion.

## 5. SOLVING PLDES

We turn to the problem of solving difference equations in radical extensions of difference fields. The result is summarzied in the following theorem.

THEOREM 7. *Let $(\mathbb{G}, \sigma)$ be a difference field with constant field $\mathbb{K}$ and let $\mathbb{F} = \mathbb{G}\{x\}/\langle\langle P \rangle\rangle$ be a simple algebraic extension of $\mathbb{G}$.*

1. *If the solution space of PLDEs for $(\mathbb{G}, \sigma)$ can be computed, then the solution space of PLDEs for $(\mathbb{F}, \sigma)$ can be computed.*
2. *If the solution space of PLDEs for $(\mathbb{G}, \sigma)$ can be recursively enumerated, then the solution space of PLDEs for $(\mathbb{F}, \sigma)$ can be recursively enumerated.*

The second item is included in order to cover also sophisticated summation problems which can be formulated only in difference fields $(\mathbb{G}, \sigma)$ for which no solution algorithm is known.

In the remainder of the section, we show Theorem 7 by describing an algorithm. Let $a_0, \ldots, a_r \in \mathbb{F}$ (not all zero) and $f_1, \ldots, f_m \in \mathbb{F}$ be given. We need to determine a basis for the vector space $\mathbb{V} \subseteq \mathbb{K}^m \times \mathbb{F}$ of all $(c_1, \ldots, c_m, g)$ satisfying (2).

If, actually, the coefficients $a_0, \ldots, a_r$ and $f_1, \ldots, f_m$ belong to the ground field $\mathbb{G}$, then we solve the equation in that

field, which we can do by assumption. Now suppose that at least one of the coefficients belongs to $\mathbb{F} \setminus \mathbb{G}$, i.e., some $x_i$ occur in the equation. If $l, r \in \mathbb{Z}$ denote the minimum and maximum index $i$ such that $x_i$ occurs in the equation then any solution $g$ can involve only $x_i$ with $i \in \{l, \ldots, r\}$, since any $x_i$ with $i$ outside that range would fail to cancel away with the coefficients. Since all $x_i$ are algebraic over the ground field, $\mathbb{G}[x_l, \ldots, x_r]/\langle\!\langle P \rangle\!\rangle_{l,r}$ is a finite dimensional vector space over $\mathbb{G}$, and since all solutions $g$ must belong to that field, we can find them all by an ansatz with undetermined coefficients.

Let $\tau_1, \ldots, \tau_l$ be a vector space basis of

$$\mathbb{G}[x_l, \ldots, x_r]/\langle\!\langle P \rangle\!\rangle_{l,r}$$

over $\mathbb{G}$. Plugging the ansatz $g = \sum_{i=1}^{l} g_i \tau_i$ into (2) and comparing coefficients with respect to the $\tau_i$ gives a coupled system of difference equations:

$$A_0 \begin{pmatrix} g_1 \\ \vdots \\ g_l \end{pmatrix} + \cdots + A_r \begin{pmatrix} \sigma^r(g_1) \\ \vdots \\ \sigma^r(g_l) \end{pmatrix} = c_1 F_1 + \cdots + c_m F_m.$$

Here, $A_i \in \mathbb{G}^{l \times l}$ and the $F_i \in \mathbb{G}^l$ are the coefficient vectors of the $f_i \in \mathbb{F}$ in the original equation. We can assume that $a_r = 1$ in the original equation (otherwise divide by $a_r$), and thus that $A_r$ is the identity matrix.

The system can be reduced to a first order system using the companion matrix, this gives

$$\begin{pmatrix} \sigma(g_1) \\ \vdots \\ \sigma(g_l) \\ \vdots \\ \sigma^r(g_1) \\ \vdots \\ \sigma^r(g_l) \end{pmatrix} + \begin{pmatrix} 0 & -I & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & -I \\ A_0 & A_1 & \cdots & \cdots & A_{r-1} \end{pmatrix} \begin{pmatrix} g_1 \\ \vdots \\ g_l \\ \vdots \\ \sigma^{r-1}(g_1) \\ \vdots \\ \sigma^{r-1}(g_l) \end{pmatrix}$$
$$= c_1 F_1 + \cdots + c_m F_m,$$

where it is understood that the column vectors $F_i$ on the right hand side are padded by $rl$ rows with 0 to above. After renaming the unknowns for convenience of notation, the system reads

$$\begin{pmatrix} \sigma(u_1) \\ \vdots \\ \sigma(u_k) \end{pmatrix} + A \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix} = c_1 F_1 + \cdots + c_m F_m \tag{7}$$

with $k = (r+1)l$ and $A \in \mathbb{G}^{k \times k}$.

In the next step, we apply an uncoupling algorithm to this system. Several algorithms are available for uncoupling systems of difference equations with arbitrary difference fields as ground fields [1, 16], in our implementation we use Gerhold's Mathematica implementation [4] of the Abramov/Zima algorithm. The uncoupling algorithm returns an equivalent system of the form

$$\begin{pmatrix} a_{1,0}u_1 + a_{1,1}\sigma(u_1) + \cdots + a_{1,r_1}\sigma^{r_1}(u_1) \\ \vdots \\ a_{k,0}u_k + a_{k,1}\sigma(u_k) + \cdots + a_{k,r_k}\sigma^{r_k}(u_k) \end{pmatrix}$$
$$= \begin{pmatrix} * & \cdots & * & 0 & \cdots & 0 \\ \vdots & & \vdots & * & \ddots & \vdots \\ \vdots & & \vdots & \vdots & \ddots & 0 \\ * & \cdots & * & * & \cdots & * \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_m \\ u_1 \\ \vdots \\ u_{k-1} \end{pmatrix} \tag{8}$$

The latter system consists of inhomogeneous linear difference equations for each of the $u_i$, whose right hand sides depend $\mathbb{G}$-linearly on $c_1, \ldots, c_m$ (which are still undetermined) and on $u_1, \ldots, u_{i-1}$. (Uncoupling algorithms do, for efficiency reasons, represent the system in a slightly more complicated form, but this shall not bother us here.) The uncoupled system can be solved iteratively: The first equation is a univariate PLDE for $u_1$ which can be solved by assumption on $\mathbb{G}$, giving $m'$ linearly independent solutions

$$(\bar{c}_1^{(j)}, \ldots, \bar{c}_m^{(j)}, \bar{u}_1^{(j)}) \in \mathbb{K}^m \times \mathbb{G} \qquad (j = 1, \ldots, m')$$

The general solution is thus

$$(\bar{c}_1, \ldots, \bar{c}_m, \bar{u}_1) := \sum_{j=1}^{m'} c'_j (\bar{c}_1^{(j)}, \ldots, \bar{c}_m^{(j)}, \bar{u}_1^{(j)}),$$

with $c'_j$ arbitrary. If we discard the first equation from the system and replace $c_i$ by $\bar{c}_i$ and $u_1$ by $\bar{u}_1$ in the remaining equations, we end up with a system that is again of the form (8), but with one equation less. (The role of the $c_i$ in (8) is now played by the undetermined coefficients $c'_j$.) Iterating the process eventually gives $d$ linearly independent solutions

$$(c_1^{(j)}, \ldots, c_m^{(j)}, \begin{pmatrix} u_1^{(j)} \\ \vdots \\ u_k^{(j)} \end{pmatrix}) \in \mathbb{K}^m \times \mathbb{G}^k \quad (j = 1, \ldots, d)$$

that generate the solution space of (8), and hence of (7), as $\mathbb{K}$ vector space. The solution of the original difference equation are now obtained as

$$(c_1^{(j)}, \ldots, c_m^{(j)}, \sum_{i=1}^{l} u_i^{(j)} \tau_i) \quad (j = 1, \ldots, d)$$

This completes the solution algorithm.

# 6. APPLICATIONS

Combining all the algorithmic steps from above, we can treat towers of difference field extensions

$$\mathbb{F}_0 \leq \mathbb{F}_1 \leq \cdots \leq \mathbb{F}_e \tag{9}$$

where $\mathbb{F}_0$ is $\sigma^*$-computable, $\mathbb{F}_1$ is a $\Pi\Sigma^*$-extension of $\mathbb{F}_0$ and for each $1 < i \leq e$, $\mathbb{F}_i$ is a $\Pi\Sigma^*$-extension of $\mathbb{F}_{i-1}$, or $\mathbb{F}_{i-1} = \mathbb{F}_{i-2}(t)$ is a $\Pi\Sigma^*$-extension of $\mathbb{F}_{i-1}$ and

$$\mathbb{F}_i = \mathbb{F}_{i-2}(t)\{x\}/\langle\!\langle x_0^d - h \rangle\!\rangle \tag{10}$$

is a radical extension of $\mathbb{F}_{i-1}$ where $h \in \mathbb{F}_{i-2}[t]$ is irreducible. Then by Theorems 1 and 4 we have shown that also $\mathbb{F}_e$ is $\sigma^*$-computable. Therefore, as described in Section 2, we can solve problems OHG, PLDE, and DOS in (9).

The following remarks are in place.

**Checking the correctness of** (9)**.** If one finds answers to Question 1, one might check algorithmically, if radical

extensions (10) in the tower (9) are constructed properly. In addition, using Karr's theory [6], see also [11, Thm. 1], the correctness of $\Pi\Sigma^*$-extensions can be checked by solving instances of problem OHG and PLDE in its sub-field.

**Simple algebraic extensions.** If one can solve problems PLDE and DOS without using our OHG-algorithm presented in Section 4, we can allow simple algebraic extensions in (9). This happens, e.g., if (9) is free of $\Pi$-extensions.

**Heuristic simplifier.** If one thinks pessimistic, e.g., if one does not believe that $\langle\!\langle x_0^2 - n \rangle\!\rangle$ is maximal, see Example 1, or if one even knows that a given ideal $\langle\!\langle p \rangle\!\rangle$ with $p = x_0^d - h$ is not maximal, one can use our algorithms as a heuristic simplifier.

First, one can check algorithmically if (6) is maximal in $\mathbb{G}[x_l, \dots, x_r]$ for some interval $l < r$; see Remark 1. After this check we can carry out all the operations in the field $\mathbb{F}_{l,r} := \mathbb{G}[x_l, \dots, x_r]/\langle\!\langle p \rangle\!\rangle_{l,r}$. In particular, we can run all our algorithms. E.g., for $f \in \mathbb{F}_{l,r}$ we can decide, if there is $g \in \mathbb{F}_{l,r-1}$ with (1). Similarly, one can look for solutions of problems PLDE or OHG.

Our algorithms can be executed if several algebraic ring extensions occur in the tower (9). Clearly, the more such extensions pop up, the more could go wrong: e.g., the attempt to invert elements which cannot be inverted or adjoining sums and products over a ring; notice that such extensions cannot be handled properly with $\Pi\Sigma^*$-extensions.

Summarizing, we can run our algorithms in a heuristic fashion. Here we might fail within the computations or we could obtain results which are not optimal: this means that we model the algebraic expressions not sufficiently well. Interesting enough, in all our test runs, including the examples in Section 7, we never encountered such problems.

# 7. EXAMPLES

The following identities were found by our implementation. Once the right hand side of an identity is found, a proof an also easily be found independently of our algorithm.

$$\sum_{k=0}^{n} \frac{1}{\sqrt{k+1}+\sqrt{k}} = \sqrt{n+1},$$

$$\sum_{k=0}^{n} (k - \sqrt{k} + 1)\sqrt{k!} = (n+1)\sqrt{n!},$$

$$\sum_{k=0}^{n} ((k - \sqrt{k} + 1)H_k + 1)\sqrt{k!} = (1 + (n+1)H_n)\sqrt{n!},$$

$$\sum_{k=0}^{n} \frac{n - \sqrt{k}\sqrt{k+1} - k}{\sqrt{k+1}} \binom{n}{k} = 0,$$

$$\sum_{k=1}^{n} \big(2k + 2k^2 + k^3 - \sqrt{k^2+1}\big)(k-1)! \prod_{i=1}^{k} \sqrt{i^2+1} = (2 + 2n + n^2)n! \prod_{k=1}^{n} \sqrt{k^2+1} - 2,$$

$$\sum_{k=2}^{n} H_k \Big(\frac{(\sqrt{k})^3}{k-1} + \sum_{i=1}^{k} \frac{\sqrt{i}}{i+\sqrt{i}}\Big) = \frac{1}{2}\big(-3 - 5n + (5n+3)H_n - (2n+1)H_n^2 + H_n^{(2)}\big) + \sum_{k=1}^{n} \sqrt{k} + \Big((n+1)H_n - (n-1)\Big) \sum_{k=2}^{n} \frac{\sqrt{k}}{k-1},$$

$$\sum_{k=0}^{n} \Big(\sum_{i=0}^{k} \sqrt{i}\Big)^2 \sqrt{k} = \frac{1}{6}\sum_{k=0}^{n} k\sqrt{k} - \frac{1}{2}\sum_{k=0}^{n} k^2\sqrt{k} + \frac{1}{2}n(n+1)\sum_{k=0}^{n} \sqrt{k} + \frac{1}{3}\Big(\sum_{k=0}^{n} \sqrt{k}\Big)^3.$$

We abbreviate $H_k^{(a)} := \sum_{i=1}^{k} 1/i^a$ for the $k$th Harmonic number of $a$-th order ($a \in \mathbb{N}$ fixed), and $H_k := H_k^{(1)}$.

# 8. REFERENCES


[1] S. Abramov and E. Zima. A universal program to uncouple linear systems. In *Proceedings of CMCP'97*, 1997.

[2] M. Bronstein. On the integration of elementary functions. *J. Symbol. Comput.*, 9:117–173, 1990.

[3] M. Deuring. *Lectures on the theory of algebraic functions of one variable*. Springer, 1973.

[4] S. Gerhold. Uncoupling systems of linear Ore operator equations. Master's thesis, RISC-Linz, 2002.

[5] S. Gerhold. On some non-holonomic sequences. *Electronic Journal of Combinatorics*, 11(1):1–8, 12 2004.

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

[7] M. Kauers and C. Schneider. Application of unspecified sequences in symbolic summation. In J. Dumas, editor, *Proc. ISSAC'06.*, pages 177–183. ACM Press, 2006.

[8] M. Kauers and C. Schneider. Indefinite summation with unspecified summands. *Discrete Math.*, 306(17):2021–2140, 2006.

[9] M. Petkovšek, H. S. Wilf, and D. Zeilberger. $A = B$. A. K. Peters, Wellesley, MA, 1996.

[10] R. Risch. The solution of problem of integration in finite terms. *Bulletin of the American Mathematical Society*, 79:605–608, 1970.

[11] C. Schneider. Finding telescopers with minimal depth for indefinite nested sum and product expressions. In M. Kauers, editor, *Proc. ISSAC'05*, pages 285–292. ACM, 2005.

[12] C. Schneider. A new Sigma approach to multi-summation. *Advances in Applied Math.*, 34(4):740–767, 2005.

[13] C. Schneider. Solving parameterized linear difference equations in terms of indefinite nested sums and products. *J. Differ. Equations Appl.*, 11(9):799–821, 2005.

[14] C. Schneider. Symbolic summation assists combinatorics. *Sém. Lothar. Combin.*, 56:1–36, 2007. Article B56b.

[15] B. Trager. Algebraic factoring and rational function integration. In R. Jenks, editor, *Proc. of the ACM Symposium on Symbolic and Algebraic Computation*, pages 219–226, 1976.

[16] B. Zürcher. Rationale Normalformen von pseudo-linearen Abbildungen. Master's thesis, ETH Zürich, 1994.