Shift Equivalence Testing of Polynomials and Symbolic Summation of Multivariate Rational Functions

Shaoshi Chen[1,2], Lixin Du[1,2,3] , Hanqian Fang[4]

[1]KLMM, Academy of Mathematics and Systems Science,
Chinese Academy of Sciences,
Beijing, 100190, [2]School of Mathematical Sciences,
University of Chinese Academy of Sciences,
Beijing 100049, China
[3]Institute for Algebra, Johannes Kepler University,
Linz, A4040, Austria
[4]School of Mathematical Sciences, Beihang University,
Beijing 100191, China
schen@amss.ac.cn, dulixin@amss.ac.cn, hqfang_math@163.com

April 4, 2022

Abstract

The Shift Equivalence Testing (SET) of polynomials is deciding whether two polynomials $p(x_1, \ldots, x_m)$ and $q(x_1, \ldots, x_m)$ satisfy the relation $p(x_1 + a_1, \ldots, x_m + a_m) = q(x_1, \ldots, x_m)$ for some $a_1, \ldots, a_m$ in the coefficient field. The SET problem is one of basic computational problems in computer algebra and algebraic complexity theory, which was reduced by Dvir, Oliverira and Shpilka in 2014 to the Polynomial Identity Testing (PIT) problem. This paper presents a general scheme for designing algorithms to solve the SET problem which includes Dvir-Oliverira-Shpilka's algorithm as a special case. With the algorithms for the SET problem over integers, we give complete solutions to two challenging problems in symbolic summation of multivariate rational functions, namely the rational summability problem and the existence problem of telescopers for multivariate rational functions. Our approach is based on the structure of isotropy groups of polynomials introduced by Sato in 1960s. Our results can be used to detect the applicability of the Wilf-Zeilberger method to multivariate rational functions.

Contents

1 Introduction

Polynomials are basic arithmetic structures in mathematics and computer sciences. Efficient algorithms have been developed for manipulating polynomials in computer algebra [28, 43, 62, 68] with extensive complexity studies in [15, 60, 61]. Let $\mathbb{F}$ be a computable field and $\mathbb{F}[\mathbf{x}]$ be the ring of polynomials in m variables $\mathbf{x} = x_1, \ldots, x_m$ over $\mathbb{F}$. One can ask several basic computational questions on polynomials: Given $p, q \in \mathbb{F}[\mathbf{x}]$ and $\mathbf{P}, \mathbf{Q} \in \mathbb{F}[\mathbf{x}]^n$,

1. **Polynomial Identity Testing (PIT)**: Is $p(\mathbf{x})$ identically zero?
2. **Fast Evaluation and Interpolation (FEI)**: How fast can we evaluate $p(\mathbf{x})$ at many points and interpolate it from values at many points?
3. **Fast Multiplication and Factorization (FMF):** How fast can we multiply $p(\mathbf{x})$ by $q(\mathbf{x})$ and factor $p(\mathbf{x})$ into a product of irreducible polynomials over $\mathbb{F}$?
4. **Polynomial Equivalence Testing (PET)**: Decide whether there exists some invertible matrix $A \in GL_m(\mathbb{F})$ such that $p(\mathbf{x}) = q(A \cdot \mathbf{x})$.
5. **Shift Equivalence Testing (SET)**: Decide whether there exists some vector $\mathbf{b} \in \mathbb{F}^m$ such that $q(\mathbf{x}) = p(\mathbf{x} + \mathbf{b})$.
6. **Isomorphism of Polynomials (IP)**: Decide whether there exists a pair $(A, B) \in GL_m(\mathbb{F}) \times GL_n(\mathbb{F})$ such that $\mathbf{Q} = B \cdot \mathbf{P}(A \cdot \mathbf{x})$.
7. **Affine Projection of Polynomials (APP)**: Decide whether there exists a polynomial r in $n < m$ variables such that $p(\mathbf{x}) = r(A \cdot \mathbf{x} + \mathbf{b})$ for some $n \times m$ matrix A over $\mathbb{F}$ and some vector $\mathbf{b} \in \mathbb{F}^n$.

The answers to these questions may depend on the way in which how we model polynomials. A randomized polynomial-time algorithm for PIT was given independently by Schwartz [58] and Zippel [67], whose derandomization is still a long-standing open problem in algebraic complexity theory with impressive progress in the last three decades (see surveys [52,53,59]). When polynomials are modelled as arithmetic circuits, partial derivatives of polynomials are used extensively and essentially in most of the above questions (see the comprehensive survey [24]). Kayal presented a deterministic algorithm for the first question in the case where the input circuit is a sum of powers of sums of univariate polynomials and a randomized polynomial-time algorithm for some special cases of the fourth question in [41]. Fast algorithms for the second and third questions are fundamental for solving many computational problems in computer algebra [62, 68]. The fifth question was originally motivated by sparse interpolation of polynomials [30,31,44,45] and answered in several works [25,26,32,33,40] with different methods. The sixth question was first introduced by Patarin [47] and has rich applications in multivariate cryptography [12, 14, 27, 34]. In 2012, Kayal proved that the seventh question is NP-hard in general but admits randomized polynomial-time algorithms for special classes of polynomials including permanent and determinant polynomials [24, 42]. Beside the above-mentioned results, research and extensive work on these questions have been done by combing tools from symbolic computation and algebraic complexity theory. The above seven dwarfs build an exchanging bridge between mathematics and computer science.

This paper will focus on the SET problem which boils down to solving linear systems over $\mathbb{F}$. We present a general scheme for designing algorithms to solve the SET problem which includes Dvir-Oliverira-Shpilka's algorithm in [25, 26] as a special case. To enrich the applications of the SET problem in symbolic computation, we present a group-theoretical method that reduces the following two challenging problems in symbolic summation of multivariate rational functions to the SET problem: Let $\mathbb{F}(\mathbf{x})$ be the field of rational functions in variables $\mathbf{x}$ over $\mathbb{F}$ and let σ_{x_i} be the shift operator with respect to x_i defined by

$$\sigma_{x_i}(f(x_1, \ldots, x_m)) = f(x_1, \ldots, x_{i-1}, x_i + 1, x_{i+1}, \ldots, x_m)$$

for all $f \in \mathbb{F}(\mathbf{x})$. Let $\mathbb{K}$ be a subfield of $\mathbb{F}$. If $\mathbb{F} = \mathbb{K}(t)$ for some transcendental $t \in \mathbb{F}$ over $\mathbb{K}$, we let σ_t be the shift operator with respect to t defined similarly as above.

1. **Rational Summability Problem**: Given a rational function $f(\mathbf{x}) \in \mathbb{F}(\mathbf{x})$, decide whether there exist rational functions $g_1(\mathbf{x}), \ldots, g_m(\mathbf{x}) \in \mathbb{F}(\mathbf{x})$ such that

$$f = \sigma_{x_1}(g_1) - g_1 + \cdots + \sigma_{x_m}(g_m) - g_m.$$

   If such g_i's exist, we say that f is $(\sigma_{x_1}, \ldots, \sigma_{x_m})$-*summable* in $\mathbb{F}(\mathbf{x})$.

2. **Existence Problem of Telescopers**: Given a rational function $f(t, \mathbf{x}) \in \mathbb{F}(\mathbf{x})$ with $\mathbb{F} = \mathbb{K}(t)$, decide whether there exists a nonzero linear recurrence operator $L = \sum_{i=0}^{r} \ell_i \sigma_t^i$ with $\ell_i \in \mathbb{F}$ such that

$$L(f) = \sigma_{x_1}(g_1) - g_1 + \cdots + \sigma_{x_m}(g_m) - g_m \quad \text{for some } g_1, \ldots, g_m \in \mathbb{F}(\mathbf{x}).$$

   If such an operator L exists, we call it a *telescoper* for f of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_m})$.

1.1 Related work on symbolic summation

Symbolic summation is a classical and active research topic in symbolic computation, whose central problem is evaluating and simplifying different types of sums arising from combinatorics and theoretical physics [13,55] and other areas. For a given sequence in a certain specific class, the indefinite summation problem (in the univariate case) is to determine whether the given sequence is the difference of another sequence in the same class, which is a discrete analogue of indefinite integration problem. For instance, $-1/(n^2 + n)$ is the difference of $1/n$, but $1/n$ is not the difference of any rational sequence. The definite summation problem is to find a closed form for the sum $\sum_{i=a}^{b-1} f(i)$ assuming that the function $f(x)$ is well-defined in the interval $[a, b]$. The two summation problems are connected by the discrete Leibniz–Newton formula. Since the early 1970s, efficient algorithms have been developed for symbolic summation [62, Chapter 23]. Abramov's algorithm [1–3] solves the indefinite summation problem for univariate rational functions. A Hermite-like reduction algorithm for rational summation was developed by Paule via greatest factorial factorizations in [10,46,48,50]. The indefinite summation problem for hypergeometric terms is handled by Gosper's algorithm [29]. For sequences in a general difference field, the corresponding problem is studied by Karr in [38,39] with significant improvements by Schneider [54] and recent fruitful applications in Quantum Field Theory [13,57]. Most of existing complete algorithms are mainly applicable to the summation problem with univariate inputs. A long-term project in symbolic computation is to developing theories, algorithms and softwares for symbolic summation of multivariate functions. In the multivariate case, the stimulating problem was first raised by Andrews and Paule in [9]:

"Is it possible to provide any algorithmic device for reducing multiple sums to single sums? "

For a multiple sums, one would try to detect whether the summand is summable or not. If it is, the multiple sums can be reduced to several simpler sums. So it is crucial to first solve the summability problem in order to address the problem of Andrews and Paule. This first step beyond the univariate case was started in the work [23] by Chen, Hou and Mu in 2006 and then a complete algorithm for testing the summability of bivariate rational functions was given in [21] with a practical improvement in [36]. We will solve in this paper the summability problem for general multivariate rational functions.

Creative telescoping is the core of the Wilf–Zeilberger theory of computer-generated proofs of combinatorial identities [49,63,64]. For a multivariate function, the main task of creative telescoping is to construct a nonzero linear recurrence operator in one variable, which is called a telescoper for the given function. Two fundamental problems have been studied extensively related to creative telescoping. The first problem is the *existence problem of telescopers*, i.e., deciding the existence of telescopers for a given class of functions. The second one is the *construction problem of telescopers*, i.e., designing efficient algorithms for computing telescopers if they exist.

The existence problem of telescopers is equivalent to the termination of Zeilberger's algorithm [65, 66] and can be used to detect the hypertranscendence and algebraic dependency of functions defined by indefinite sums or integrals [35,56]. A sufficient condition, namely holonomicity, on the existence of telescopers was first given by Zeilberger in 1990 using Bernstein's theory of holonomic D-modules [11]. Wilf and Zeilberger in [64] proved that telescopers exist for proper hypergeometric terms. However, holonomicity and properness are only sufficient conditions. Abramov and Le [6] solved the existence problem of telescopers for rational functions in two discrete variables. This work was soon extended to the hypergeometric case by Abramov [5], the q-hypergeometric case in [22], and the mixed rational and hypergeometric case in [16,20]. All of the above work only focused on the problem for bivariate functions of a special class. The criteria on the existence of telescopers beyond the bivariate case were given in [17–19]. We will solve in this paper the existence problem of telescopers for general rational functions in several discrete variables.

1.2 The main results

From now on, we assume that $\mathbb{F}$ is a computational field of characteristic zero. We now present our main results on the SET problem, rational summability problem, and existence problem of telescopers for rational functions in several variables.

1.2.1 Algorithms for the SET problem

Given two polynomials $p, q \in \mathbb{F}[\mathbf{x}]$, we say that p is *shift equivalent* to q over $\mathbb{F}$ if there exist $a_1, \ldots, a_m \in \mathbb{F}$ such that

$$p(x_1 + a_1, \ldots, x_m + a_m) = q(x_1, \ldots, x_m).$$

We call the set $\{\mathbf{a} \in \mathbb{F}^m \mid p(\mathbf{x} + \mathbf{a}) = q(\mathbf{x})\}$ the *dispersion set* of p and q over $\mathbb{F}$, denoted by $F_{p,q}$. The Shift Equivalence Testing (SET) problem is to decide whether the dispersion set $F_{p,q}$ is empty or not. Write $p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x}) = \sum_{\boldsymbol{\alpha}\in\boldsymbol{\Lambda}} c_{\boldsymbol{\alpha}}(\mathbf{a})\mathbf{x}^{\boldsymbol{\alpha}}$ with $\boldsymbol{\Lambda}$ being a finite subset of $\mathbb{N}^m$. In general, the coefficients $c_{\boldsymbol{\alpha}}(\mathbf{a})\mathbf{x}^{\boldsymbol{\alpha}}$ are polynomials in $\mathbf{a}$ that may not be linear. So it seems that we need to solve a polynomial system in order to determine the set $F_{p,q}$. However, Grigoriev in [32,33] proved that $F_{p,q}$ is actually a linear variety and he also gave a recursive algorithm for determining this variety using the following relation

$$F_{p,q} = \left(\bigcap_{i=1}^{m} F_{\partial_{x_i}(p), \partial_{x_i}(q)} \right) \cap \{\mathbf{a} \in \mathbb{F}^m \mid p(\mathbf{a}) = q(\mathbf{0})\},$$

where ∂_{x_i} denotes the partial derivation with respect to x_i. Since partial derivations decrease the degree of polynomials, the SET problem boils down to solving a linear system. Another way to derive the linear system that defines $F_{p,q}$ was given by Kauers and Schneider (**KS**) in [40] with applications in solving linear partial difference equations. The idea is to compute the radical of the ideal I generated by the set $\{c_{\boldsymbol{\alpha}}(\mathbf{a})\}_{\boldsymbol{\alpha}\in\boldsymbol{\Lambda}}$ in $\mathbb{F}[\mathbf{a}]$ via Gröbner basis method. A more efficient algorithm was given by Dvir, Oliveira and Shpilka (**DOS**) in [25]. They reduced the SET problem to the PIT problem, then solved the latter one by randomized algorithms. Inspired by the **DOS** algorithm, we now present a general scheme for designing algorithms to solve the SET problem.

Let $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \cdots, \alpha_m)$ and $\boldsymbol{\beta} = (\beta_1, \beta_2, \cdots, \beta_m)$ be two vectors in $\mathbb{N}^m$. We say $\boldsymbol{\alpha} > \boldsymbol{\beta}$ if $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$ and $\alpha_i \geq \beta_i$ for all $1 \leq i \leq m$ and we denote the sum $\sum_{i=1}^m \alpha_i$ by $|\boldsymbol{\alpha}|$. Let $\mathrm{Supp}_{\mathbf{x}}(p)$ denote the support of p consisting of monomials $\mathbf{x}^{\boldsymbol{\alpha}}$ whose corresponding coefficients in p are nonzero.

Definition 1.1 (Admissible partition)**.** *Let $S_{p,q} = \{c_{\boldsymbol{\alpha}}(\mathbf{a}) \mid \mathbf{x}^{\boldsymbol{\alpha}} \in \mathrm{Supp}_{\mathbf{x}}(p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x}))\} \subseteq \mathbb{F}[\mathbf{a}]$. A set partition $S_{p,q} = S_0 \cup S_1 \cup \cdots \cup S_k$ is said to be* admissible *if the following two conditions hold:*

1. *All polynomials in S_0 are of degree in $\mathbf{a}$ at most one.*
2. *For all $\ell = 1, 2, \cdots, k$, if $c_{\boldsymbol{\alpha}}(\mathbf{a}) \in S_\ell$, then $c_{\boldsymbol{\beta}}(\mathbf{a}) \in \cup_{i=0}^{\ell-1} S_i$ for all $\boldsymbol{\beta} \in \mathbb{N}^m$ with $\boldsymbol{\beta} > \boldsymbol{\alpha}$ and $\mathbf{x}^{\boldsymbol{\beta}} \in \mathrm{Supp}_{\mathbf{x}}(p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x}))$.*

Without loss of generality, we may assume that the two given polynomials p and q in the SET problem are of the same degree d in $\mathbf{x}$. Let $H_{\mathbf{x}}^i(p(\mathbf{x}))$ denote the homogeneous component of $p(\mathbf{x})$ of total degree i in $\mathbf{x}$. Then $p(\mathbf{x}+\mathbf{a}) = q(\mathbf{x})$ if and only if $H_{\mathbf{x}}^i(p(\mathbf{x}+\mathbf{a})) = H_{\mathbf{x}}^i(q(\mathbf{x}))$ for all i with $0 \leq i \leq d$.

Definition 1.2 (Linearization)**.** *Let $p = p_0 + p_1 + \cdots + p_d$ be the homogeneous decomposition of $p \in \mathbb{F}[\mathbf{x}]$ in $\mathbf{x}$. For a vector $\mathbf{s} \in \mathbb{F}^m$, we call the linear polynomial $p_0(\mathbf{x}) + p_1(\mathbf{x}) + \sum_{i=2}^d p_i(\mathbf{s})$ the* linearization *of p at $\mathbf{s}$, denoted by $L_{\mathbf{x}=\mathbf{s}}(p)$. Note that $L_{\mathbf{x}=\mathbf{s}}(p) = p$ if $d \leq 1$.*

For a polynomial set $\mathbf{P} \subseteq \mathbb{F}[\mathbf{x}]$, we let $L_{\mathbf{x}=\mathbf{s}}(\mathbf{P}) = \{L_{\mathbf{x}=\mathbf{s}}(p) \mid p \in \mathbf{P}\}$ and $\mathbb{V}_{\mathbb{F}}(\mathbf{P}) = \{\mathbf{a} \in \mathbb{F}^m \mid p(\mathbf{a}) = 0 \text{ for all } p \in \mathbf{P}\}$. Our first main result says that any admissible partition of $S_{p,q}$ leads to an algorithm for solving the polynomial system $S_{p,q}$ which only requires solving several linear systems.

Theorem 1.3. *Let $S_{p,q} = \{c_{\boldsymbol{\alpha}}(\mathbf{a}) \mid \mathbf{x}^{\boldsymbol{\alpha}} \in Supp_{\mathbf{x}}(p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x}))\}$. If the partition $S_{p,q} = S_0 \cup S_1 \cup \cdots \cup S_k$ is admissible, then for all $\ell = 1, \cdots, k$, we have either $\mathbb{V}_{\mathbb{F}}\left(\bigcup_{i=0}^{\ell-1} S_i\right) = \varnothing$ or*

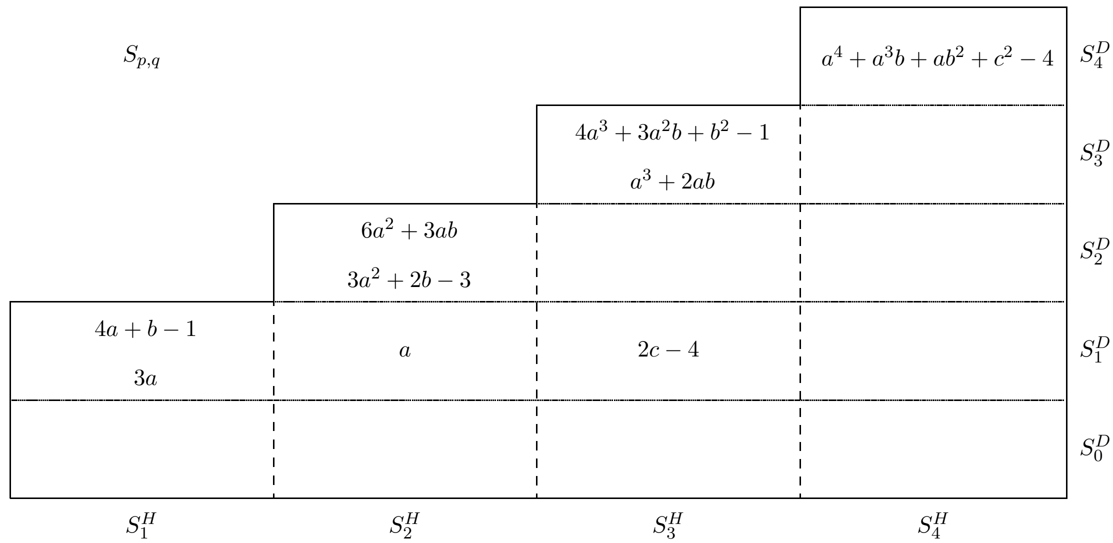
$$\mathbb{V}_{\mathbb{F}}\left(\bigcup_{i=0}^{\ell} S_i\right) = \mathbb{V}_{\mathbb{F}}\left(\bigcup_{i=0}^{\ell} L_{\mathbf{a}=\mathbf{s}}(S_i)\right) \quad \text{for any } \mathbf{s} \in \mathbb{V}_{\mathbb{F}}\left(\bigcup_{i=0}^{\ell-1} S_i\right).$$

In particular, the partitions $S_0^D \cup S_1^D \cup \cdots \cup S_d^D$ and $S_0^H \cup S_1^H \cup \cdots \cup S_d^H$ are admissible, where

$$S_i^D := \{c_{\boldsymbol{\alpha}}(\mathbf{a}) \in S \mid \deg_{\mathbf{a}}(c_{\boldsymbol{\alpha}}(\mathbf{a})) = i\} \quad \text{and} \quad S_i^H := \{c_{\boldsymbol{\alpha}}(\mathbf{a}) \in S_{p,q} \mid |\boldsymbol{\alpha}| = d - i\}.$$

We call the above two typical admissible partitions $\mathbf{a}$-*degree partition* and $\mathbf{x}$-*homogeneous partition* of $S_{p,q}$ respectively. The latter one corresponds to the **DOS** algorithm. We illustrate these two admissible partitions via a concrete example.

Example 1.4. *Let $p = x^4 + x^3y + xy^2 + z^2$ and $q = p(x, y+1, z+2) + xy$. By collecting the coefficients of $p(x+a, y+b, z+c) - q(x, y, z)$ with respect to the variables x, y, z, we get the set $S_{p,q}$. Then the $\mathbf{a}$-degree partition and $\mathbf{x}$-homogeneous partition of $S_{p,q}$ are*



1.2.2 Reduction for rational summability

The rational summability problem has been solved in the univariate and bivariate cases [1,2,21,36]. In order to address the problem in the general multivariate case, it suffices to provide a method that reduces the problem in n variables to that in fewer variables. The reduction method relies on the theory of isotropy groups of polynomials introduced by Sato in 1960s [51]. The computation of isotropy groups needs solving the SET problem over integers, for which we can use polynomial-time algorithms for computing the Hermite normal forms of an integer matrix [37].

Let $G = \langle \sigma_{x_1}, \ldots, \sigma_{x_m} \rangle$ be the free abelian multiplicative group generated by the shift operators $\sigma_{x_1}, \ldots, \sigma_{x_m}$ that acts on $\mathbb{F}(\mathbf{x})$. For any $\tau \in G$, define the difference operator $\Delta_\tau(g) = \tau(g) - g$ for any $g \in \mathbb{F}(\mathbf{x})$. Let $f \in \mathbb{F}[\mathbf{x}]$ and H be a subgroup of G. The set

$$[f]_H := \{\sigma(f) \mid \sigma \in H\}$$

is called the H-*orbit* at f. The *isotropy* group H_f of f in H is defined as

$$H_f := \{\sigma \in H \mid \sigma(f) = f\}.$$

Note that H_f is a free abelian group and the quotient group H/H_f is also free by [51, Lemma A-3]. The isotropy groups of polynomials will play an important role in the reduction for rational summability. A basis of the isotropy group of a polynomial can be computed by any algorithm for the SET problem over integers.

Similar to the bivariate case, we also use Abramov's reduction [2, 3] repeatedly to decompose $f \in \mathbb{F}(\mathbf{x})$ into the form

$$f = \Delta_{\sigma_{x_1}}(u_1) + \ldots + \Delta_{\sigma_{x_m}}(u_m) + r \quad \text{with } r = \sum_{i=1}^{I} \sum_{j=1}^{J_i} \frac{a_{i,j}}{d_i^j}, \tag{1.1}$$

where $u_1, \ldots, u_m \in \mathbb{F}(\mathbf{x})$, $a_{i,j} \in \mathbb{F}(\hat{\mathbf{x}}_1)[x_1]$ with $\hat{\mathbf{x}}_1 = \{x_2, \ldots, x_m\}$, $d_i \in \mathbb{F}[\mathbf{x}]$ with $\deg_{x_1}(a_{i,j}) < \deg_{x_1}(d_i)$ and the d_i's are monic irreducible polynomials in distinct $\langle \sigma_{x_1}, \ldots, \sigma_{x_m} \rangle$-orbits. The following lemma reduces the rational summability problem from general rational functions to simple fractions.

Lemma 1.5. *Let f be as in (1.1). Then f is summable in $\mathbb{F}(\mathbf{x})$ if and only if each $a_{i,j}/d_i^j$ is summable in $\mathbb{F}(\mathbf{x})$.*

We now only need to study the rational summability problem for rational functions of the form

$$f = \frac{a}{d^j}, \tag{1.2}$$

where $j \in \mathbb{N}\setminus\{0\}$, $a \in \mathbb{F}(\hat{\mathbf{x}}_1)[x_1]$ with $\hat{\mathbf{x}}_1 = \{x_2, \ldots, x_m\}$ and $d \in \mathbb{F}[\mathbf{x}]$ is irreducible with $\deg_{x_1}(a) < \deg_{x_1}(d)$. The following theorem further reduces the problem in m variables to another similar problem in r variables, where r is the rank of the isotropy group that is strictly less than m.

Theorem 1.6 (Summability criterion)**.** *Let $f = a/d^j \in \mathbb{F}(\mathbf{x})$ be of the form (1.2). Let $\{\tau_i\}_{i=1}^r (1 \leq r < n)$ be a basis of the free group G_d (take $\tau_1 = \mathbf{1}$, if $G_d = \{\mathbf{1}\}$). Then f is summable in $\mathbb{F}(\mathbf{x})$ if and only if*

$$a = \Delta_{\tau_1}(b_1) + \cdots + \Delta_{\tau_r}(b_r)$$

for some $b_i \in \mathbb{F}(\hat{\mathbf{x}}_1)[x_1]$ with $\hat{\mathbf{x}}_1 = \{x_2, \ldots, x_m\}$ and $\deg_{x_1}(b_i) < \deg_{x_1}(d)$ for all $1 \leq i \leq r$.

Note that the above reduced problem is related to the operators $\tau_1, \ldots, \tau_r$ in the isotropy group G_d. In order to turn back to the usual shifts, we can construct an $\mathbb{F}$-automorphism ϕ of $\mathbb{F}(\mathbf{x})$ such that a is $(\tau_1, \ldots, \tau_r)$-summable in $\mathbb{F}(\mathbf{x})$ if and only if each $\phi(a)$ is $(\sigma_{x_1}, \ldots, \sigma_{x_r})$-summable in $\mathbb{F}(\mathbf{x})$. So the rational summability problem in n variables can be completely reduced to the same problem in fewer variables. Combing the existing methods in the univariate case, we now obtain a complete solution to the rational summability problem for multivariate rational functions.

1.2.3 Reduction for existence of telescopers

The existence problem of telescoper can be viewed as a parameterization of the rational summabilty problem. The latter problem is equivalent to testing whether the identity operator is a telescoper or not. Similar to the strategy used in the rational summability problem, we now provide a method for reducing the existence problem of telescoper in $m+1$ variables to that in fewer variables.

For a rational function $f(t, \mathbf{x}) \in \mathbb{F}(\mathbf{x})$ with $\mathbb{F} = \mathbb{K}(t)$, the existence problem of telescopers for f can also be reduced to simple fractions of the form a/d^j as in (1.2). The second reduction of the number of variables also relies on the structure of isotropy groups. Let $G_t = \langle \sigma_t, \sigma_{x_1}, \ldots, \sigma_{x_m}\rangle$ be the group generated by $\sigma_t, \sigma_{x_1}, \ldots, \sigma_{x_m}$ and $G_{t,d}$ be the isotropy group of d in G_t. Then the quotient group $G_{t,d}/G_d$ is still a free abelian group with $\operatorname{rank}(G_{t,d}/G_d) \leq 1$. If $\operatorname{rank}(G_{t,d}/G_d) = 0$, then we can show that f has a telescoper of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_m})$ if and only if f is $(\sigma_{x_1}, \ldots, \sigma_{x_m})$-summable in $\mathbb{F}(\mathbf{x})$. So in this case, the existence problem of telescopers for f is equivalent to the rational summability problem. If $\operatorname{rank}(G_{t,d}/G_d) = 1$, we have the following existence criteria.

Theorem 1.7 (Existence criterion)**.** *Let $f = a/d^j \in \mathbb{K}(t, \mathbf{x})$ as above with $\operatorname{rank}(G_{t,d}/G_d) = 1$. Let $\{\tau_0, \tau_1, \ldots, \tau_r\} (1 \leq r < n)$ be a basis of $G_{t,d}$ such that $G_{t,d}/G_d = \langle \bar{\tau}_0\rangle$ and let $\{\tau_1, \ldots, \tau_r\}$ be a basis of G_d (take $\tau_1 = \mathbf{1}$, if $G_d = \{\mathbf{1}\}$). Then f has a telescoper of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_m})$ if and only if there exists a nonzero operator $L = \sum_{i=0}^{\rho} \ell_i \sigma_t^i$ with $\ell_i \in \mathbb{K}(t)$ such that*

$$L(a) = \Delta_{\tau_1}(b_1) + \cdots \Delta_{\tau_r}(b_r)$$

for some $b_i \in \mathbb{K}(t, \hat{\mathbf{x}}_1)[x_1]$ with $\hat{\mathbf{x}}_1 = \{x_2, \ldots, x_m\}$ and $\deg_{x_1}(b_i) < \deg_{x_1}(d)$ for $1 \leq i \leq r$.

Similar to the summability problem, after a suitable transformation of rational functions, the existence problem of telescopers in $n+1$ variables can also be reduced to that in fewer variables. Since the bivariate case has been solved in [6], we now have a complete solution to the existence problem of telescopers for rational functions in several discrete variables.

1.3 An example

We now show an example to illustrate the main steps of deciding the rational summability problem with the help of algorithms for the SET problem over integers.

Let f be a rational function in $\mathbb{Q}(x, y, z)$ of the form

$$f = \frac{-z^2 + x}{x^2 + 2xy + z^2} + \frac{x - y - 2z}{x^2 + 2xy + z^2 + 2x} + \frac{z^2 + y}{x^2 + 2xy + z^2 + 8x + 2y - 2z + 8} + \frac{x + z}{(x - 3y)^2(y + z) + 1} + \left(y + \frac{z}{y^2 + z - 1} - \frac{1}{y^2 + z}\right) \frac{1}{(x + 2y + z)^2}.$$

Let $G = \langle \sigma_x, \sigma_y, \sigma_z \rangle$ be the free abelian group generated by the shift operators $\sigma_x, \sigma_y, \sigma_z$. In order to decide whether f is $(\sigma_x, \sigma_y, \sigma_z)$-summable in $\mathbb{Q}(x, y, z)$, the first step is so-called *orbital decomposition*, where we first compute the irreducible partial fraction decomposition of f with respect to x and then classify all irreducible factors of the denominator of f according to the shift equivalence relation. Applying algorithms for the partial fraction decomposition and the SET problem over integers, we obtain the orbital decomposition $f = f_1 + f_2 + f_3$, where

$$f_1 = \frac{x - z^2}{d_1} + \frac{x - y - 2z}{\sigma_y(d_1)} + \frac{y + z^2}{\sigma_x \sigma_y^3 \sigma_z^{-1}(d_1)}, \quad f_2 = \frac{x + z}{d_2} \quad \text{and} \quad f_3 = \left(y + \frac{z}{y^2 + z - 1} - \frac{1}{y^2 + z}\right) \frac{1}{d_3^2}$$

with $d_1 = x^2 + 2xy + z^2$, $d_2 = (x - 3y)^2(y + z) + 1$ and $d_3 = x + 2y + z$. Here f_1, f_2, f_3 are three orbital components of f, since any two elements of d_1, d_2, d_3 are not shift equivalent. By Lemma 1.5, we have f is $(\sigma_x, \sigma_y, \sigma_z)$-summable in $\mathbb{Q}(x, y, z)$ if and only if each f_i is summable.

The second step is using Abramov's reduction to reduce the summability problem from a general rational function to simple fractions. Since f_2, f_3 are already simple fractions with denominator being the power of one irreducible polynomial, we only need to reduce f_1. For any $a, d \in \mathbb{F}(x, y, z)$ and any integer $k \in \mathbb{Z}$, Abramov's reduction decomposes $a/\sigma^k(b)$ as

$$\frac{a}{\sigma^k(b)} = \sigma(h) - h + \frac{\sigma^{-k}(a)}{b}, \tag{1.3}$$

where $h = 0$ if $k = 0$, $h = \sum_{i=0}^{k-1} \frac{\sigma^{i-k}(a)}{\sigma^i(b)}$ if $k > 0$ and $h = -\sum_{i=0}^{-k-1} \frac{\sigma^i(a)}{\sigma^{i+k}(b)}$ if $k < 0$. Applying the reduction formula to f_1 with $\sigma = \sigma_x, \sigma_y, \sigma_z$ successively yields

$$f_1 = \Delta_x(u_1) + \Delta_y(v_1) + \Delta_z(w_1) + r_1 \text{ with } r_1 = \frac{2x - 1}{d_1},$$

for some $u_1, v_1, w_1 \in \mathbb{Q}(x, y, z)$. Then f_1 is summable if and only if r_1 is $(\sigma_x, \sigma_y, \sigma_z)$-summable.

The third step is using the summability criterion to reduce the summability problem into few variables. For r_1, the isotropy group of d_1 in G is $G_{d_1} = \{\mathbf{1}\}$. By Theorem 1.6, r_1 is summable if and only if its numerator is zero. Hence r_1 is not $(\sigma_x, \sigma_y, \sigma_z)$-summable and neither are f_1 and f. For f_2, the isotropy group of d_2 in G is $G_{d_2} = \{\tau\}$ with $\tau = \sigma_x^3 \sigma_y \sigma_z^{-1}$. By Theorem 1.6, we see that f_2 is summable in $\mathbb{Q}(x, y, z)$ if and only if $a_2 = x + z$ is (τ)-summable in $\mathbb{Q}(x, y, z)$. Since $a_2 = x + z = \Delta_\tau(b)$ with $b = \frac{1}{9}(x - 3)(2x + 3z)$, so a_2 is (τ)-summable, which implies that f_2 is $(\sigma_x, \sigma_y, \sigma_z)$-summable. Since $f_2 = \Delta_\tau(\frac{b}{d_2})$, its certificates can be obtained by Abramov's reduction. For f_3, a basis of the isotropy group G_{d_3} is $\{\tau_1, \tau_2\}$, where $\tau_1 = \sigma_x^2 \sigma_y^{-1}$ and $\tau_2 = \sigma_x \sigma_z^{-1}$. Construct a $\mathbb{Q}$-automorphism ϕ_3 of $\mathbb{Q}(x, y, z)$ as follows

$$\phi_3(h(x, y, z)) = h(2x + y, -x, -y + z),$$

for any $h \in \mathbb{Q}(x, y, z)$. It can be checked that $\phi_3 \circ \tau_1 = \sigma_x \circ \phi_3$ and $\phi_3 \circ \tau_2 = \sigma_y \circ \phi_3$. So $a_3 = f_3 d_3$ is (τ_1, τ_2)-summable in $\mathbb{Q}(x, y, z)$ if and only if $\phi_3(a_3)$ is (σ_x, σ_y)-summable in $\mathbb{Q}(x, y, z)$. This reduces the summability problem in three variables to the summability problem in two variables. By induction, we get $\phi_3(a_3)$ is not (σ_x, σ_y)-summable. Therefore f_3 is not $(\sigma_x, \sigma_y, \sigma_z)$-summable. In this case, f_3 can be decomposed into the sum of a summable part and a non-summable one:

$$f_3 = \Delta_x(u_3) + \Delta_y(v_3) + \Delta_z(w_3) + \frac{z}{(y^2 + z)d_3^2}$$

for some $u_3, v_3, w_3 \in \mathbb{Q}(x, y, z)$.

1.4 Organization

The rest of this paper is organized as follows. In Section 2, we define the existence problem of telescopers and the summability problem precisely. In Section 3, we present a general scheme for designing algorithms to solve the shift equivalence testing problem and compare our new algorithms with the other known algorithms. In Section 4, we first recall the notion of isotropy groups of polynomials and their basic properties, and then introduce orbital decompositions for rational functions. We apply orbital decompositions in Section 5 to reduce the rational summability problem for general rational functions to that for simple fractions. After this, we present a criterion on the summability of such simple fractions. In Section 6, we again use the structure of isotropy groups and orbital decompositions to derive criteria for the existence of telescopers for rational functions in variables t and $\mathbf{x}$.

2 Preliminaries

Thought out the paper, let $\mathbb{K}$ be a field of characteristic zero and $\mathbb{K}(t, \mathbf{x})$ be the field of rational functions in t and $\mathbf{x} = \{x_1, \cdots, x_m\}$ over $\mathbb{K}$. For each $v \in \mathbf{v} = \{t, x_1, \ldots, x_m\}$, the shift operator σ_v with respect to v is defined as the $\mathbb{K}$-automorphism of $\mathbb{K}(\mathbf{v})$ such that

$$\sigma_v(v) = v + 1 \text{ and } \sigma_v(w) = w \text{ for all } w \in \mathbf{v} \setminus \{v\}.$$

Let $\mathcal{R} := \mathbb{K}(\mathbf{v})\langle S_t, S_{x_1}, \ldots, S_{x_m}\rangle$ denote the ring of linear recurrence operators over $\mathbb{K}(\mathbf{v})$, in which $S_{v_i} S_{v_j} = S_{v_j} S_{v_i}$ for all $v_i, v_j \in \mathbf{v}$ and $S_v \cdot f = \sigma_v(f) \cdot S_v$ for any $f \in \mathbb{K}(\mathbf{v})$ and $v \in \mathbf{v}$. The action of an operator $L = \sum_{i_0, i_1, \ldots, i_m \geq 0} a_{i_0, i_1, \ldots, i_m} S_t^{i_0} S_{x_1}^{i_1} \cdots S_{x_m}^{i_m} \in \mathcal{R}$ on a rational function $f \in \mathbb{K}(\mathbf{v})$ is defined as

$$L(f) = \sum_{i_0, i_1, \ldots, i_m \geq 0} a_{i_0, i_1, \ldots, i_m} \sigma_t^{i_0} \sigma_{x_1}^{i_1} \cdots \sigma_{x_m}^{i_m}(f).$$

For each $v \in \mathbf{v}$, the difference operator Δ_v with respect to v is defined by $\Delta_v = S_v - \mathbf{1}$, where $\mathbf{1}$ stands for the identity map on $\mathbb{K}(\mathbf{v})$.

We now introduce the notion of telescopers for rational functions in $\mathbb{K}(t, \mathbf{x})$.

Definition 2.1 (telescopers)**.** *Let n be a positive integer such that $1 \leq n \leq m$ and let $f \in \mathbb{K}(t, \mathbf{x})$ be a rational function. A nonzero linear recurrence operator $L \in \mathbb{K}(t)\langle S_t\rangle$ is called a* telescoper *of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_n})$ for f if there exist $g_1, \ldots, g_n \in \mathbb{K}(t, \mathbf{x})$ such that*

$$L(f) = \Delta_{x_1}(g_1) + \cdots + \Delta_{x_n}(g_n). \tag{2.1}$$

The rational functions $g_1, \ldots, g_n$ are called the certificates *of L.*

Problem 2.2 (Existence Problem of Telescopers)**.** *Given a rational function $f \in \mathbb{K}(t, \mathbf{x})$ and an integer n with $1 \leq n \leq m$, decide the existence of telescopers of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_n})$ for f.*

In order to detect the existence of telescopers for $f \in \mathbb{K}(t, \mathbf{x})$, we first need to decide whether $L = \mathbf{1}$ is a telescoper for f. This is equivalent to the following summability problem of f in $\mathbb{F}(\mathbf{x})$ with $\mathbb{F} = \mathbb{K}(t)$.

Definition 2.3 (Summability)**.** *Let $\mathbb{F}$ be a field of characteristic zero and n be a positive integer such that $1 \leq n \leq m$. A rational function $f \in \mathbb{F}(\mathbf{x})$ is called $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-*summable *in $\mathbb{F}(\mathbf{x})$ if there exist $g_1, \ldots, g_n \in \mathbb{F}(\mathbf{x})$ such that*

$$f = \Delta_{x_1}(g_1) + \cdots + \Delta_{x_n}(g_n). \tag{2.2}$$

Problem 2.4 (Rational Summability Problem)**.** *Given a rational function $f \in \mathbb{F}(\mathbf{x})$ and an integer n with $1 \leq n \leq m$, decide whether or not f is $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summable in $\mathbb{F}(\mathbf{x})$.*

The main idea of solving the summability problem is using mathematical induction to reduce the number of difference operators in this problem. To say explicitly, we shall reduce the $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summability problem for $f \in \mathbb{F}(\mathbf{x})$ to the $(\sigma_{x_1}, \ldots, \sigma_{x_r})$-summability problem for another rational function $a \in \mathbb{F}(\mathbf{x})$, where r is smaller than n and the base field $\mathbb{F}(\mathbf{x})$ in the summability problem is unchanged. Similarly, we shall reduce the existence problem of telescopers of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_n})$ for $f \in \mathbb{K}(t, \mathbf{x})$ to the existence problem of telescopers of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_r})$ for some rational function $a \in \mathbb{K}(t, \mathbf{x})$.

We introduce below a general definition of the summability problem and existence problem of telescopers, which plays a role of bridge in the method of mathematical induction for solving Problems 2.4 and 2.2. Let $G_t = \langle \sigma_t, \sigma_{x_1}, \ldots, \sigma_{x_n} \rangle$ be the group generated by the shift operators $\sigma_t, \sigma_{x_1}, \ldots, \sigma_{x_n}$ under the operation of composition of functions. Then G_t is a free abelian group. For any $\tau \in G_t$, the difference operator Δ_τ is defined by

$$\Delta_\tau = S_t^{i_0} S_{x_1}^{i_1} \cdots S_{x_n}^{i_n} - \mathbf{1} \quad \text{if } \tau = \sigma_t^{i_0} \sigma_{x_1}^{i_1} \cdots \sigma_{x_n}^{i_n}.$$

For short, we use Δ_v to denote Δ_{σ_v} for each $v \in \mathbf{v}$. A finite subset $\{\tau_1, \ldots, \tau_r\}$ of G_t is said to be *$\mathbb{Z}$-linearly independent* if for all $a_1, \ldots, a_r \in \mathbb{Z}$, we have

$$\tau_1^{a_1} \cdots \tau_r^{a_r} = \mathbf{1} \quad \Rightarrow \quad a_1 = a_2 = \cdots = a_r = 0.$$

Let $G = \langle \sigma_{x_1}, \ldots, \sigma_{x_n} \rangle$ be the subgroup of G_t generated by shift operators $\sigma_{x_1}, \ldots, \sigma_{x_n}$. Let $\{\tau_1, \ldots, \tau_r\} (1 \leq r \leq n)$ be a family of $\mathbb{Z}$-linearly independent elements in G. In general, a rational function $f \in \mathbb{F}(\mathbf{x})$ is called $(\tau_1, \ldots, \tau_r)$-*summable* in $\mathbb{F}(\mathbf{x})$ if

$$f = \Delta_{\tau_1}(g_1) + \cdots + \Delta_{\tau_r}(g_r) \tag{2.3}$$

for some $g_1, \ldots, g_r \in \mathbb{F}(\mathbf{x})$. Choose an element $\tau_0 = \sigma_t^{k_0} \sigma_{x_1}^{k_1} \cdots \sigma_{x_n}^{k_n} \in G_t$ such that k_0 is nonzero. Then $\tau_0, \tau_1, \ldots, \tau_r$ are $\mathbb{Z}$-linearly independent in G_t. Let $T_0 = S_t^{k_0} S_{x_1}^{k_1} \cdots S_{x_n}^{k_n} \in \mathcal{R}$ be the operator corresponding to τ_0. We say a nonzero operator $L \in \mathbb{K}(t)\langle T_0 \rangle$ is a *telescoper of type* $(\tau_0; \tau_1, \ldots, \tau_r)$ for $f \in \mathbb{K}(t, \mathbf{x})$ if $L(f)$ is $(\tau_1, \ldots, \tau_r)$-summable in $\mathbb{K}(t, \mathbf{x})$.

Let R be a ring and $\sigma \colon R \to R$ be a ring homomorphism of R. The pair (R, σ) is called a *difference ring*. If R is a field, we call the pair (R, σ) a *difference field*. Let (R_1, σ_1) and (R_2, σ_2)

be two difference rings and $\phi\colon R_1 \to R_2$ be a ring homomorphism. If ϕ satisfies the property that $\phi \circ \sigma_1 = \sigma_2 \circ \phi$, that means the following diagram

$$\begin{array}{ccc} R_1 & \xrightarrow{\phi} & R_2 \\ {\scriptstyle \sigma_1}\downarrow & & \downarrow{\scriptstyle \sigma_2} \\ R_1 & \xrightarrow{\phi} & R_2 \end{array}$$

commutes, then ϕ is called a *difference homomorphism*. If in addition ϕ is a bijection, then its inverse ϕ^{-1} is also a difference homomorphism. In this case, we call ϕ a *difference isomorphism*. The notion of difference isomorphisms will be used to state our summability criteria and the existence criteria of telescopers.

An operator $L \in \mathbb{K}(t)\langle S_t\rangle$ is called a *common left multiple* of operators $L_1, \ldots, L_r \in \mathbb{K}(t)\langle S_t\rangle$ if there exist $R_1, \ldots, R_r \in \mathbb{K}(t)\langle S_t\rangle$ such that

$$L = R_1L_1 = \cdots = R_rL_r.$$

Since $\mathbb{K}(t)\langle S_t\rangle$ is a left Euclidean domain, such an operator L always exists. Among all of such multiples, the monic one of smallest degree in S_t is called the *least common left multiple* (LCLM). Efficient algorithms for computing LCLM have been developed in [7, 8].

Remark 2.5. *Let $f = f_1 + \cdots + f_r$ with $f_i \in \mathbb{K}(t, \mathbf{x})$. If each f_i has a telescoper L_i of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_n})$ for $i = 1, \ldots, r$, then the LCLM of L_i's is a telescopoer of the same type for f. This fact follows from the commutativity between operators in $\mathbb{K}(t)\langle S_t\rangle$ and the difference operators Δ_{x_i}'s.*

3 Shift equivalence testing of polynomials

In this section, we first state the Shift Equivalence Testing (SET) problem and define admissible partitions of the associated polynomial system with the SET problem. We then prove that any admissible partition leads to an algorithm to solve the SET problem via linear system solving. This gives a general scheme for constructing algorithms to solve the SET problem which includes Dvir-Oliverira-Shpilka's algorithm in [25, 26] by taking a special admissible partition. At the end of this section, we will compare the practical efficiency of different algorithms and show that our new algorithms outperform the others for most of the testing examples.

3.1 Admissible partitions for the SET problem

In order to be compatible with the next section, we take $m = n$ in this section. Let $\mathbb{F}[\mathbf{x}]$ be the ring of polynomials in $\mathbf{x} = \{x_1, \ldots, x_n\}$ over $\mathbb{F}$. Given two polynomials $p, q \in \mathbb{F}[\mathbf{x}]$, we say that they are *shift equivalent* if there exists $a_1, a_2, \ldots, a_n \in \mathbb{F}$ such that

$$p(x_1 + a_1, \ldots, x_n + a_n) = q(x_1, \ldots, x_n).$$

The set $\{\mathbf{a} \in \mathbb{F}^n \mid p(\mathbf{x} + \mathbf{a}) = q(\mathbf{x})\}$ is called the *dispersion set* of p and q over $\mathbb{F}$, denoted by $F_{p,q}$. Then the Shift Equivalence Testing (SET) problem can be stated as follow.

Problem 3.1 (Shift Equivalence Testing (SET))**.** *Given $p, q \in \mathbb{F}[x_1, \ldots, x_n]$, decide whether there exists $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}^n$ such that*

$$p(\mathbf{x} + \mathbf{a}) = q(\mathbf{x}).$$

If such $\mathbf{a}$ exists, compute the dispersion set of p and q over $\mathbb{F}$.

A related problem is to test shift equivalence over integers, i.e. decide whether there exists a vector $\mathbf{a} \in \mathbb{Z}^n$ such that $p(\mathbf{x}+\mathbf{a}) = q(\mathbf{x})$. We denote the set $\{\mathbf{a} \in \mathbb{Z}^n \mid p(\mathbf{x}+\mathbf{a}) = q(\mathbf{x})\}$ by $Z_{p,q}$. The computation of $Z_{p,q}$ will play an important role in next section where we study the rational summability problem and the existence problem of telescopers. Since the computation of $F_{p,q}$ boils down to solving linear systems, we can also compute $Z_{p,q}$ by combing the same methods for the SET problem over $\mathbb{F}$ and any algorithm for computing integer solutions of linear systems.

There are three different methods for solving the SET problem in the literature. In 1996, Grigoriev first gave a recursive algorithm (**G**) for the SET problem in [32, 33]. Motivated by solving linear partial difference equations, another algorithm (**KS**) for computing $Z_{p,q}$ via Gröbner basis method was given by Kauers and Schneider in [40]. In 2014, a new algorithm with better complexity was given by Dvir, Oliveira and Shpilka (**DOS**) in [25]. We have implemented all of the three algorithms in Maple and the experimental comparison will be tabulated at the end of this section. The timings indicate that the **DOS** algorithm is the most efficient one in practice.

We will put the DOS algorithm into a more general scheme. From the relation $p(\mathbf{x}+\mathbf{a}) = q(\mathbf{x})$ in the SET problem, we obtain a polynomial system $\{c_{\boldsymbol{\alpha}}(\mathbf{a}) = 0 \mid \boldsymbol{\alpha} \in \Lambda\}$ by collecting coefficients of the polynomial $p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x})$ in $\mathbf{x}$. So a direct approach to the SET problem is solving this polynomial systems. Without exploring the hidden structure of the polynomial system, this naive approach could be very in-efficient. The main idea of the **DOS** algorithm is partitioning the polynomial system $\{c_{\boldsymbol{\alpha}}(\mathbf{a}) = 0 \mid \boldsymbol{\alpha} \in \Lambda\}$ into several subsets in a appropriate way so that we can reduce the problem into solving several linear systems recursively. This idea inspires us to introduce the notion of admissible partitions for the polynomial systems from the SET problem. To this end, we first recall some basic properties of the dispersion sets from [25, 33, 40].

Lemma 3.2. *Let $p \in \mathbb{F}[x]$ and let F_p denote $F_{p,p}$. Then F_p is a vector subspace of $\mathbb{F}^n$ over $\mathbb{F}$.*

Proof. see [25, Observation 4.2]. ∎

Lemma 3.3. *Let $p, q \in \mathbb{F}[\mathbf{x}]$. If $F_{p,q} \neq \emptyset$, then $F_p = F_q$ and $F_{p,q} = \mathbf{a} + F_p$ for any $\mathbf{a} \in F_{p,q}$.*

Proof. It is easy to check and see details in [25, Lemma 4.4]. ∎

From the above lemmas, we know $F_{p,q}$ is a linear variety over $\mathbb{F}$. Then our task is to find the defining linear system of $F_{p,q}$ so that we can compute $F_{p,q}$ without solving the polynomial equations. We will give a general scheme for partitioning the polynomial system associated with the given SET problem so that we can solve them via solving several linear systems. We first introduce some notations for latter use. For any two vectors $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \cdots, \alpha_n), \boldsymbol{\beta} = (\beta_1, \beta_2, \cdots, \beta_n) \in \mathbb{N}^n$, we can define $\boldsymbol{\alpha} > \boldsymbol{\beta}$ if and only if $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$ and $\alpha_i \geq \beta_i$ for all $1 \leq i \leq n$. We use $|\boldsymbol{\alpha}|$ to denote the sum $\sum_{i=1}^n \alpha_i$. For a subset $\mathbf{y} = \{y_1, y_2, \cdots, y_m\}$ of $\mathbf{x} = \{x_1, x_2, \cdots, x_n\}$ with $\hat{\mathbf{y}} := \mathbf{x} \setminus \mathbf{y}$, let $f(\mathbf{x}) = \sum_{\alpha} c_{\boldsymbol{\alpha}}(\hat{\mathbf{y}})\mathbf{y}^{\boldsymbol{\alpha}} \in \mathbb{F}[\hat{\mathbf{y}}][\mathbf{y}]$. Let $H_{\mathbf{y}}^d(f(\mathbf{x}))$ denote the homogeneous component of $f(\mathbf{x})$ of degree d in $\mathbf{y}$ and $\mathrm{Supp}_{\mathbf{y}}(f)$ denote the set $\{\mathbf{y}^{\boldsymbol{\alpha}} \mid c_{\boldsymbol{\alpha}}(\hat{\mathbf{y}}) \neq 0\}$. For simplicity, we write $H_{\mathbf{y}}^{\ell}(f(\mathbf{x}))$ as $H^{\ell}(f(\mathbf{x}))$ and $\mathrm{Supp}_{\mathbf{y}}(f)$ as $\mathrm{Supp}(f)$ when $\mathbf{y} = \mathbf{x}$. For a subset $S = \{f_\lambda(\mathbf{x})\}_{\lambda \in \Lambda}$ of $\mathbb{F}[\mathbf{x}]$, we denote $\mathbb{V}_{\mathbb{F}}(S) := \{\mathbf{s} \in \mathbb{F}^n \mid f_\lambda(\mathbf{s}) = 0, \forall \lambda \in \Lambda\}$. Finally, we present an operation on polynomials as follow.

Definition 3.4 (Linearization, Definition 1.2, restated)**.** *Let $f(\mathbf{x}) = H_{\mathbf{y}}^0(f)(\mathbf{y}) + H_{\mathbf{y}}^1(f)(\mathbf{y}) + \cdots + H_{\mathbf{y}}^d(f)(\mathbf{y})$ be the homogeneous decomposition of $f \in \mathbb{F}[\mathbf{x}] = \mathbb{F}[\hat{\mathbf{y}}][\mathbf{y}]$. For a vector $\mathbf{s} \in \mathbb{F}^m$, we call the linear polynomial $H_{\mathbf{y}}^0(f)(\mathbf{y}) + H_{\mathbf{y}}^1(f)(\mathbf{y}) + \sum_{i=2}^d H_{\mathbf{y}}^i(f)(\mathbf{s})$ the linearization of f at $\mathbf{s}$ with respect to $\mathbf{y}$, denoted by $L_{\mathbf{y}=\mathbf{s}}(f)$. Note that $L_{\mathbf{y}=\mathbf{s}}(f) = f$ if $d \leq 1$. For a polynomial set $S \subseteq \mathbb{F}[\mathbf{x}]$, let $L_{\mathbf{y}=\mathbf{s}}(S) := \{L_{\mathbf{y}=\mathbf{s}}(f) \mid f \in S\}$.*

Fixing $p(\mathbf{x}), q(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ in the following discussion of this section, we will compute $F_{p,q}$. We assume $p(\mathbf{x}) = \sum_{\boldsymbol{\alpha}} c^p_{\boldsymbol{\alpha}} \mathbf{x}^{\boldsymbol{\alpha}}$ and $q(\mathbf{x}) = \sum_{\boldsymbol{\alpha}} c^q_{\boldsymbol{\alpha}} \mathbf{x}^{\boldsymbol{\alpha}}$. We expand $p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x})$ and assume $p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x}) = \sum_{\boldsymbol{\alpha}} c_{\boldsymbol{\alpha}}(\mathbf{a})\mathbf{x}^{\boldsymbol{\alpha}}$, where $c_{\boldsymbol{\alpha}}(\mathbf{a}) \in \mathbb{F}[\mathbf{a}]$ is the coefficient of $\mathbf{x}^{\boldsymbol{\alpha}}$. Let $S := \{c_{\boldsymbol{\alpha}}(\mathbf{a}) \mid \mathbf{x}^{\boldsymbol{\alpha}} \in \mathrm{Supp}_{\mathbf{x}}(p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x}))\} \subseteq \mathbb{F}[\mathbf{a}]$. Without loss of generality, we suppose there are nonlinear polynomials in S. Now we introduce the key notion in this section.

Definition 3.5 (Admissible partition, Definition 1.1, restated)**.** *A set partition $S = S_0 \cup S_1 \cup \cdots \cup S_m$ is said to be* admissible *if the following two conditions hold:*

1. *All polynomials in S_0 are of degree in $\mathbf{a}$ at most one.*
2. *For all $\ell = 1, 2, \cdots, m$, if $c_{\boldsymbol{\alpha}}(\mathbf{a}) \in S_\ell$, then $c_{\boldsymbol{\beta}}(\mathbf{a}) \in \cup_{i=0}^{\ell-1} S_i$ for all $\boldsymbol{\beta} \in \mathbb{N}^n$ with $\boldsymbol{\beta} > \boldsymbol{\alpha}$ and $\mathbf{x}^{\boldsymbol{\beta}} \in \mathrm{Supp}_{\mathbf{x}}(p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x}))$.*

Then we have that any admissible partition of S leads to an algorithm for reducing the polynomial system S into several linear systems.

Theorem 3.6 (Theorem 1.3, restated)**.** *If the partition $S = S_0 \cup S_1 \cup \cdots \cup S_m$ is admissible, then for all $\ell = 1, \cdots, m$, we have either $\mathbb{V}_{\mathbb{F}}\left(\bigcup_{i=0}^{\ell-1} S_i\right) = \varnothing$ or*

$$\mathbb{V}_{\mathbb{F}}\left(\bigcup_{i=0}^{\ell} S_i\right) = \mathbb{V}_{\mathbb{F}}\left(\bigcup_{i=0}^{\ell} L_{\mathbf{a}=\mathbf{s}^{(\ell)}}(S_i)\right) \quad \textit{for any } \mathbf{s}^{(\ell)} \in \mathbb{V}_{\mathbb{F}}\left(\bigcup_{i=0}^{\ell-1} S_i\right).$$

Let V_ℓ denote $\mathbb{V}_{\mathbb{F}}(\cup_{i=0}^{\ell} S_i)$. The above theorem says that we can compute $F_{p,q} = V_m$ by computing $V_0, V_1, \cdots, V_m$ successively. Since the polynomials in $L_{\mathbf{a}=\mathbf{s}^{(\ell)}}(S_i)$ are linear, we can compute V_i by linear-system solvers which is much more efficient than solving a general algebraic system. Moreover, two arbitrary polynomials in $\mathbb{F}[\mathbf{x}]$ are most likely not shift equivalent. When $F_{p,q} = \emptyset$, the algorithms from admissible partitions are usually early terminated which improves the efficiency in practice.

To prove Theorem 3.6, we need to present some facts and lemmas. In the first place, we would like to illustrate the relation among the elements in $\mathrm{Supp}(p(\mathbf{x}))$ and $\mathrm{Supp}_{\mathbf{x}}(p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x}))$, as well as the monomials of some $c_{\boldsymbol{\alpha}}(\mathbf{a}) \in S$.

Fact 3.7. *For arbitrary $\boldsymbol{\alpha} \in \mathbb{N}^n$, we have*

(i) If $c_{\boldsymbol{\alpha}}(\mathbf{a}) \in S$ for some monomial $\mathbf{a}^{\boldsymbol{\beta}} \in \mathrm{Supp}(c_{\boldsymbol{\alpha}}(\mathbf{a}))$, then we have $\mathbf{a}^{\boldsymbol{\beta}}\mathbf{x}^{\boldsymbol{\alpha}} \in \mathrm{Supp}(p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x}))$ and $\mathbf{x}^{\boldsymbol{\alpha}} \in \mathrm{Supp}_{\mathbf{x}}(p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x}))$. In addition, if $\boldsymbol{\beta} > \mathbf{0}$, then $\mathbf{a}^{\boldsymbol{\beta}}\mathbf{x}^{\boldsymbol{\alpha}}$ can only come from the expansion of $(\mathbf{x}+\mathbf{a})^{\boldsymbol{\alpha}+\boldsymbol{\beta}}$, so $\mathbf{x}^{\boldsymbol{\alpha}+\boldsymbol{\beta}} \in \mathrm{Supp}(p(\mathbf{x}))$.

(ii) Conversely, if $\mathbf{x}^{\boldsymbol{\alpha}} \in \mathrm{Supp}(p(\mathbf{x}))$, then we have $(\mathbf{x}+\mathbf{a})^{\boldsymbol{\alpha}}$ in $p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x})$. Combining (i), for all $\boldsymbol{\beta} \in \mathbb{N}^n$ such that $\boldsymbol{\alpha} > \boldsymbol{\beta}$, we have $\mathbf{a}^{\boldsymbol{\alpha}-\boldsymbol{\beta}}\mathbf{x}^{\boldsymbol{\beta}} \in \mathrm{Supp}(p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x}))$ and $\mathbf{x}^{\boldsymbol{\beta}} \in \mathrm{Supp}_{\mathbf{x}}(p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x}))$.

Now we can give an explicit expression of the nonlinear homogeneous component of $c_{\boldsymbol{\alpha}}(\mathbf{a})$.

Lemma 3.8. *Let $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \cdots, \alpha_n) \in \mathbb{N}^n$, such that $c_{\boldsymbol{\alpha}}(\mathbf{a}) \in S$ and $d := \deg(c_{\boldsymbol{\alpha}}(\mathbf{a})) > 1$. Then for all $2 \le k \le d$,*

$$H^k(c_{\boldsymbol{\alpha}}(\mathbf{a})) = \sum_{j_1=1}^{n} \cdots \sum_{j_k=1}^{n} \Big(\frac{c^p_{\boldsymbol{\alpha}+\sum_{i=1}^k \mathbf{e}_{j_i}}}{\binom{k}{\sum_{i=1}^k \mathbf{e}_{j_i}}} \prod_{\ell=1}^{n} \binom{\alpha_\ell + \sum_{i=1}^k \delta_{j_i}^\ell}{\alpha_\ell} \Big) \mathbf{a}^{\sum_{i=1}^k \mathbf{e}_{j_i}},$$

where $\mathbf{e}_i \in \mathbb{N}^n$ is a unit vector with only the i-th component nonzero and δ_i^ℓ is one only when $i = \ell$.

Proof. For arbitrary $\boldsymbol{\beta} = (\beta_1, \beta_2, \cdots, \beta_n) \in \mathbb{N}^n, |\boldsymbol{\beta}| = k$, if the monomial $\mathbf{a}^{\boldsymbol{\beta}}$ is in $\mathrm{Supp}(c_{\boldsymbol{\alpha}}(\mathbf{a}))$, then by item (i) in Fact 3.7, it can only come from the expansion of $c^p_{\boldsymbol{\alpha}+\boldsymbol{\beta}} \cdot (\mathbf{x}+\mathbf{a})^{\boldsymbol{\alpha}+\boldsymbol{\beta}}$. Therefore, the coefficient of $\mathbf{a}^{\boldsymbol{\beta}}$ is $c^p_{\boldsymbol{\alpha}+\boldsymbol{\beta}} \cdot \prod_{\ell=1}^n \binom{\alpha_\ell+\beta_\ell}{\alpha_\ell}$ and

$$H^k(c_{\boldsymbol{\alpha}}(\mathbf{a})) = \sum_{|\boldsymbol{\beta}|=k} \Big(c^p_{\boldsymbol{\alpha}+\boldsymbol{\beta}} \prod_{\ell=1}^n \binom{\alpha_\ell+\beta_\ell}{\alpha_\ell} \Big) \mathbf{a}^{\boldsymbol{\beta}}.$$

On the other hand, $\boldsymbol{\beta}$ can be expressed as a sum of k unit vectors. Note that there are $\binom{k}{\boldsymbol{\beta}}$ different k-tuples $(j_1, j_2, \cdots, j_k)$ such that $\boldsymbol{\beta} = \sum_{i=1}^k \mathbf{e}_{j_i}$. Then we also have $\beta_\ell = \sum_{i=1}^k \delta^\ell_{j_i}$. Therefore, the right-hand side of the above equation is equal to

$$\sum_{j_1=1}^n \cdots \sum_{j_k=1}^n \Big(\frac{c^p_{\boldsymbol{\alpha}+\sum_{i=1}^k \mathbf{e}_{j_i}}}{\binom{k}{\sum_{i=1}^k \mathbf{e}_{j_i}}} \prod_{\ell=1}^n \binom{\alpha_\ell + \sum_{i=1}^k \delta^\ell_{j_i}}{\alpha_\ell} \Big) \mathbf{a}^{\sum_{i=1}^k \mathbf{e}_{j_i}},$$

which completes the proof. ∎

This lemma not only expresses the $H^k(c_{\boldsymbol{\alpha}}(\mathbf{a}))$, but also converts $\mathbf{a}^{\boldsymbol{\beta}}$ into $\mathbf{a}^{\sum_{i=1}^k \mathbf{e}_{j_i}}$. This form gives us convenience to the factorization as following.

Lemma 3.9. *Let $k \in \mathbb{N}$ with $k \geq 2$ and assume that $f(x_1, x_2, \cdots, x_k)$ is any symmetric function, i.e. for all i, j with $1 \leq i < j \leq k$, we have*

$$\begin{aligned} &f(x_1, \cdots, x_{i-1}, x_i, x_{i+1}, \cdots, x_{j-1}, x_j, x_{j+1}, \cdots, x_k) \\ =&f(x_1, \cdots, x_{i-1}, x_j, x_{i+1}, \cdots, x_{j-1}, x_i, x_{j+1}, \cdots, x_k). \end{aligned}$$

Then we have

$$\begin{aligned} &\sum_{j_1=1}^n \cdots \sum_{j_k=1}^n f(x_{j_1}, x_{j_2}, \cdots, x_{j_k})(\mathbf{a}^{\sum_{i=1}^k \mathbf{e}_{j_i}} - \mathbf{b}^{\sum_{i=1}^k \mathbf{e}_{j_i}}) \\ =&\sum_{j_1=1}^n \cdots \sum_{j_k=1}^n f(x_{j_1}, x_{j_2}, \cdots, x_{j_k})(\mathbf{a}^{\mathbf{e}_{j_k}} - \mathbf{b}^{\mathbf{e}_{j_k}})(\sum_{\ell=1}^k \mathbf{a}^{\sum_{i=1}^{k-\ell} \mathbf{e}_{j_i}} \mathbf{b}^{\sum_{i=k-\ell+1}^{k-1} \mathbf{e}_{j_i}}). \end{aligned}$$

Proof. By a direct calculation, we have

$$\begin{aligned} &(\mathbf{a}^{\mathbf{e}_{j_k}} - \mathbf{b}^{\mathbf{e}_{j_k}})(\sum_{\ell=1}^k \mathbf{a}^{\sum_{i=1}^{k-\ell} \mathbf{e}_{j_i}} \mathbf{b}^{\sum_{i=k-\ell+1}^{k-1} \mathbf{e}_{j_i}}) \\ =&\sum_{\ell=1}^k \mathbf{a}^{\mathbf{e}_{j_k} + \sum_{i=1}^{k-\ell} \mathbf{e}_{j_i}} \mathbf{b}^{\sum_{i=k-\ell+1}^{k-1} \mathbf{e}_{j_i}} - \sum_{\ell=1}^k \mathbf{a}^{\sum_{i=1}^{k-\ell} \mathbf{e}_{j_i}} \mathbf{b}^{\sum_{i=k-\ell+1}^{k} \mathbf{e}_{j_i}} \\ =&(\mathbf{a}^{\sum_{i=1}^k \mathbf{e}_{j_i}} - \mathbf{b}^{\sum_{i=1}^k \mathbf{e}_{j_i}}) \\ &+(\sum_{\ell=2}^k \mathbf{a}^{\mathbf{e}_{j_k} + \sum_{i=1}^{k-\ell} \mathbf{e}_{j_i}} \mathbf{b}^{\sum_{i=k-\ell+1}^{k-1} \mathbf{e}_{j_i}} - \sum_{\ell=1}^{k-1} \mathbf{a}^{\sum_{i=1}^{k-\ell} \mathbf{e}_{j_i}} \mathbf{b}^{\sum_{i=k-\ell+1}^{k} \mathbf{e}_{j_i}}). \end{aligned}$$

Therefore, we merely need to check that

$$\begin{aligned} &\sum_{j_1=1}^n \cdots \sum_{j_k=1}^n f(x_{j_1}, x_{j_2}, \cdots, x_{j_k}) \sum_{\ell=2}^k \mathbf{a}^{\mathbf{e}_{j_k} + \sum_{i=1}^{k-\ell} \mathbf{e}_{j_i}} \mathbf{b}^{\sum_{i=k-\ell+1}^{k-1} \mathbf{e}_{j_i}} \\ =&\sum_{j_1=1}^n \cdots \sum_{j_k=1}^n f(x_{j_1}, x_{j_2}, \cdots, x_{j_k}) \sum_{\ell=1}^{k-1} \mathbf{a}^{\sum_{i=1}^{k-\ell} \mathbf{e}_{j_i}} \mathbf{b}^{\sum_{i=k-\ell+1}^{k} \mathbf{e}_{j_i}}. \end{aligned} \tag{3.1}$$

We have

$$\begin{aligned}
&\sum_{j_1=1}^{n}\cdots\sum_{j_k=1}^{n} f(x_{j_1},x_{j_2},\cdots,x_{j_k})\sum_{\ell=2}^{k}\mathbf{a}^{\mathbf{e}_{j_k}+\sum_{i=1}^{k-\ell}\mathbf{e}_{j_i}}\mathbf{b}^{\sum_{i=k-\ell+1}^{k-1}\mathbf{e}_{j_i}}\\
=&\sum_{j_1=1}^{n}\cdots\sum_{j_k=1}^{n} f(x_{j_1},x_{j_2},\cdots,x_{j_k})\sum_{\ell=1}^{k-1}\mathbf{a}^{\mathbf{e}_{j_k}+\sum_{i=1}^{k-\ell-1}\mathbf{e}_{j_i}}\mathbf{b}^{\sum_{i=k-\ell}^{k-1}\mathbf{e}_{j_i}}\\
=&\sum_{\ell=1}^{k-1}\sum_{j_1=1}^{n}\cdots\sum_{j_k=1}^{n} f(x_{j_1},x_{j_2},\cdots,x_{j_k})\mathbf{a}^{\mathbf{e}_{j_k}+\sum_{i=1}^{k-\ell-1}\mathbf{e}_{j_i}}\mathbf{b}^{\mathbf{e}_{j_{k-\ell}}+\sum_{i=k-\ell+1}^{k-1}\mathbf{e}_{j_i}}.
\end{aligned}$$

For any $\ell=1,2,\cdots,k-1$, when we fix ℓ, we can commute j_k and $j_{k-\ell}$ in the expression above by the symmetry of $f(x_{j_1},x_{j_2},\cdots,x_{j_k})$. So we get

$$\begin{aligned}
&\sum_{j_1=1}^{n}\cdots\sum_{j_k=1}^{n} f(x_{j_1},x_{j_2},\cdots,x_{j_k})\mathbf{a}^{\mathbf{e}_{j_k}+\sum_{i=1}^{k-\ell-1}\mathbf{e}_{j_i}}\mathbf{b}^{\mathbf{e}_{j_{k-\ell}}+\sum_{i=k-\ell+1}^{k-1}\mathbf{e}_{j_i}}\\
=&\sum_{j_1=1}^{n}\cdots\sum_{j_k=1}^{n} f(x_{j_1},x_{j_2},\cdots,x_{j_k})\mathbf{a}^{\mathbf{e}_{j_{k-\ell}}+\sum_{i=1}^{k-\ell-1}\mathbf{e}_{j_i}}\mathbf{b}^{\mathbf{e}_{j_k}+\sum_{i=k-\ell+1}^{k-1}\mathbf{e}_{j_i}}\\
=&\sum_{j_1=1}^{n}\cdots\sum_{j_k=1}^{n} f(x_{j_1},x_{j_2},\cdots,x_{j_k})\mathbf{a}^{\sum_{i=1}^{k-\ell}\mathbf{e}_{j_i}}\mathbf{b}^{\sum_{i=k-\ell+1}^{k}\mathbf{e}_{j_i}},
\end{aligned}$$

which completes the proof of Equation (3.1). So we finally prove the result as we want. ∎

With these lemmas, we can finally prove the following proposition, which is crucial in the proof of Theorem 3.6.

Proposition 3.10. *Let $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\cdots,\alpha_n)\in\mathbb{N}^n$ be such that $c_{\boldsymbol{\alpha}}(\mathbf{a})\in S$ and $d:=\deg(c_{\boldsymbol{\alpha}}(\mathbf{a}))>1$. Let $k\in\mathbb{N}$, $2\le k\le d$, and $\mathbf{r},\mathbf{s}\in\mathbb{F}^n$. If for all $\boldsymbol{\beta}\in\mathbb{N}^n$ with $\boldsymbol{\beta}\ge\boldsymbol{\alpha}$ and $|\boldsymbol{\beta}|=|\boldsymbol{\alpha}|+k-1$,*

$$H^1(c_{\boldsymbol{\beta}}(\mathbf{r}))=H^1(c_{\boldsymbol{\beta}}(\mathbf{s})),$$

then we have

$$H^k(c_{\boldsymbol{\alpha}}(\mathbf{r}))=H^k(c_{\boldsymbol{\alpha}}(\mathbf{s})).$$

Proof. We would like to verify that $H^k(c_{\boldsymbol{\alpha}}(\mathbf{a}))-H^k(c_{\boldsymbol{\alpha}}(\mathbf{b}))$ is a combination of $\{H^1(c_{\boldsymbol{\beta}}(\mathbf{a}))-H^1(c_{\boldsymbol{\beta}}(\mathbf{b}))\mid\boldsymbol{\beta}\ge\boldsymbol{\alpha},\ |\boldsymbol{\beta}|=|\boldsymbol{\alpha}|+k-1\}$. By Lemma 3.8 and Lemma 3.9, we have

$$\begin{aligned}
&H^1(c_{\boldsymbol{\alpha}+\sum_{i=1}^{k-1}\mathbf{e}_{j_i}}(\mathbf{a}))-H^1(c_{\boldsymbol{\alpha}+\sum_{i=1}^{k-1}\mathbf{e}_{j_i}}(\mathbf{b}))\\
=&\sum_{j_k=1}^{n}\left(c^p_{\boldsymbol{\alpha}+\sum_{i=1}^{k}\mathbf{e}_{j_i}}\prod_{\ell=1}^{n}\binom{\alpha_\ell+\sum_{i=1}^{k}\delta^\ell_{j_i}}{\delta^\ell_{j_k}}\right)\cdot(\mathbf{a}^{\mathbf{e}_{j_k}}-\mathbf{b}^{\mathbf{e}_{j_k}}),
\end{aligned}$$

and

$$
\begin{aligned}
&H^k(c_{\boldsymbol{\alpha}}(\mathbf{a})) - H^k(c_{\boldsymbol{\alpha}}(\mathbf{b})) \\
&= \sum_{j_1=1}^{n} \cdots \sum_{j_k=1}^{n} f(j_1, j_2, \cdots, j_k)(\mathbf{a}^{\sum_{i=1}^{k} \mathbf{e}_{j_i}} - \mathbf{a}^{\sum_{i=1}^{k} \mathbf{e}_{j_i}}) \\
&= \sum_{j_1=1}^{n} \cdots \sum_{j_k=1}^{n} f(j_1, j_2, \cdots, j_k)(\mathbf{a}^{\mathbf{e}_{j_k}} - \mathbf{b}^{\mathbf{e}_{j_k}})(\sum_{\ell=1}^{k} \mathbf{a}^{\sum_{i=1}^{k-\ell} \mathbf{e}_{j_i}} \mathbf{b}^{\sum_{i=k-\ell+1}^{k-1} \mathbf{e}_{j_i}}) \\
&= \sum_{j_1=1}^{n} \cdots \sum_{j_k=1}^{n} \frac{f(j_1, j_2, \cdots, j_k)}{c^p_{\boldsymbol{\alpha}+\sum_{i=1}^{k} \mathbf{e}_{j_i}} \prod_{\ell=1}^{n} \binom{\alpha_\ell + \sum_{i=1}^{k} \delta^\ell_{j_i}}{\delta^\ell_{j_k}}} \sum_{\ell=1}^{k} \mathbf{a}^{\sum_{i=1}^{k-\ell} \mathbf{e}_{j_i}} \mathbf{b}^{\sum_{i=k-\ell+1}^{k-1} \mathbf{e}_{j_i}} \\
&\qquad \cdot \Big(c^p_{\boldsymbol{\alpha}+\sum_{i=1}^{k} \mathbf{e}_{j_i}} \prod_{\ell=1}^{n} \binom{\alpha_\ell + \sum_{i=1}^{k} \delta^\ell_{j_i}}{\delta^\ell_{j_k}} \Big) \cdot (\mathbf{a}^{\mathbf{e}_{j_k}} - \mathbf{b}^{\mathbf{e}_{j_k}}) \\
&= \sum_{j_1=1}^{n} \cdots \sum_{j_k=1}^{n} g(j_1, j_2, \cdots, j_k) \sum_{\ell=1}^{k} \mathbf{a}^{\sum_{i=1}^{k-\ell} \mathbf{e}_{j_i}} \mathbf{b}^{\sum_{i=k-\ell+1}^{k-1} \mathbf{e}_{j_i}} \\
&\qquad \cdot \Big(c^p_{\boldsymbol{\alpha}+\sum_{i=1}^{k} \mathbf{e}_{j_i}} \prod_{\ell=1}^{n} \binom{\alpha_\ell + \sum_{i=1}^{k} \delta^\ell_{j_i}}{\delta^\ell_{j_k}} \Big) \cdot (\mathbf{a}^{\mathbf{e}_{j_k}} - \mathbf{b}^{\mathbf{e}_{j_k}}),
\end{aligned}
$$

where

$$
f(j_1, j_2, \cdots, j_k) := \frac{c^p_{\boldsymbol{\alpha}+\sum_{i=1}^{k} \mathbf{e}_{j_i}}}{\binom{k}{\sum_{i=1}^{k} \mathbf{e}_{j_i}}} \prod_{\ell=1}^{n} \binom{\alpha_\ell + \sum_{i=1}^{k} \delta^\ell_{j_i}}{\alpha_\ell}
$$

is a symmetric function, and

$$
g(j_1, j_2, \cdots, j_k) := \frac{f(j_1, j_2, \cdots, j_k)}{c^p_{\boldsymbol{\alpha}+\sum_{i=1}^{k} \mathbf{e}_{j_i}} \prod_{\ell=1}^{n} \binom{\alpha_\ell + \sum_{i=1}^{k} \delta^\ell_{j_i}}{\delta^\ell_{j_k}}}.
$$

Notice that $\sum_{\ell=1}^{k} \mathbf{a}^{\sum_{i=1}^{k-\ell} \mathbf{e}_{j_i}} \mathbf{b}^{\sum_{i=k-\ell+1}^{k-1} \mathbf{e}_{j_i}}$ is free of j_k. So if we can prove that $g(j_1, j_2, \cdots, j_k)$ is free of j_k as well, then we get

$$
\begin{aligned}
&H^k(c_{\boldsymbol{\alpha}}(\mathbf{a})) - H^k(c_{\boldsymbol{\alpha}}(\mathbf{b})) \\
&= \sum_{j_1=1}^{n} \cdots \sum_{j_{k-1}=1}^{n} g(j_1, j_2, \cdots, j_k) \sum_{\ell=1}^{k} \mathbf{a}^{\sum_{i=1}^{k-\ell} \mathbf{e}_{j_i}} \mathbf{b}^{\sum_{i=k-\ell+1}^{k-1} \mathbf{e}_{j_i}} \\
&\qquad \cdot \Big(\sum_{j_k=1}^{n} \Big(c^p_{\boldsymbol{\alpha}+\sum_{i=1}^{k} \mathbf{e}_{j_i}} \prod_{\ell=1}^{n} \binom{\alpha_\ell + \sum_{i=1}^{k} \delta^\ell_{j_i}}{\delta^\ell_{j_k}} \Big) \cdot (\mathbf{a}^{\mathbf{e}_{j_k}} - \mathbf{b}^{\mathbf{e}_{j_k}}) \Big) \\
&= \sum_{j_1=1}^{n} \cdots \sum_{j_{k-1}=1}^{n} g(j_1, j_2, \cdots, j_k) \sum_{\ell=1}^{k} \mathbf{a}^{\sum_{i=1}^{k-\ell} \mathbf{e}_{j_i}} \mathbf{b}^{\sum_{i=k-\ell+1}^{k-1} \mathbf{e}_{j_i}} \\
&\qquad \cdot \Big(H^1(c_{\boldsymbol{\alpha}+\sum_{i=1}^{k-1} \mathbf{e}_{j_i}}(\mathbf{a})) - H^1(c_{\boldsymbol{\alpha}+\sum_{i=1}^{k-1} \mathbf{e}_{j_i}}(\mathbf{b})) \Big),
\end{aligned}
$$

which completes the proof. Now we only need to compute $g(j_1, j_2, \cdots, j_k)$ in order to verify that it is free of j_k.

$$
\begin{aligned}
g(j_1,j_2,\cdots,j_k) &= \frac{f(j_1,j_2,\cdots,j_k)}{c^p_{\boldsymbol{\alpha}+\sum_{i=1}^k \mathbf{e}_{j_i}} \prod_{\ell=1}^n \binom{\alpha_\ell+\sum_{i=1}^k \delta^\ell_{j_i}}{\delta^\ell_{j_k}}} \\
&= \frac{\prod_{\ell=1}^n \binom{\alpha_\ell+\sum_{i=1}^k \delta^\ell_{j_i}}{\alpha_\ell}}{\binom{k}{\sum_{i=1}^k \mathbf{e}_{j_i}} \prod_{\ell=1}^n \binom{\alpha_\ell+\sum_{i=1}^k \delta^\ell_{j_i}}{\delta^\ell_{j_k}}} = \frac{\prod_{\ell=1}^n \binom{\alpha_\ell+\sum_{i=1}^k \delta^\ell_{j_i}}{\alpha_\ell}}{\binom{k}{\sum_{i=1}^k \mathbf{e}_{j_i}} (\alpha_{j_k} + \sum_{i=1}^k \delta^{j_k}_{j_i})} \\
&= \frac{\prod_{\ell=1}^n \frac{(\alpha_\ell+\sum_{i=1}^k \delta^\ell_{j_i})!}{\alpha_\ell! (\sum_{i=1}^k \delta^\ell_{j_i})!}}{\frac{k!}{\prod_{\ell=1}^n (\sum_{i=1}^k \delta^\ell_{j_i})!}(\alpha_{j_k} + \sum_{i=1}^k \delta^{j_k}_{j_i})} = \frac{\prod_{\ell=1}^n (\alpha_\ell + \sum_{i=1}^k \delta^\ell_{j_i})!}{k! (\prod_{\ell=1}^n \alpha_\ell!)(\alpha_{j_k} + \sum_{i=1}^k \delta^{j_k}_{j_i})} \\
&= \frac{\prod_{\ell=1}^n (\alpha_\ell + \sum_{i=1}^{k-1} \delta^\ell_{j_i})!}{k! \prod_{\ell=1}^n \alpha_\ell!}.
\end{aligned}
$$

∎

Now we are ready to prove Theorem 3.6.

Proof of Theorem 3.6. For convenience, we denote $S_i^{(\ell)} := L_{\mathbf{a}=\mathbf{s}^{(\ell)}}(S_i)$ and $c_{\boldsymbol{\alpha}}^{(\ell)} := L_{\mathbf{a}=\mathbf{s}^{(\ell)}}(c_{\boldsymbol{\alpha}})$.

At first, it is simple to find that we must have $m \geq 1$ because there are nonlinear polynomials in S. When $m > 1$, we claim that for all $1 \leq \ell \leq m-1$, if $V_\ell \neq \varnothing$, then $c_{\boldsymbol{\alpha}}^{(\ell+1)}(\mathbf{a}) = c_{\boldsymbol{\alpha}}^{(\ell)}(\mathbf{a})$ for all $c_{\boldsymbol{\alpha}}(\mathbf{a}) \in \cup_{i=0}^{\ell} S_i$. We shall prove the theorem by induction on ℓ, as well as the claim if $m > 1$.

When $\ell = 1$, we have $V_0 = \mathbb{V}_{\mathbb{F}}(S_0)$ and for any $c_{\boldsymbol{\beta}}(\mathbf{a}) \in S_0$, $\deg(c_{\boldsymbol{\beta}}(\mathbf{a})) \leq 1$. Hence, $S_0^{(1)} = S_0$. Then we know that both V_1 and $\mathbb{V}_{\mathbb{F}}(S_0^{(1)} \cup S_1^{(1)})$ are the subsets of V_0. Therefore, to prove the theorem, we just need to verify that for all $\mathbf{r} \in V_0$, $\mathbf{r} \in V_1$ if and only if $\mathbf{r} \in \mathbb{V}_{\mathbb{F}}(S_0^{(1)} \cup S_1^{(1)})$. Let $\mathbf{r} \in V_0$. For arbitrary $c_{\boldsymbol{\alpha}}(\mathbf{a}) \in S_0 \cup S_1$, assume the degree of $c_{\boldsymbol{\alpha}}(\mathbf{a})$ is $d \geq 2$. Then for $2 \leq k \leq d$, let $\boldsymbol{\beta} \in \mathbb{N}^n$ be such that $\boldsymbol{\beta} \geq \boldsymbol{\alpha}$ and $|\boldsymbol{\beta}| = |\boldsymbol{\alpha}| + k - 1 > |\boldsymbol{\alpha}|$, so we have $\boldsymbol{\beta} > \boldsymbol{\alpha}$, which means either $c_{\boldsymbol{\beta}}(\mathbf{a}) \in S_0$ or $c_{\boldsymbol{\beta}}(\mathbf{a}) = 0$. Both of these cases imply that $c_{\boldsymbol{\beta}}(\mathbf{a})$ is a linear polynomial, so $H^1(c_{\boldsymbol{\beta}})(\mathbf{r}) = -H^0(c_{\boldsymbol{\beta}}) = H^1(c_{\boldsymbol{\beta}})(\mathbf{s}^{(1)})$. By Proposition 3.10, we know $H^k(c_{\boldsymbol{\alpha}})(\mathbf{r}) = H^k(c_{\boldsymbol{\alpha}})(\mathbf{s}^{(1)})$, which tells us exactly $\mathbf{r} \in V_1$ if and only if $\mathbf{r} \in \mathbb{V}_{\mathbb{F}}(S_0^{(1)} \cup S_1^{(1)})$. If $m = 1$, we have completed all of the proof. Else, we shall go on by proving the claim when $\ell = 1$. If $V_1 \neq \varnothing$, then $\mathbf{s}^{(2)} \in V_1 \subset V_0$. Therefore, $H^k(c_{\boldsymbol{\alpha}})(\mathbf{s}^{(2)}) = H^k(c_{\boldsymbol{\alpha}})(\mathbf{s}^{(1)})$, which implies that $c_{\boldsymbol{\alpha}}^{(2)}(\mathbf{a}) = c_{\boldsymbol{\alpha}}^{(1)}(\mathbf{a})$.

Now we consider the case where $\ell > 1$ and suppose the theorem and claim hold for smaller ℓ. Then we have $V_{\ell-1} = \mathbb{V}_{\mathbb{F}}(\cup_{i=0}^{\ell-1} S_i^{(\ell-1)})$ and for all $c_{\boldsymbol{\beta}}(\mathbf{a}) \in \cup_{i=0}^{\ell-1} S_i$, $c_{\boldsymbol{\beta}}^{(\ell)}(\mathbf{a}) = c_{\boldsymbol{\beta}}^{(\ell-1)}(\mathbf{a})$. Therefore, $\cup_{i=0}^{\ell-1} S_i^{(\ell)} = \cup_{i=0}^{\ell-1} S_i^{(\ell-1)}$. It means that both V_ℓ and $\mathbb{V}_{\mathbb{F}}(\cup_{i=0}^{\ell} S_i^{(\ell)})$ are the subset of $V_{\ell-1}$. Consequently, in order to prove the theorem, we merely should prove that for all $\mathbf{r} \in V_{\ell-1}$, $\mathbf{r} \in V_\ell$ if and only if $\mathbf{r} \in \mathbb{V}_{\mathbb{F}}(\cup_{i=0}^{\ell} S_i^{(\ell)})$. Let $\mathbf{r} \in V_{\ell-1}$. Note that $H^1(c_{\boldsymbol{\beta}}(\mathbf{a})) = H^1(c_{\boldsymbol{\beta}}^{(\ell-1)}(\mathbf{a}))$. Hence, $H^1(c_{\boldsymbol{\beta}})(\mathbf{r}) = H^1(c_{\boldsymbol{\beta}}^{(\ell-1)})(\mathbf{r}) = -H^0(c_{\boldsymbol{\beta}}^{(\ell-1)}) = H^1(c_{\boldsymbol{\beta}}^{(\ell-1)})(\mathbf{s}^{(\ell)}) = H^1(c_{\boldsymbol{\beta}})(\mathbf{s}^{(\ell)})$. For arbitrary $c_{\boldsymbol{\alpha}}(\mathbf{a}) \in \cup_{i=0}^{\ell} S_i$, assume the degree of $c_{\boldsymbol{\alpha}}(\mathbf{a})$ is $d \geq 2$. Then for $2 \leq k \leq d$, we can similarly get $H^k(c_{\boldsymbol{\alpha}})(\mathbf{r}) = H^k(c_{\boldsymbol{\alpha}})(\mathbf{s}^{(\ell)})$, which completes the proof of the theorem. If $\ell < m$ and $V_\ell \neq \varnothing$, we get $\mathbf{s}^{(\ell+1)} \in V_\ell \subset V_{\ell-1}$. The proof of the claim is similar to the case when $\ell = 1$. ∎

3.2 Two special admissible partitions

By Theorem 3.6, we see that any admissible partition leads to an algorithm for solving the SET problem via linear system solving. We now show that two special partitions are admissible. The first admissible partition defined below is partitioning the polynomial system $S_{p,q}$ according to their degree in $\mathbf{a}$, which will be called the $\mathbf{a}$-*degree partition*.

Theorem 3.11 ($\mathbf{a}$-degree partition, Theorem 1.3, restated)**.** *Let* $S_i^D := \{c_{\boldsymbol{\alpha}}(\mathbf{a}) \in S \mid \deg(c_{\boldsymbol{\alpha}}(\mathbf{a})) = i\}$. *Then the partition* $S = S_0^D \cup S_1^D \cup \cdots \cup S_m^D$ *is admissible.*

Proof. Let us check this partition satisfies two conditions mentioned in Definition 3.5. The condition (i) can be checked directly by definition. As for (ii), let us assume $c_{\boldsymbol{\alpha}}(\mathbf{a}) \in S_\ell^D$ and $\boldsymbol{\beta}$ is an arbitrary vector in $\mathbb{N}^n$, such that $\boldsymbol{\beta} > \boldsymbol{\alpha}$ and $\mathbf{x}^{\boldsymbol{\beta}} \in \mathrm{Supp}_{\mathbf{x}}(p(\mathbf{x}+\mathbf{a})-q(\mathbf{x}))$. We will argue by contradiction that $\deg(c_{\boldsymbol{\alpha}}(\mathbf{a})) > \deg(c_{\boldsymbol{\beta}}(\mathbf{a}))$. By assumption, we know that $\deg(c_{\boldsymbol{\alpha}}(\mathbf{a})) = \ell$. If there is a monomial $\mathbf{a}^{\boldsymbol{\gamma}} \in \mathrm{Supp}(c_{\boldsymbol{\beta}}(\mathbf{a}))$ with $|\boldsymbol{\gamma}| \geq \ell$, then by Fact 3.7 (i), we have $\mathbf{x}^{\boldsymbol{\gamma}+\boldsymbol{\beta}} \in \mathrm{Supp}(p(\mathbf{x}))$. Since $\boldsymbol{\gamma}+\boldsymbol{\beta} \geq \boldsymbol{\beta} > \boldsymbol{\alpha}$, use Fact 3.7 (ii) we know $\mathbf{a}^{\boldsymbol{\gamma}+\boldsymbol{\beta}-\boldsymbol{\alpha}}\mathbf{x}^{\boldsymbol{\alpha}} \in \mathrm{Supp}(p(\mathbf{x}+\mathbf{a})-q(\mathbf{x}))$. As a result, $\mathbf{a}^{\boldsymbol{\gamma}+\boldsymbol{\beta}-\boldsymbol{\alpha}} \in \mathrm{Supp}(c_{\boldsymbol{\alpha}}(\mathbf{a}))$. However, notice that $\boldsymbol{\beta} > \boldsymbol{\alpha}$ implies $|\boldsymbol{\beta}| > |\boldsymbol{\alpha}|$, so $|\boldsymbol{\gamma}+\boldsymbol{\beta}-\boldsymbol{\alpha}| = |\boldsymbol{\gamma}|+|\boldsymbol{\beta}|-|\boldsymbol{\alpha}| > \ell$, which leads to a contradiction to the fact that ℓ is the degree of $c_{\boldsymbol{\alpha}}(\mathbf{a})$. ∎

Note that $\boldsymbol{\beta} > \boldsymbol{\alpha}$ implies $|\boldsymbol{\beta}| > |\boldsymbol{\alpha}|$. This inspires the second admissible partition called $\mathbf{x}$-*homogeneous partition*. Before we prove this, let us first present a useful lemma.

Lemma 3.12. *Let d be the degree of $p(\mathbf{x})$. For any $\boldsymbol{\alpha} \in \mathbb{N}^n$, $c_{\boldsymbol{\alpha}}(\mathbf{a}) \in S$, we have $\deg(c_{\boldsymbol{\alpha}}(\mathbf{a})) \leq d - |\boldsymbol{\alpha}|$.*

Proof. Similar with the proof in Theorem 3.11, we will argue by contradiction. If there is a monomial $\mathbf{a}^{\boldsymbol{\beta}} \in \mathrm{Supp}(c_{\boldsymbol{\alpha}}(\mathbf{a}))$ with $|\boldsymbol{\beta}| > d - |\boldsymbol{\alpha}|$, then by Fact 3.7 (i), we have $\mathbf{x}^{\boldsymbol{\alpha}+\boldsymbol{\beta}} \in \mathrm{Supp}(p(\mathbf{x}))$. However, $|\boldsymbol{\alpha}+\boldsymbol{\beta}| = |\boldsymbol{\alpha}|+|\boldsymbol{\beta}| > d$, which leads to a contradiction to that d is the degree of $p(\mathbf{x})$. ∎

Theorem 3.13 ($\mathbf{x}$-homogeneous partition, Theorem 1.3, restated)**.** *Let d be the degree of $p(\mathbf{x}+\mathbf{a})-q(\mathbf{x})$ with respect to $\mathbf{x}$. Let $S_i^H := \{c_{\boldsymbol{\alpha}}(\mathbf{a}) \in S \mid |\boldsymbol{\alpha}| = d - i\}$. Then the partition $S = S_0^H \cup S_1^H \cup \cdots \cup S_d^H$ is admissible.*

Proof. We first need to show that $S = S_0^H \cup S_1^H \cup \cdots \cup S_d^H$ is exactly a partition of S. It is true because for arbitrary $c_{\boldsymbol{\alpha}}(\mathbf{a}) \in S$, we have $\mathbf{x}^{\boldsymbol{\alpha}} \in \mathrm{Supp}_{\mathbf{x}}(p(\mathbf{x}+\mathbf{a})-q(\mathbf{x}))$, so $0 \leq |\boldsymbol{\alpha}| \leq d$.

Then we check this partition is admissible. If there is some $c_{\boldsymbol{\alpha}}(\mathbf{a}) \in S_0^H$ with a nonlinear monomial $\mathbf{a}^{\boldsymbol{\beta}}$, then by Fact 3.7 (i), we have $\mathbf{x}^{\boldsymbol{\alpha}+\boldsymbol{\beta}} \in \mathrm{Supp}(p(\mathbf{x}))$. For $|\boldsymbol{\beta}| \geq 2$, there is a uint vector $\mathbf{e}_j \in \mathbb{N}^n$ such that $\mathbf{e}_j < \boldsymbol{\alpha}+\boldsymbol{\beta}$. By Fact 3.7 (i), we get $\mathbf{x}^{\boldsymbol{\alpha}+\boldsymbol{\beta}-\mathbf{e}_j} \in \mathrm{Supp}_{\mathbf{x}}(p(\mathbf{x}+\mathbf{a})-q(\mathbf{x}))$. However, $|\boldsymbol{\alpha}+\boldsymbol{\beta}-\mathbf{e}_j| = |\boldsymbol{\alpha}|+|\boldsymbol{\beta}|-|\mathbf{e}_1| \geq d+2-1$, which leads to a contradiction to the fact that the degree of $p(\mathbf{x}+\mathbf{a})-q(\mathbf{x})$ with respect to $\mathbf{x}$ is at most d. So the condition (i) in Definition 3.5 is satisfied. Finally, for all $\ell = 1, 2, \cdots, d$, if $c_{\boldsymbol{\alpha}}(\mathbf{a}) \in S_\ell^H$, then for all $\boldsymbol{\beta} \in \mathbb{N}^n$ with $\boldsymbol{\beta} > \boldsymbol{\alpha}$ and $\mathbf{x}^{\boldsymbol{\beta}} \in \mathrm{Supp}_{\mathbf{x}}(p(\mathbf{x}+\mathbf{a})-q(\mathbf{x}))$, we have $|\boldsymbol{\beta}| > |\boldsymbol{\alpha}| = d - \ell$, so $c_{\boldsymbol{\beta}}(\mathbf{a}) \in S_{d-|\boldsymbol{\beta}|}^H \subset \cup_{i=0}^{\ell-1} S_i^H$, which means $S_0^H, S_1^H, \cdots, S_d^H$ also satiesfy condition (ii) in Definition 3.5. This completes the proof. ∎

In fact, this partition is the one in [25]. The polynomials in S_{d-i}^H are exactly the coefficients of $H_{\mathbf{x}}^i(p(\mathbf{x}+\mathbf{a})-q(\mathbf{x}))$ with respect to $\mathbf{x}$. In this reason, when we compute $\mathbb{V}_{\mathbb{F}}(S_{d-i}^H)$, we just solve the identical equation $H_{\mathbf{x}}^i(p(\mathbf{x}+\mathbf{a})) \equiv H_{\mathbf{x}}^i(q(\mathbf{x}))\, w.r.t.\mathbf{x}$, which is the reason why we call it $\mathbf{x}$-homogeneous partition. The **DOS** algorithm tells us if $\deg(p(\mathbf{x})) = \deg(q(\mathbf{x}))$ and reassume d is not $\deg_{\mathbf{x}}(p(\mathbf{x}+\mathbf{a})-q(\mathbf{x}))$ but $\deg(p(\mathbf{x}))$, then $p(\mathbf{x}+\mathbf{a}) = q(\mathbf{x})$ if and only if $H_{\mathbf{x}}^i(p(\mathbf{x}+\mathbf{a})) = H_{\mathbf{x}}^i(q(\mathbf{x}))$ for $0 \leq i \leq d$. The **DOS** algorithm also uses the identity

$$H_{\mathbf{x}}^i(p(\mathbf{x}+\mathbf{a})) = \sum_{j=i}^{d} \frac{1}{(j-i)!} \cdot \sum_{\mathbf{e}\in[n]^{j-i}} (\prod_{k=1}^{j-i} a^{e_k}) \frac{\partial^{j-i} H^j(p)}{\partial x_{e_1} \cdots \partial_{x_{e_{j-i}}}}(\mathbf{x}). \tag{3.2}$$

Hence, we can get S^H_{d-i} not by expanding $p(\mathbf{x}+\mathbf{a})-q(\mathbf{x})$, but only computing partial derivative dynamically. We may guess computing partial derivative dynamically is more efficient than expanding a polynomial in $2n$ variables. Note that partial derivatives commute, so there are some partial derivatives have the same result. The experiments tell us that if we avoid calculating these same results repeatedly, the derivation is much more efficient than expansion. That's why we use the **DOS** algorithm when we apply $\mathbf{x}$-homogeneous partition to practice. In addition, when we generate $p(\mathbf{x})$ and $q(\mathbf{x})$ at random, it is most likely that there is no $\mathbf{a}\in\mathbb{F}^n$ to satisfy $H^d_{\mathbf{x}}(p(\mathbf{x}+\mathbf{a}))=H^d_{\mathbf{x}}(q(\mathbf{x}))$. As a result, we hope to get this result directly but not after expanding. A simple claim is that if $p(\mathbf{x})\neq 0$ or $q(\mathbf{x})\neq 0$, then $H^d_{\mathbf{x}}(p(\mathbf{x}+\mathbf{a}))=H^d_{\mathbf{x}}(q(\mathbf{x}))$ with $\deg(p(\mathbf{x}))=\deg(q(\mathbf{x}))=d$ if and only if $\deg(p(\mathbf{x})-q(\mathbf{x}))<\deg(p(\mathbf{x}))$. Therefore, we would like to check

$$\deg(p(\mathbf{x})-q(\mathbf{x}))<\deg(p(\mathbf{x})) \tag{3.3}$$

before we start to separate. In fact, the equation (3.3) is not only efficient to verify, but also can detect the situation when $F_{p,q}=\varnothing$ quickly, so it can be applied to all of the algorithms we mentioned above for greater efficiency. In particular, it can be used when we apply $\mathbf{a}$-degree partition in practice. Now we can give the **DOS** algorithm as follows for convenience.

Algorithm 3.14 (Dvir, Oliveira and Shpilka's algorithm (**DOS**) [25]). *INPUT: two multivariate polynomials* $p,q\in\mathbb{F}[\mathbf{x}]$*;*
OUTPUT: $F_{p,q}$*;*

If $p(\mathbf{x})=q(\mathbf{x})=0$, **return** $\mathbb{F}^n$.
let $d=\deg_{\mathbf{x}}(p)$. *If* $\deg(p(\mathbf{x})-q(\mathbf{x}))\geq d$, **return** $\{\}$.
let $H^0(p),H^1(p),\ldots,H^{d-1}(p)$ *and* $H^0(q),H^1(q),\ldots,H^{d-1}(q)$ *be the homogeneous components of* p *and* q*, respectively.*
set $L=\{\}$ *and* $\mathbf{s}=\mathbf{0}$.
for $\ell=0,\ldots,d-1$ **do**
  set $S_\ell:=\text{Coefficients}(H^{d-\ell-1}_{\mathbf{x}}(p(\mathbf{x}+\mathbf{a}))-H^{d-\ell-1}(q(\mathbf{x})),\mathbf{x})\subset\mathbb{F}[\mathbf{a}]$.
  update $L=L_{\mathbf{a}=\mathbf{s}}\left(\cup_{i=0}^{\ell}S_i\right)$.
  if this linear system has no solution, **return** $\{\}$.
  else there is a special solution $\mathbf{s}'\in\mathbb{F}^n$*, then update* $\mathbf{s}=\mathbf{s}'$.
return *solutions of the linear system defined by* L.

Another inspiration of the **DOS** algorithm is that we can try to get $\mathbf{a}$-degree partition by partial derivatives instead of expanding coefficients. For a polynomial $f(\mathbf{x})\in\mathbb{F}[\mathbf{x}]$, we call a monomial $\mathbf{x}^{\boldsymbol{\alpha}}\in\text{Supp}(f(\mathbf{x}))$ a root monomial of $f(\mathbf{x})$, if $\mathbf{x}^{\boldsymbol{\alpha}}$ can not divide any monomial in $\text{Supp}(f(\mathbf{x}))$ except itself. For any term $c_{\boldsymbol{\alpha}}\mathbf{x}^{\boldsymbol{\alpha}}$, let

$$T_1:=\{|\boldsymbol{\beta}-\boldsymbol{\alpha}|\mid \mathbf{x}^{\boldsymbol{\beta}}\text{ is the root monomial of }f(\mathbf{x}),\boldsymbol{\alpha}\leq\boldsymbol{\beta}\},$$

$$T_2:=\{|\boldsymbol{\beta}-\boldsymbol{\alpha}|\mid \mathbf{x}^{\boldsymbol{\beta}}\in\text{Supp}(f(\mathbf{x})),\boldsymbol{\alpha}\leq\boldsymbol{\beta}\},$$

then we can define the level of $\mathbf{x}^{\boldsymbol{\alpha}}$ in $f(\mathbf{x})$ as

$$\begin{cases}\max(T_1), & T_1\neq\varnothing\\ 0, & T_1=\varnothing\end{cases}.$$

Note that it is easy to check that

$$\begin{cases}\max(T_1), & T_1\neq\varnothing\\ 0, & T_1=\varnothing\end{cases}=\begin{cases}\max(T_2), & T_2\neq\varnothing\\ 0, & T_2=\varnothing\end{cases}.$$

So we may use the set T_2 to calculate the level as well. As a result, for a subset $\mathbf{y}$ of $\mathbf{x} = \{x_1, x_2, \cdots, x_n\}$, we can define the level decomposition of a polynomial $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}] = \mathbb{F}[\hat{\mathbf{y}}][\mathbf{y}]$ as

$$f(\mathbf{x}) = L^0_{\mathbf{y}}(f)(\mathbf{x}) + L^1_{\mathbf{y}}(f)(\mathbf{x}) + \cdots + L^d_{\mathbf{y}}(f)(\mathbf{x}),$$

where $d = \deg_{\mathbf{y}}(f(\mathbf{x}))$ and $L^i_{\mathbf{y}}(f)$ denotes the sum of monomials with level i in $f(\mathbf{x})$ with respect to $\mathbf{y}$. For the sake of simplicity, we also write $L^i_{\mathbf{x}}(f)$ as $L^i(f)$. To be more understandable, we give an example below.

Example 3.15. *Let $\mathbb{F} = \mathbb{Q}$, $f(x, y) = 3x^5y^3 + 5x^3 + 9xy + 2xy^4 \in \mathbb{Q}[x, y]$.*

It is easy to check that the root monomials of $f(x, y)$ are x^5y^3 and xy^4, whose levels are 0. Then we can calculate the levels of the rest monomials in $f(x, y)$. The monomial x^3 only divides the root monomial x^5y^3, so its level is $(5 + 3) - 3 = 5$. The monomial xy divides both of the root monomials of $f(x, y)$, so its level is $\max\{(5 + 3) - 2, (1 + 4) - 2\} = 6$. Finally, we can get the level decomposition of $f(x, y)$ is that $f(x, y) = L^0(f) + L^5(f) + L^6(f)$, where $L^0(f) = 3x^5y^3 + 2xy^4$, $L^5(f) = 5x^3$ and $L^6(f) = 9xy$.

Note that $\mathrm{Supp}(L^0(f))$ is the set consisting of all root monomials of $f(\mathbf{x})$ and $\deg(L^i(f)) \leq \deg(f) - i$. Then we have the following lemma.

Lemma 3.16. *For a monomial $\mathbf{x}^{\boldsymbol{\alpha}} \in \mathrm{Supp}_{\mathbf{x}}(p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x}))$ with its coefficient $c_{\boldsymbol{\alpha}}(\mathbf{a})$, $\deg(c_{\boldsymbol{\alpha}}(\mathbf{a}))$ is equal to the level of $\mathbf{x}^{\boldsymbol{\alpha}}$ in $p(\mathbf{x})$.*

Proof. Assume $\deg(c_{\boldsymbol{\alpha}}(\mathbf{a})) = d$ and the level of $\mathbf{x}^{\boldsymbol{\alpha}}$ in $p(\mathbf{x})$ is ℓ. Let $T_2 := \{|\boldsymbol{\beta} - \boldsymbol{\alpha}| \mid \mathbf{x}^{\boldsymbol{\beta}} \in \mathrm{Supp}(p(\mathbf{x})), \boldsymbol{\alpha} \leq \boldsymbol{\beta}\}$.

When $d \geq 1$, we have some $\mathbf{a}^{\boldsymbol{\beta}} \in \mathrm{Supp}(c_{\boldsymbol{\alpha}}(\mathbf{a}))$ with $|\boldsymbol{\beta}| = d > 0$. Therefore, by Fact 3.7 (i), we have $\mathbf{x}^{\boldsymbol{\alpha}+\boldsymbol{\beta}} \in \mathrm{Supp}(p(\mathbf{x}))$, which means $d = |\boldsymbol{\beta}| = |(\boldsymbol{\alpha} + \boldsymbol{\beta}) - \boldsymbol{\alpha}| \leq \ell$. So we get $\ell \geq 1$ and $T_2 \neq \varnothing$. In the other hand, according to the definition of level, we have $\mathbf{x}^{\boldsymbol{\gamma}} \in \mathrm{Supp}(p(\mathbf{x}))$ with $|\boldsymbol{\gamma} - \boldsymbol{\alpha}| = l$ and $\boldsymbol{\gamma} > \boldsymbol{\alpha}$. So we can assume $\boldsymbol{\gamma} = \boldsymbol{\alpha} + \boldsymbol{\beta}$, then $\boldsymbol{\beta} > \mathbf{0}$ and $|\boldsymbol{\beta}| = \ell$. By Fact 3.7 (ii), we have $\mathbf{a}^{\boldsymbol{\beta}}\mathbf{x}^{\boldsymbol{\alpha}} \in \mathrm{Supp}_{\mathbf{x}}(p(\mathbf{x} + \mathbf{a}) - q(\mathbf{x}))$, which means $\ell = |\boldsymbol{\beta}| \leq d$. So we get $d = \ell$.

When $d = 0$, we can suppose $T_2 \neq \varnothing$. Then we just need to show that $\ell \leq d$. Else, we suppose $\ell > d = 0$, then just similar to the proof above, we will get $\ell \leq d$. Therefore, we have $0 \leq \ell \leq d$, which completes our proof. ∎

Hence, to calculate S^D_i, we just find all terms in $p(\mathbf{x} + \mathbf{a}) - q(\mathbf{x})$ whose level are i in $p(\mathbf{x})$. Let $L_i := \{\mathbf{x}^{\boldsymbol{\alpha}} \in \mathrm{Supp}_{\mathbf{x}}(p(\mathbf{x} + \mathbf{a}) - q(\mathbf{x})) \mid \text{the level of } \mathbf{x}^{\boldsymbol{\alpha}} \text{ in } p(\mathbf{x}) \text{ is } i\}$. Assume $\deg(p(\mathbf{x})) = d$. Notice that

$$p(\mathbf{x} + \mathbf{a}) - q(\mathbf{x}) = \sum_{i=0}^{d} L^i(p)(\mathbf{x} + \mathbf{a}) - q(\mathbf{x}),$$

and for any $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$, we have

$$f(\mathbf{x} + \mathbf{a}) = \sum_{i=0}^{d'} \sum_{i_1+\cdots+i_n=i} \frac{a_1^{i_1} \cdots a_n^{i_n}}{i!} \frac{\partial f}{\partial x_1^{i_1} \cdots x_n^{i_n}}, \forall d' \geq \deg(f(\mathbf{x})).$$

Therefore, we have

$$p(\mathbf{x} + \mathbf{a}) - q(\mathbf{x}) = \sum_{i=0}^{d} \sum_{j=0}^{d-i} \sum_{j_1+\cdots+j_n=j} \frac{a_1^{j_1} \cdots a_n^{j_n}}{j!} \frac{\partial L^i(p)}{\partial x_1^{j_1} \cdots x_n^{j_n}} - q(\mathbf{x}).$$

Let

$$p_k(\mathbf{x},\mathbf{a}) = \begin{cases} \sum_{i=0}^{k} \sum_{i_1+\cdots+i_n=i} \frac{a_1^{i_1}\cdots a_n^{i_n}}{i!} \frac{\partial L^{k-i}(p)}{\partial x_1^{i_1}\cdots x_n^{i_n}}, & 1 \le k \le d \\ L^0(p)(\mathbf{x}) - q(\mathbf{x}), & k = 0 \end{cases}.$$

Then by simple check we know $p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x}) = \sum_{k=0}^{d} p_k(\mathbf{x},\mathbf{a})$. Now we can give the following lemma to narrow our search for the terms in L_i.

Lemma 3.17. *Let $\mathbf{x}^{\boldsymbol{\alpha}} \in \mathrm{Supp}(p)$, assume its level in $p(\mathbf{x})$ is i. For $\boldsymbol{\beta} < \boldsymbol{\alpha}$, suppose $|\boldsymbol{\alpha} - \boldsymbol{\beta}| = j$, then the level of $\mathbf{x}^{\boldsymbol{\beta}}$ in $p(\mathbf{x})$ is $i + j$ at least. Therefore, $\mathrm{Supp}_{\mathbf{x}}(p_k(\mathbf{x},\mathbf{a})) \subset \cup_{i=k}^{d} L_i$.*

Proof. Let $T_2 := \{|\boldsymbol{\beta} - \boldsymbol{\alpha}| \mid \mathbf{x}^{\boldsymbol{\beta}} \in \mathrm{Supp}(p(\mathbf{x})), \boldsymbol{\alpha} \le \boldsymbol{\beta}\}$. It is clear that $T_2 \ne \varnothing$. So there is a monomial $\mathbf{x}^{\boldsymbol{\gamma}} \in \mathrm{Supp}(p)$ such that $|\boldsymbol{\gamma} - \boldsymbol{\alpha}| = i$ and $\boldsymbol{\gamma} \ge \boldsymbol{\alpha}$. Hence, we have $\boldsymbol{\gamma} > \boldsymbol{\beta}$ and $|\boldsymbol{\gamma} - \boldsymbol{\beta}| = i + j \in T_2$. So the level of $\mathbf{x}^{\boldsymbol{\beta}}$ in $p(\mathbf{x})$ is $i + j$ at least. What's more, we can get that for any monomial in $\frac{a_1^{i_1}\cdots a_n^{i_n}}{i!} \frac{\partial L^{k-i}(p)}{\partial x_1^{i_1}\cdots x_n^{i_n}}$, its level in $p(\mathbf{x})$ is $(k - i) + i = k$ at least. So we get $\mathrm{Supp}_{\mathbf{x}}(p_k(\mathbf{x},\mathbf{a})) \subset \cup_{i=k}^{d} L_i$. ∎

As a result, we get the following two algorithms to apply **a**-degree partition in practice. The former one gets the partition by partial derivative while the latter one by expansion. The experiments shown later will tell us that the one by expansion is more efficient obviously.

Algorithm 3.18 (**a**-degree partition by partial derivative (**ADPD**)).
INPUT: two multivariate polynomials $p, q \in \mathbb{F}[\mathbf{x}]$;
OUTPUT: $F_{p,q}$;

If $p(\mathbf{x}) = q(\mathbf{x}) = 0$, **return** $\mathbb{F}^n$.
let $d = \deg_{\mathbf{x}}(p)$. If $\deg(p(\mathbf{x}) - q(\mathbf{x})) \ge d$, **return** $\{\}$.
Calculate $L^0(p), L^1(p), \ldots, L^d(p)$, where $L^i(p)$ is the sum of monomials with level i in p.
set $L = \{\}$, $\mathbf{s} = \mathbf{0}$ and $r_\ell = 0$, $\ell = 0, 1, \cdots, d$.
for $\ell = 0, \ldots, d$ **do**
    set

$$p_\ell(\mathbf{x},\mathbf{a}) = \begin{cases} \sum_{i=0}^{\ell} \sum_{i_1+\cdots+i_n=i} \frac{a_1^{i_1}\cdots a_n^{i_n}}{i!} \frac{\partial L^{\ell-i}(p)}{\partial x_1^{i_1}\cdots x_n^{i_n}}, & 1 \le \ell \le d \\ L^0(p)(\mathbf{x}) - q(\mathbf{x}), & \ell = 0 \end{cases} \in \mathbb{F}[\mathbf{a}][\mathbf{x}].$$

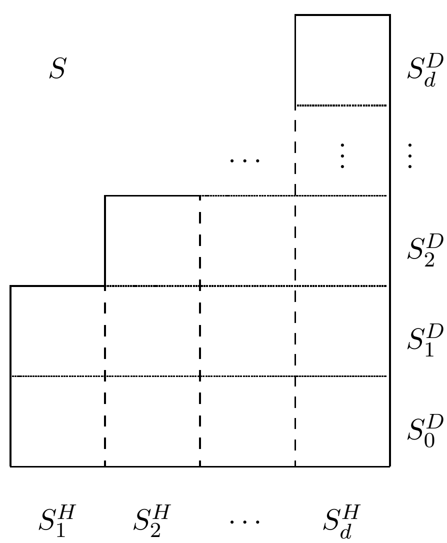
    for *term* **in** $p_\ell + r_\ell$ **do**
        calculate the level of term in $p(\mathbf{x})$.
        if level is ℓ, let $c(\mathbf{a}) := \mathrm{Coefficients}(term, \mathbf{x}) \subset \mathbb{F}[\mathbf{a}]$ and update $L = L \cup \{L_{\mathbf{a}=\mathbf{s}}(c(\mathbf{a}))\}$.
        else update $r_{level} = r_{level} + term$.
    if L has no solution, **return** $\{\}$.
    else there is a special solution $\mathbf{s}' \in \mathbb{F}^n$, then update $\mathbf{s} = \mathbf{s}'$.
return *solutions of the linear system defined by L.*

Algorithm 3.19 (**a**-degree partition by expansion (**ADPE**)).
INPUT: two multivariate polynomials $p, q \in \mathbb{F}[\mathbf{x}]$;
OUTPUT: $F_{p,q}$;

If $p(\mathbf{x}) = q(\mathbf{x}) = 0$, **return** $\mathbb{F}^n$.
let $d = \deg_{\mathbf{x}}(p)$. If $\deg(p(\mathbf{x}) - q(\mathbf{x})) \ge \deg(p(\mathbf{x}))$, **return** $\{\}$.
$S := \mathrm{Coefficients}(p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x}), \mathbf{x}) \subset \mathbb{F}[\mathbf{a}]$.

separate elements in S according to their total degree with respect to $\mathbf{a}$ and set $S_i = \{c \in S \mid \deg(c) = i\}$ for $0 \le i \le d$.
set $L = \{\}$ and $\mathbf{s} = \mathbf{0}$.
for $\ell = 0, \ldots, d$ **do**
  update $L = L_{\mathbf{a}=\mathbf{s}}\left(\cup_{i=0}^{\ell} S_i\right)$.
  solve the linear system in $\mathbf{a}$ defined by L.
  If this linear system has no solution, **return** $\{\}$.
  else there is a special solution $\mathbf{s}' \in \mathbb{F}^n$, then update $\mathbf{s} = \mathbf{s}'$.
return *solutions of the linear system defined by L.*

After introducing two concrete methods to separate, we would like to compare them and explain their connection. Because we would check the equation (3.3) in advance, we will always assume $H_{\mathbf{x}}^d(p(\mathbf{x}+\mathbf{a})) = H_{\mathbf{x}}^d(q(\mathbf{x}))$ with $\deg(p(\mathbf{x})) = \deg(q(\mathbf{x})) = d$ in our following discussion. By the equation (3.2), we know $\deg_{\mathbf{a}}(H_{\mathbf{x}}^{d-1}(p(\mathbf{x}+\mathbf{a}))) = 1$, so we get $\deg_{\mathbf{x}}(p(\mathbf{x}+\mathbf{a}) - q(\mathbf{x})) = d-1$. In addition, by Lemma 3.12, we know that $S_\ell^H \subset \cup_{i=0}^{\ell+1} S_i^D$. Hence, the connection between two different partition methods is like the following figure.



Now we give some examples to show our different partition methods and algorithms.

Example 3.20. *Let $\mathbb{F} = \mathbb{Q}$, $p_i(x,y,z), q_i(x,y,z) \in \mathbb{Q}[x,y,z]$, $i = 1,2$ with $p_1(x,y,z) = x^4+x^2y+y^2$, $q_1(x,y,z) = p_2(x,y+1,z+2)+z$, $p_2(x,y,z) = x^4+x^3y+xy^2+z^2$ and $q_2(x,y,z) = p_2(x,y+1,z+2)+xy$.*

1. *Compute F_{p_1,q_1}. We expand $p_1(x+a,y+b,z+c) - q_1(x,y,z)$ and get that*

$$\begin{aligned}&p_1(x+a,y+b,z+c) - q_1(x,y,z)\\ =&(4a\cdot x^3) + ((6a^2+b-1)\cdot x^2 + 2a\cdot xy)\\ &+((4a^3+2ab)\cdot x + (a^2+2b-2)\cdot y - z) + (a^4+a^2b+b^2-1)\end{aligned}$$

Then we can separate the coefficients of $p_1(x+a,y+b,z+c) - q_1(x,y,z)$ with respect to x, y and z in two different methods as following.

S	S_1^H	S_2^H	S_3^H	S_4^H
S_4^D				$a^4+a^2b+b^2-1$
S_3^D			$4a^3+2ab$	
S_2^D		$6a^2+b-1$	a^2+2b-2	
S_1^D	$4a$	$2a$		
S_0^D			-1	

So we can get $F_{p_1,q_1}=\varnothing$ at once if we use **a***-degree partition, while by* **x***-homogeneous partition, we will calculate until we get S_2^H.*

2. *Compute F_{p_2,q_2}. We expand $p_2(x+a,y+b,z+c)-q_2(x,y,z)$ and get that*

$$
\begin{aligned}
&p_2(x+a,y+b,z+c)-q_2(x,y,z)\\
=&((4a+b-1)\cdot x^3+3a\cdot x^2y)\\
&+((6a^2+3ab)\cdot x^2+(3a^2+2b-3)\cdot xy+a\cdot y^2)\\
&+((4a^3+3a^2b+b^2-1)\cdot x+(a^3+2ab)\cdot y+(2c-4)\cdot z)\\
&+(a^4+a^3b+ab^2+c^2-4)
\end{aligned}
$$

Then we can separate the coefficients of $p_2(x+a,y+b,z+c)-q_2(x,y,z)$ with respect to x, y and z in two different methods as following.

S	S_1^H	S_2^H	S_3^H	S_4^H
S_4^D				$a^4+a^3b+ab^2+c^2-4$
S_3^D			$4a^3+3a^2b+b^2-1$ a^3+2ab	
S_2^D		$6a^2+3ab$ $3a^2+2b-3$		
S_1^D	$4a+b-1$ $3a$	a	$2c-4$	
S_0^D				

So we can get $F_{p_2,q_2}=\varnothing$ if we use **x***-homogeneous partition and calculate S_1^H, while by* **a***-degree partition, we have to solve $2c-4=0$ needlessly.*

3.3 Implementations and timings

We have implemented the **G** algorithm, **KS** algorithm, as well as Algorithm 3.14, Algorithm 3.18 and Algorithm 3.19 in Maple 2020 with $\mathbb{F} = \mathbb{Q}$. The test suite was generated as follow.

Let $n, d, t, d' \in \mathbb{N}$ and $d' < d$. We first generated randomly a polynomial $p(x_1, x_2, \cdots, x_n)$ with degree d and t terms, as well as a polynomial $dis(x_1, x_2, \cdots, x_n)$ with degree d'. Then we generated randomly a vector $\mathbf{a} = (a_1, a_2, \cdots, a_n) \in \mathbb{Z}^n$ and let $q(x_1, x_2, \cdots, x_n) = p(x_1 + a_1, x_2 + a_2, \cdots, x_n + a_n) + dis(x_1, x_2, \cdots, x_n)$. By setting $0 \leq a_i \leq 99$, the calculation will terminate after we computed $\mathbb{V}_{\mathbb{F}}(\cup_{i=0}^{d-d'} S_i^H)$ with large probability.

Note that, in all the tests, the algorithms take the expanded forms of examples given above as input. All timings are measured in seconds on a Windows 11 home computer with 128GB RAM and 3.7GHz Intel(R) core(TM) i9-10900K processors.

For a selection of random polynomials and vectors for different choices of n, t, d, d' as above, we first tabulate the timings of the **G** algorithm, the **KS** algorithm and the **DOS** algorithm. Note that $d' = -\infty$ means we let $dis = 0$ then p and q are shift equivalent.

n	t	d	d'	**G**	**KS**	**DOS**
3	10	10	8	< 0.001	0.125	0.016
3	10	10	5	0.454	0.203	< 0.001
3	10	10	0	4.641	0.250	0.015
3	10	10	$-\infty$	5.813	0.531	0.016
3	40	10	8	0.078	0.359	0.016
3	40	10	5	0.485	0.468	< 0.001
3	40	10	0	7.672	0.828	0.016
3	40	10	$-\infty$	6.469	1.203	0.015
3	10	15	13	0.610	1.843	< 0.001
3	10	15	10	0.156	1.500	0.016
3	10	15	5	3.422	1.015	0.016
3	10	15	0	246.141	2.422	0.016
3	10	15	$-\infty$	418.343	3.329	0.015
3	10	20	18	0.781	10.266	0.016
3	10	20	15	1.484	4.219	< 0.001
3	10	20	10	6.500	8.391	0.015
3	10	20	5	3304.860	19.297	0.015
3	10	20	$-\infty$	13948.313	11.437	0.047

The experimental results illustrate that the **DOS** algorithm indeed outperforms the other two algorithms. Now we tabulate the timings of the **DOS** algorithm, the algorithm using **a**-degree partition by expansion (**ADPE**) and the algorithm using **a**-degree partition by partial derivative (**ADPD**).

n	t	d	d'	**DOS**	**ADPE**	**ADPD**
5	10	30	28	0.016	< 0.001	< 0.001
5	10	30	25	8.859	0.156	1.047
5	10	30	20	7.969	0.109	0.797
5	10	30	15	8.360	0.203	11.375
5	10	30	10	1.032	0.578	22.843
5	10	30	5	9.125	0.938	53.359
5	10	30	0	8.594	0.578	16.110
5	10	30	$-\infty$	0.297	0.281	1.329
5	30	30	28	11.609	0.234	10.235
5	30	30	25	8.281	0.266	9.218
5	30	30	20	0.797	6.735	1.968
5	30	30	15	8.203	6.422	1.766
5	30	30	10	33.640	1.563	204.890
5	30	30	5	25.532	8.406	161.515
5	30	30	0	25.172	8.500	163.797
5	30	30	$-\infty$	16.172	2.922	95.703
5	90	30	28	24.187	6.797	27.610
5	90	30	25	20.688	7.000	19.140
5	90	30	20	28.562	12.563	19.687
5	90	30	15	55.141	9.281	635.172
5	90	30	10	51.125	11.063	721.812
5	90	30	5	88.125	9.750	807.453
5	90	30	0	79.250	9.875	763.485
5	90	30	$-\infty$	27.125	7.125	430.672

The experimental results illustrate that the **ADPE** algorithm indeed outperforms the other two algorithms in most cases. It can be that **a**-degree partition solves all linear equations at first and it's most likely that there is only a vector satisfying these linear equations. Then for the rest equations it is easy to check whether $F_{p,q}$ is empty or not.

4 Isotropy groups and orbital decompositions

In this section, we first recall the notion of isotropy groups under shifts, which plays a central role in the summability criteria and existence criteria of telescopers. Then we present different types of partial fraction decomposition of $\mathbb{F}(\mathbf{x})$ with respect to different orbital factorizations as in [17]. These decompositions can be computed via algorithms for the SET problem over integers and will be used in the next sections for simplifying the rational summability problem and the existence problem of telescopers.

4.1 Isotropy groups

Let $G = \langle \sigma_{x_1}, \ldots, \sigma_{x_n} \rangle$ be the free abelian group generated by shift operators $\sigma_{x_1}, \ldots, \sigma_{x_n}$ and A be a subgroup of G. Let p be a multivariate polynomial in $\mathbb{F}[\mathbf{x}]$. The set

$$[p]_A := \{\sigma(p) \mid \sigma \in A\}$$

is called the A-*orbit* of p. Two polynomials $p, q \in \mathbb{F}[\mathbf{x}]$ are said to be A-*shift equivalent* or A-*equivalent* if $[p]_A = [q]_A$, denoted by $p \sim_A q$. The relation $\sim_A$ is an equivalence relation.

Definition 4.1 (Sato's Isotropy Group [51])**.** *Let A and p be defined as above. The set*

$$A_p := \{\sigma \in A \mid \sigma(p) = p\}.$$

is a subgroup of A, called the isotropy *group of p in A.*

If two polynomials p, q in $\mathbb{F}[\mathbf{x}]$ are A-shift equivalent, then $A_p = A_q$. The following remark says that we can test the A-equivalence of polynomials and compute a basis of A_p by algorithms for the SET problem over integers in Section 3.

Remark 4.2. *(1) Two polynomials $p, q \in \mathbb{F}[\mathbf{x}]$ are G-equivalent if and only if there exists $\sigma \in G$ such that $\sigma(p) = q$. Therefore, the G-equivalence relation of p, q can be obtained via the computation of $Z_{p,q}$ in Section 3. When $p = q$, the group G_p is isomorphic to $Z_{p,p}$. Both of them are free abelian groups and a basis G_p can be given by a basis of $Z_{p,p}$.*

(2) When $A = \langle \sigma_{x_1}, \ldots, \sigma_{x_r} \rangle$ with $1 \leq r \leq n$, we can view p, q as polynomials in $x_1, \ldots, x_r$ and the other variables are parameters. Then the A-equivalence relation of p, q and a basis of the isotropy A_p are also available by algorithms in Section 3.

(3) In general, let $A = \langle \tau_1, \ldots, \tau_r \rangle$, where $\{\tau_1, \ldots, \tau_r\}(1 \leq r \leq n)$ are $\mathbb{Z}$-linearly independent. We can use Proposition 5.11 to construct a difference isomorphism between $(\mathbb{F}(\mathbf{x}), \tau_i)$ and $(\mathbb{F}(\mathbf{x}), \sigma_{x_i})$ such that $\phi \circ \tau_i = \sigma_{x_i} \circ \phi$ for $1 \leq i \leq r$. Write $B = \langle \sigma_{x_1}, \ldots, \sigma_{x_r} \rangle$, then p and q are A-equivalent if and only if $\phi(p)$ is B-equivalent to $\phi(q)$. Furthermore, we have $\tau_1^{a_1} \cdots \tau_r^{a_r} \in A_p$ if and only if $\sigma_{x_1}^{a_r} \cdots \sigma_{x_r}^{a_r} \in B_{\phi(p)}$ for any $a_1, \ldots, a_r \in \mathbb{Z}$.

A structure property of the quotient group G/G_p is given by Sato [51, Lemma A-3] as follows.

Lemma 4.3. *G/G_p is a free abelian group.*

If $p \in \mathbb{F}[\mathbf{x}] \setminus \mathbb{F}$ is a non-constant polynomial, then G_p is a proper subgroup of G. By Lemma 4.3, we have $\operatorname{rank}(G_p) < \operatorname{rank}(G)$, where $\operatorname{rank}(G)$ denotes the rank of the free abelian group G. This property about the rank of isotropy groups plays a key rule in the reduction method of solving rational summability problem and the existence problem of telescopers.

If $n > 1$, let $H = \langle \sigma_{x_1}, \ldots, \sigma_{x_{n-1}} \rangle$ be the subgroup of G generated by $\sigma_{x_1}, \ldots, \sigma_{x_{n-1}}$. The isotropy group of p in H is $H_p = \{\tau \in H \mid \tau(p) = p\}$. By Lemma 4.3, both G/G_p and H/H_p are free abelian groups. So the rank of G_p and H_p are strictly less than that of G and H respectively if p has positive degree in x_1.

Lemma 4.4. *G_p/H_p is a free abelian group of $\operatorname{rank}(G_p/H_p) \leq 1$.*

Proof. Define a group homomorphism $\varphi : G_p/H_p \to \mathbb{Z}$ by

$$\sigma_{x_1}^{k_1} \ldots \sigma_{x_n}^{k_n} H_p \mapsto k_n.$$

It can be verified that φ is well-defined. For any $\tau_1, \tau_2 \in G_p$, if they are in the same coset of H_p in G_p, then $\tau_1 \tau_2^{-1} \in H_p$. This implies $\tau_1 \tau_2^{-1} \in H$ and hence $\varphi(\tau_1 H_p) = \varphi(\tau_2 H_p)$. Moreover, the converse is true since $G_p \cap H = H_p$. So φ is injective. Then we have $G_p/H_p \cong \operatorname{im} \varphi = k\mathbb{Z}$ for some integer $k \in \mathbb{Z}$. So G_p/H_p is a free abelian group generated by $\varphi^{-1}(k)$. ∎

Example 4.5. *Consider polynomials in $\mathbb{Q}[x, y, z]$. Let $G = \langle \sigma_x, \sigma_y, \sigma_z \rangle$ and $H = \langle \sigma_x, \sigma_y \rangle$.*

1. *For $p = x^2 + 2xy + z^2$, we have $G_p = H_p = \{\mathbf{1}\}$.*
2. *For $p = (x - 3y)^2(y + z) + 1$, we have $G_p = \langle \tau \rangle$ and $H_p = \{\mathbf{1}\}$, where $\tau = \sigma_x^3 \sigma_y \sigma_z^{-1}$. So $G_p/H_p = \langle \bar{\tau} \rangle$, where $\bar{\tau} = \tau H_p$ denotes the coset in G_p/H_p repesented by $\tau \in G_p$.*
3. *Let $p = x + 2y + z$, we have $G_p = \langle \tau_1, \tau_2 \rangle$ and $H_p = \langle \tau_2 \rangle$, where $\tau_1 = \sigma_x \sigma_y^{-1} \sigma_z$ and $\tau_2 = \sigma_x^2 \sigma_y^{-1}$. So $G_p/H_p = \langle \bar{\tau}_1 \rangle$.*

4.2 Orbital decompositions

A polynomial $p \in \mathbb{F}[\mathbf{x}]$ is said to be *monic* if the leading coefficient of p is 1 under a fix monomial order. Let $\hat{\mathbf{x}}_1$ denote the $m-1$ variables $x_2, \ldots, x_m$. For any subgroup A of $G = \langle \sigma_{x_1}, \ldots, \sigma_{x_n} \rangle$ and any polynomial Q in $\mathbb{F}(\hat{\mathbf{x}}_1)[x_1]$, one can classify all of monic irreducible factors in x_1 of Q into distinct A-orbits which leads to a factorization

$$Q = c \cdot \prod_{i=1}^{I} \prod_{j=1}^{J_i} \tau_{i,j}(d_i)^{e_{i,j}}, \tag{4.1}$$

where $c \in \mathbb{F}(\hat{\mathbf{x}}_1)$, $I, J_i, e_{i,j} \in \mathbb{N}$, $\tau_{i,j} \in A$, $d_i \in \mathbb{F}[\mathbf{x}]$ being monic irreducible polynomials in distinct A-orbits, and for each i, $\tau_{i,j}(d_i) \neq \tau_{i,j'}(d_i)$ if $1 \leq j \neq j' \leq J_i$. With respect to this fixed representation, we have the unique irreducible partial fraction decomposition for a rational function $f = P/Q \in \mathbb{F}(\mathbf{x})$ of the form

$$f = p + \sum_{i=1}^{I} \sum_{j=1}^{J_i} \sum_{\ell=1}^{e_{i,j}} \frac{a_{i,j,\ell}}{\tau_{i,j}(d_i)^{\ell}}, \tag{4.2}$$

where $p, a_{i,j,\ell} \in \mathbb{F}(\hat{\mathbf{x}}_1)[x_1]$ with $\deg_{x_1}(a_{i,j,\ell}) < \deg_{x_1}(d_i)$ for all i, j, ℓ. Note that the representation in (4.2) depends on the choice of representatives d_i in distinct A-orbits. However, the sum $\sum_{j=1}^{J_i} \frac{a_{i,j,\ell}}{\tau_{i,j}(d_i)^{\ell}}$ only depends on the multiplicity ℓ and the orbit $[d_i]_A$ instead of its representative d_i. Based on this fact, we shall formulate a unique decomposition of a rational function with respect to the group A. In this sense, we can decompose $\mathbb{F}(\mathbf{x})$ as a vector space over $\mathbb{E} = \mathbb{F}(\hat{\mathbf{x}}_1)$.

Given an irreducible polynomial $d \in \mathbb{F}[\mathbf{x}]$ with $\deg_{x_1}(d) > 0$ and $j \in \mathbb{N}^+$, we define a subspace of $\mathbb{F}(\mathbf{x})$

$$V_{[d]_A,j} = \operatorname{Span}_{\mathbb{E}} \left\{ \frac{a}{\tau(d)^j} \,\middle|\, a \in \mathbb{E}[x_1], \tau \in A, \deg_{x_1}(a) < \deg_{x_1}(d) \right\}. \tag{4.3}$$

For any fraction in $V_{[d]_A,j}$, the irreducible factors of its denominator are in the same A-orbit as d. Let $V_0 = \mathbb{E}[x_1]$ denote the set of all polynomials in x_1. By the irreducible partial fraction decomposition, any rational function $f \in \mathbb{F}(\mathbf{x})$ can be uniquely written in the form

$$f = f_0 + \sum_{j} \sum_{[d]_A} f_{[d]_A,j}, \tag{4.4}$$

where $f_0 \in V_0$ and $f_{[d]_A,j}$ are in distint $V_{[d]_A,j}$ spaces. Let T_A be the set of all distinct A-orbits of monic irreducible polynomials in $\mathbb{F}[\mathbf{x}]$, whose degrees with respect to x_1 are positive. Then $\mathbb{F}(\mathbf{x})$ has the following direct sum decomposition

$$\mathbb{F}(\mathbf{x}) = V_0 \bigoplus \left(\bigoplus_{j} \bigoplus_{[d]_A} V_{[d]_A,j} \right), \tag{4.5}$$

where j runs over all positive integer and $[d]_A$ runs over all elements in T_A.

Definition 4.6. *The decomposition* (4.5) *of* $\mathbb{F}(\mathbf{x})$ *is called the* orbital decomposition *of* $\mathbb{F}(\mathbf{x})$ *with respect to the variable* x_1 *and the group* A. *If* f *is written in the form* (4.4), *we call* f_0 *and* $f_{[d]_A,j}$ orbital components *of* f *with respect to* x_1 *and* A.

A key feature of subspaces $V_{[d]_A,j}$ is the A-invariant property. In the field of univariate rational functions, the orbital decomposition of $\mathbb{F}(x_1)$ with respect to the group $A = \langle \sigma_{x_1} \rangle$ was first given in [38] by Karr.

Lemma 4.7. *If $f \in V_{[d]_A,j}$ and $P \in \mathbb{F}(\hat{\mathbf{x}}_1)[A]$, then $P(f) \in V_{[d]_A,j}$.*

Proof. Let $f = \sum a_i/\tau_i(d)^j$ and $P = \sum p_\sigma \sigma$ with $p_\sigma \in \mathbb{F}(\hat{\mathbf{x}}_1)$ and $\sigma \in A$. For any $\sigma \in A$, we have $\sigma\tau_i$ is still in A, because A is a group. Since the shift operators do not change the degree and multiplicity of a polynomial, we have $\deg_{x_1}(\sigma(a_i)) < \deg_{x_1}(d)$ and then $\frac{p_\sigma \sigma(a_i)}{\sigma(\tau_i(d))^j}$ is in $V_{[d]_A,j}$. So $P(f) \in V_{[d]_A,j}$ by the linearity of the space. ∎

Example 4.8. *Let $\mathbb{F} = \mathbb{Q}$, $\mathbb{E} = \mathbb{Q}(y,z)$ and $G = \langle \sigma_x, \sigma_y, \sigma_z \rangle$. Consider the rational function f_1 in $\mathbb{Q}(x,y,z)$ of the form*

$$f_1 = \underbrace{\frac{x - z^2}{x^2 + 2xy + z^2}}_{d_1 := d_{1,1}} + \underbrace{\frac{x - y - 2z}{x^2 + 2xy + 2x + z^2}}_{d_{1,2}} + \underbrace{\frac{y + z^2}{x^2 + 2xy + 8x + 2y + z^2 - 2z + 8}}_{d_{1,3}}.$$

If $A = \langle \sigma_x \rangle$, then the orbital partial fraction decomposition of f_1 is

$$f_1 = f_{1,1} + f_{1,2} + f_{1,3} \text{ with } f_{1,1} = \frac{x - z^2}{d_{1,1}},\ f_{1,2} = \frac{x - y - 2z}{d_{1,2}} \text{ and } f_{1,3} = \frac{y + z^2}{d_{1,3}},$$

where $f_{1,i} \in V_{[d_{1,i}]_A,1}$ for $i = 1,2,3$ and $d_1, d_{1,2}, d_{1,3}$ are in distinct $\langle \sigma_x \rangle$-orbits. If $A = \langle \sigma_x, \sigma_y \rangle$, then the orbital partial fraction decomposition of f_1 is

$$f_1 = f_{1,1} + f_{1,2} \text{ with } f_{1,1} = \frac{x - z^2}{d_1} + \frac{x - y - 2z}{\sigma_y(d_1)} \text{ and } f_{1,2} = \frac{y + z^2}{d_{1,3}},$$

where $f_{1,1} \in V_{[d_1]_A,1}$, $f_{1,2} \in V_{[d_{1,3}]_A,1}$ and $d_1, d_{1,3}$ are in distinct $\langle \sigma_x, \sigma_y \rangle$-orbits. If $A = \langle \sigma_x, \sigma_y, \sigma_z \rangle$, then $f_1 \in V_{[d_1]_A,1}$ is one component in the orbital decomposition. Because

$$f_1 = \frac{x - z^2}{d_1} + \frac{x - y - 2z}{\sigma_y(d_1)} + \frac{y + z^2}{\sigma_x \sigma_y^3 \sigma_z^{-1}(d_1)}.$$

Example 4.9. *Let $\mathbb{F} = \mathbb{Q}$ and $G = \langle \sigma_x, \sigma_y, \sigma_z \rangle$. Consider the rational function $f = f_1 + f_2 + f_3$ in $\mathbb{Q}(x,y,z)$ with f_1 given in Example 4.8,*

$$f_2 = \underbrace{\frac{x + z}{(x - 3y)^2(y + z) + 1}}_{d_2} \text{ and } f_3 = \left(y + \frac{z}{y^2 + z - 1} - \frac{1}{y^2 + z} \right) \frac{1}{\underbrace{(x + 2y + z)}_{d_3}{}^2}.$$

If $A = G$, then the orbital partial fraction decomposition of f is

$$f = f_1 + f_2 + f_3 \quad \text{with} \quad f_i \in V_{[d_i]_G,1} \text{ for } i = 1,2 \text{ and } f_3 \in V_{[d_3]_G,2},$$

where d_1, d_2, d_3 are in distinct $\langle \sigma_x, \sigma_y, \sigma_z \rangle$-orbits.

5 Rational summability problem

In this section, we solve the rational summability problem for mulitivariate rational functions and design an algorithm for rational summability testing. In Section 5.1 we use a special orbital decomposition in Section 4.2 to reduce the summmability problem of a general rational function to its orbital components and then further to simple frations by Abramov's reduction. In Section 5.2, we use the structure of isotropy groups to reduce the number of variables in the summability problem inductively.

5.1 Orbital reduction for summability

Let f be a rational function in $\mathbb{F}(\mathbf{x})$, where $\mathbf{x} = \{x_1, \ldots, x_m\}$. Let n be an integer such that $1 \leq n \leq m$. We consider the $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summability problem of f in $\mathbb{F}(\mathbf{x})$. Let $G = \langle \sigma_{x_1}, \ldots, \sigma_{x_n} \rangle$. Taking $\mathbb{E} = \mathbb{F}(\hat{\mathbf{x}}_1)$ and $A = G$ in equality (4.3), we get the subspace $V_{[d]_G,j}$ of $\mathbb{F}(\mathbf{x})$

$$V_{[d]_G,j} = \operatorname{Span}_{\mathbb{E}} \left\{ \frac{a}{\tau(d)^j} \,\middle|\, a \in \mathbb{E}[x_1], \tau \in G, \deg_{x_1}(a) < \deg_{x_1}(d) \right\}. \tag{5.1}$$

According to Equation (4.4), f can be decomposed into the form

$$f = f_0 + \sum_j \sum_{[d]_G} f_{[d]_G,j}, \tag{5.2}$$

where $f_0 \in V_0 = \mathbb{E}[x_1]$ and $f_{[d]_G,j}$ are in distint $V_{[d]_G,j}$ spaces. The orbital decomposition (4.5) of $\mathbb{F}(\mathbf{x})$ with respect to the group G is as follows

$$\mathbb{F}(\mathbf{x}) = V_0 \bigoplus \left(\bigoplus_{j \in \mathbb{N}^+} \bigoplus_{[d]_G \in T_G} V_{[d]_G,j} \right). \tag{5.3}$$

Lemma 5.1. *Let $f \in \mathbb{F}(\mathbf{x})$. Then f is $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summable if and only if f_0 and each $f_{[d]_G,j}$ are $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summable for all $[d]_G \in T_G$ and $j \in \mathbb{N}^+$.*

Proof. The sufficiency is due to the linearity of difference operators Δ_{x_i}. For the necessity, suppose $f = \sum_{i=1}^n \Delta_{x_i}(g^{(i)})$ with $g^{(i)} \in \mathbb{F}(\mathbf{x})$. By the orbital decomposition of rational functions (5.2), we can write $f, g^{(i)}$ in the form

$$f = f_0 + \sum_j \sum_{[d]_G} f_{[d]_G,j} \quad \text{and} \quad g^{(i)} = g_0^{(i)} + \sum_j \sum_{[d]_G} g^{(i)}_{[d]_G,j} \quad \text{for } 1 \leq i \leq n.$$

By the linearity of Δ_{x_i}, we see

$$f = \sum_{i=1}^n \Delta_{x_i}\left(g_0^{(i)}\right) + \sum_j \sum_{[d]_G} \left(\sum_{i=1}^n \Delta_{x_i}\left(g^{(i)}_{[d]_G,j}\right) \right). \tag{5.4}$$

From Lemma 4.7, it is another expression of f with respect to $V_{[d]_G,j}$. Such a decomposition is unique, so $f_0 = \sum_{i=1}^n \Delta_{x_i}(g_0^{(i)})$ and $f_{[d]_G,j} = \sum_{i=1}^n \Delta_{x_i}(g^{(i)}_{[d]_G,j})$, which are $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summable. ∎

Using Lemma 5.1, we can reduce the summability problem of a rational function to its orbital components. Note that polynomials in x_1 are always (σ_{x_1})-summable. Thus Problem 2.4 can be reduced to that for rational functions in $V_{[d]_G,j}$, which are of the form

$$f = \sum_\tau \frac{a_\tau}{\tau(d)^j}, \tag{5.5}$$

where $\tau \in G$, $a_\tau \in \mathbb{F}(\hat{\mathbf{x}}_1)[x_1]$, $d \in \mathbb{F}[\mathbf{x}]$ with $\deg_{x_1}(a_\tau) < \deg_{x_1}(d)$ and d is irreducible in x_1 over $\mathbb{F}(\hat{\mathbf{x}}_1)$.

Let σ be an automorphism on $\mathbb{F}(\mathbf{x})$ and $a, b \in \mathbb{F}(\mathbf{x})$. Then for any integer $k \in \mathbb{Z}$, we have the reduction formula

$$\frac{a}{\sigma^k(b)} = \sigma(h) - h + \frac{\sigma^{-k}(a)}{b}, \tag{5.6}$$

where $h=0$ if $k=0$, $h=\sum_{i=0}^{k-1}\frac{\sigma^{i-k}(a)}{\sigma^i(b)}$ if $k>0$ and $h=-\sum_{i=0}^{-k-1}\frac{\sigma^i(a)}{\sigma^{i+k}(b)}$ if $k<0$. For any $\tau=\sigma_{x_1}^{k_1}\ldots\sigma_{x_n}^{k_n}\in G$, applying the reduction formula (5.6) with $\sigma=\sigma_{x_i}$ for $i=1,\ldots,n$, we get

$$\frac{a}{\sigma_{x_1}^{k_1}\cdots\sigma_{x_n}^{k_n}(b)}=\sum_{i=1}^{n}(\sigma_{x_i}(h_i)-h_i)+\frac{\sigma_{x_1}^{-k_1}\cdots\sigma_{x_n}^{-k_n}(a)}{b}, \tag{5.7}$$

where

$$h_i=\begin{cases} 0, & \text{if } k_i=0,\\ \displaystyle\sum_{\ell=0}^{k_i-1}\frac{\sigma_{x_i}^{\ell-k_i}\sigma_{x_{i-1}}^{-k_{i-1}}\cdots\sigma_{x_1}^{-k_1}(a)}{\sigma_{x_i}^{\ell}\sigma_{x_{i+1}}^{k_{i+1}}\cdots\sigma_{x_n}^{k_n}(b)}, & \text{if } k_i>0,\\ \displaystyle -\sum_{\ell=0}^{-k_i-1}\frac{\sigma_{x_i}^{\ell}\sigma_{x_{i-1}}^{-k_{i-1}}\cdots\sigma_{x_1}^{-k_1}(a)}{\sigma_{x_i}^{\ell+k_i}\sigma_{x_{i+1}}^{k_{i+1}}\cdots\sigma_{x_n}^{k_n}(b)}, & \text{if } k_i<0.\end{cases}$$

for $i=1,\ldots,n$. The equation (5.7) is called the $(\sigma_{x_1},\ldots,\sigma_{x_n})$-*reduction* formula. Rewriting every fraction of f in (5.5) by the reduction formula (5.7), we get the following lemma.

Lemma 5.2. *Let $f\in V_{[d]_G,j}$ be in the form (5.5). Then we can decompose it into the form*

$$f=\sum_{i=1}^{n}\Delta_{x_i}(g_i)+r \textit{ with } r=\frac{a}{d^j}, \tag{5.8}$$

where $g_i\in\mathbb{F}(\mathbf{x})$, $a=\sum_\tau \tau^{-1}(a_\tau)$ with $\deg_{x_1}(a)<\deg_{x_1}(d)$. In particular, f is $(\sigma_{x_1},\ldots,\sigma_{x_n})$-summable if and only if r is $(\sigma_{x_1},\ldots,\sigma_{x_n})$-summable.

Example 5.3. *Consider the rational function $f_1\in\mathbb{Q}(x,y,z)$ given in Example 4.8. Then $f_1\in V_{[d_1]_G,1}$ and it can be written as*

$$f_1=\frac{x-z^2}{d_1}+\frac{x-y-2z}{\sigma_y(d_1)}+\frac{y+z^2}{\sigma_x\sigma_y^3\sigma_z^{-1}(d_1)},$$

where $d_1=x^2+2xy+z^2$. By applying the $(\sigma_x,\sigma_y,\sigma_z)$-reduction formula, we have

$$f_1=\Delta_x(u_1)+\Delta_y(v_1)+\Delta_z(w_1)+r_1 \textit{ with } r_1=\frac{2x-1}{d_1}, \tag{5.9}$$

where

$$u_1=\frac{y+z^2}{\sigma_y^3\sigma_z^{-1}(d_1)},\ v_1=\frac{x-y+1-2z}{d_1}+\sum_{\ell=0}^{2}\frac{y+\ell-3+z^2}{\sigma_y^\ell\sigma_z^{-1}(d_1)},\ w_1=-\frac{y-3+z^2}{\sigma_z^{-1}(d_1)}.$$

Then f_1 is $(\sigma_x,\sigma_y,\sigma_z)$-summable if and only if r_1 is $(\sigma_x,\sigma_y,\sigma_z)$-summable.

The results in Lemmas 5.1 and 5.2 are summarized in Lemma 1.5.

5.2 Summability criteria

Combining Lemma 5.1 and Lemma 5.2, we reduce the rational summability problem to that for simple fractions

$$f=\frac{a}{d^j}, \tag{5.10}$$

where $j \in \mathbb{N} \setminus \{0\}$, $a \in \mathbb{F}(\hat{\mathbf{x}}_1)[x_1]$ and $d \in \mathbb{F}[\mathbf{x}]$ is irreducible with $\deg_{x_1}(a) < \deg_{x_1}(d)$. In this section, we shall present a criterion on the summability for such simple fractions.

For the univariate summability problem, we recall the following well known result in [2, 4, 10, 46, 48, 50]. Since the univariate case is the base of our induction method, we give a proof for the sake of completeness.

Lemma 5.4. *Let $f \in \mathbb{F}(\mathbf{x})$ be of the form (5.10). Then f is (σ_{x_1})-summable in $\mathbb{F}(\mathbf{x})$ if and only if $a = 0$.*

Proof. The sufficiency is trivial since $f = \Delta_{x_1}(0)$. To show the necessity, suppose f is (σ_{x_1})-summable but $a \neq 0$. Since $f = a/d^j \in V_{[d]_G,j}$, by the proof of Lemma 5.1 we can further assume $f = \Delta_{x_1}(g)$ for some $g \in V_{[d]_G,j}$. Write g in the form $g = \sum_{i=\ell_0}^{\ell_1} a_i/\sigma_{x_1}^i(d)^j$ with $a_{\ell_0}a_{\ell_1} \neq 0$. Then

$$f = \Delta_{x_1}(g) = \sum_{i=\ell_0}^{\ell_1+1} \frac{\tilde{a}_i}{\sigma_{x_1}^i(d)^j}, \tag{5.11}$$

where $\tilde{a}_i = \sigma_{x_1}(a_{i-1}) - a_i$ for $\ell_0 + 1 \leq i \leq \ell_1$, $\tilde{a}_{\ell_0} = -a_{\ell_0}$ and $\tilde{a}_{\ell_1+1} = \sigma_{x_1}(a_{\ell_1})$. Note that $\tilde{a}_{\ell_0}$ and $\tilde{a}_{\ell_1+1}$ are nonzero. For any integer $i \in \mathbb{Z}$, $\sigma_{x_1}^i(d)$ is still an irreducible polynomial. However, there is only one irreducible factor in the denominator of $f = a/d^j$. So we must have $\sigma_{x_1}^i(d) = d$ for some nonzero integer i. It implies that d is free of x_1. This is a contradiction because d has positive degree in x_1. ∎

For the multivariate summability problem with $n > 1$, let $G = \langle \sigma_{x_1}, \ldots, \sigma_{x_n} \rangle$ and $H = \langle \sigma_{x_1}, \ldots, \sigma_{x_{n-1}} \rangle$. The isotropy group of the polynomial d in G and H are denoted by G_d and H_d, respectively, i.e.,

$$G_d = \{\tau \in G \mid \tau(d)\} \quad \text{and} \quad H_d = \{\tau \in H \mid \tau(d) = d\}.$$

By Lemma 4.4, we know either $\operatorname{rank}(G_d/H_d) = 0$ or $\operatorname{rank}(G_d/H_d) = 1$.

When $\operatorname{rank}(G_d/H_d) = 0$, the summability problem in n variables can be reduced to that in $n-1$ variables.

Lemma 5.5. *Let $f = a/d^j \in \mathbb{F}(\mathbf{x})$ be of the form (5.10). If $n > 1$ and $\operatorname{rank}(G_d/H_d) = 0$, then f is $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summable in $\mathbb{F}(\mathbf{x})$ if and only if f is $(\sigma_{x_1}, \ldots, \sigma_{x_{n-1}})$-summable in $\mathbb{F}(\mathbf{x})$.*

Proof. The sufficiency is obvious by definition. For the necessity, suppose f is $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summable but not $(\sigma_{x_1}, \ldots, \sigma_{x_{n-1}})$-summable. By the orbital decomposition of f in (5.3) and Lemma 5.1, we get

$$f = \Delta_{x_1}(g_1) + \cdots + \Delta_{x_n}(g_n) \tag{5.12}$$

with $g_1, \ldots, g_n$ in the same subspace $V_{[d]_G,j}$ as f. As an analogue to (5.8) in $n-1$ variables $x_1, \ldots, x_{n-1}$, we can decompose g_n as

$$g_n = \sum_{i=1}^{n-1} \Delta_{x_i}(u_i) + \sum_{\ell=0}^{\rho} \frac{\lambda_\ell}{\sigma_{x_n}^\ell(\mu)^j}, \tag{5.13}$$

where $u_i \in \mathbb{F}(\mathbf{x})$, $\rho \in \mathbb{N}$, $\lambda_\ell \in \mathbb{F}(\hat{\mathbf{x}}_1)[x_1]$, $\mu \in \mathbb{F}[\mathbf{x}]$ with $\deg_{x_1}(\lambda_\ell) < \deg_{x_1}(d)$ and μ is in the same G-orbit as d.

Furthermore, we can assume $\lambda_0\lambda_\rho \neq 0$ and each nonzero $\lambda_\ell/\sigma_{x_n}^\ell(\mu)^j$ is not $(\sigma_{x_1},\ldots,\sigma_{x_{n-1}})$-summable. Substituting g_n in (5.13) into (5.12), we get

$$f + \sum_{\ell=0}^{\rho+1} \frac{\tilde{\lambda}_\ell}{\sigma_{x_n}^\ell(\mu)^j} = \sum_{i=1}^{n-1} \Delta_{x_i}(h_i), \tag{5.14}$$

where $\tilde{\lambda}_0 = \lambda_0$, $\tilde{\lambda}_{\rho+1} = -\sigma_{x_n}(\lambda_\rho)$, $\tilde{\lambda}_\ell = \lambda_\ell - \sigma_{x_n}(\lambda_{\ell-1})$ for all $1 \leq \ell \leq \rho$ and $h_i = g_i + \Delta_{x_n}(u_i)$ for all $1 \leq i \leq n-1$.

Since $\operatorname{rank}(G_d/H_d) = 0$ and $G_d = G_\mu$, it follows that all $\sigma_{x_n}^\ell(\mu)$ with $\ell \in \mathbb{Z}$ are in distinct H-orbits. In particular, $[\mu]_H, [\sigma_{x_n}(\mu)]_H \ldots, [\sigma_{x_n}^{\rho+1}(\mu)]_H$ are distinct H-orbits. On the other hand, the left hand side of (5.14) is $(\sigma_{x_1},\ldots,\sigma_{x_{n-1}})$-summable, but $\tilde{\lambda}_0/\mu^j$ is not $(\sigma_{x_1},\ldots,\sigma_{x_{n-1}})$-summable according to the assumption. By Lemma 5.1 (in $n-1$ variables), the only choice is that $\mu \sim_H d$. Similarly, $\sigma_{x_n}^{\rho+1}(\mu) \sim_H d$ and hence $\mu \sim_H \sigma_{x_n}^{\rho+1}(\mu)$. This leads to a contradiction since ρ is a nonnegative integer ∎

Lemma 5.6. *Let $f \in \mathbb{F}(\mathbf{x})$ and K be a subgroup of $G = \langle \sigma_{x_1},\ldots,\sigma_{x_n}\rangle$ with rank r $(1 \leq r \leq n)$. If $\{\sigma_i\}_{i=1}^r$ and $\{\tau_i\}_{i=1}^r$ are two bases of K, then f is $(\sigma_1,\ldots,\sigma_r)$-summable if and only if f is $(\tau_1,\ldots,\tau_r)$-summable.*

To prove the basis exchange property of summability problem in Lemma 5.6, we first show the following formula. It can be seen as an variant of the reduction formula (5.7). Since it is useful in computation, we give a strict proof by induction.

Formula 5.7. *Let $\sigma_1,\ldots,\sigma_r$ be elements in G and $\tau \in \langle \sigma_1,\ldots,\sigma_r\rangle$. Then*

$$\tau - \mathbf{1} = (\sigma_1 - \mathbf{1})\tilde{\sigma}_1 + \cdots + (\sigma_r - \mathbf{1})\tilde{\sigma}_r, \tag{5.15}$$

for some $\tilde{\sigma}_i \in \mathbb{F}[K]$ with K being the subgroup of G generated by $\sigma_1,\ldots,\sigma_r$.

Proof. We prove this formula by induction on the number of σ_i. If r=1, then $\tau = \sigma_1^{k_1}$ for some $k_1 \in \mathbb{Z}$. We have $\sigma_1^{k_1} - \mathbf{1} = (\sigma_1 - \mathbf{1})\mu$, where $\mu = 0$ if $k_1 = 0$, $\mu = \sum_{i=0}^{k_1-1}\sigma_1^i$ if $k_1 > 0$ and $\mu = -\sum_{i=0}^{-k_1-1}\sigma_1^{i+k_1}$ if $k_1 < 0$. If $r \geq 2$, assume that the conclusion holds for $r-1$. Write $\tau = \sigma_1^{k_1}\cdots\sigma_r^{k_r}$ for some $k_1,\ldots,k_r \in \mathbb{Z}$. Then

$$\tau - \mathbf{1} = \left(\sigma_1^{k_1} - \mathbf{1}\right)\sigma_2^{k_2}\cdots\sigma_r^{k_r} + \left(\sigma_2^{k_2}\cdots\sigma_r^{k_r} - \mathbf{1}\right).$$

If $\sigma_2^{k_2}\cdots\sigma_r^{k_r} = \mathbf{1}$, then we are done. Otherwise, by the inductive hypothesis, we get $\tau - \mathbf{1} = (\sigma_1 - \mathbf{1})\tilde{\sigma}_1 + \ldots + (\sigma_r - \mathbf{1})\tilde{\sigma}_r$ for some $\tilde{\sigma}_1,\ldots,\tilde{\sigma}_r \in \mathbb{F}[K]$. In fact, the above argument gives the following explicit expression

$$\tilde{\sigma}_i = \begin{cases} 0 & \text{if } k_i = 0, \\ \displaystyle\sum_{\ell=0}^{k_i-1} \sigma_i^\ell \sigma_{i+1}^{k_{i+1}}\cdots\sigma_r^{k_r} & \text{if } k_i > 0, \\ \displaystyle -\sum_{\ell=0}^{-k_i-1} \sigma_i^{\ell+k_i}\sigma_{i+1}^{k_{i+1}}\cdots\sigma_r^{k_r} & \text{if } k_i < 0, \end{cases}$$

for $i = 1,\ldots,r$. ∎

Proof of Lemma 5.6. Suppose f is $(\tau_1, \ldots, \tau_r)$-summable. This means

$$f = \Delta_{\tau_1}(h_1) + \cdots + \Delta_{\tau_r}(h_r), \tag{5.16}$$

for some $h_1, \ldots, h_r \in \mathbb{F}(\mathbf{x})$. For each $i = 1, \ldots, r$, since $\tau_i \in \langle \sigma_1, \ldots, \sigma_r \rangle$, it follows from Formula 5.7 that $\tau_i - \mathbf{1} = (\sigma_1 - \mathbf{1})\tilde{\sigma}_{i,1} + \ldots + (\sigma_r - \mathbf{1})\tilde{\sigma}_{i,r}$ for some $\tilde{\sigma}_{i,j} \in \mathbb{F}[K]$ with K being the subgroup generated by $\sigma_1, \ldots, \sigma_r$. Applying this operator to h_i yields that

$$\Delta_{\tau_i}(h_i) = \Delta_{\sigma_1}(h_{i,1}) + \cdots + \Delta_{\sigma_r}(h_{i,r}), \tag{5.17}$$

where $h_{i,j} = \tilde{\sigma}_{i,j}(h_i)$ for $j = 1, \ldots, r$. Combining Equations (5.16) and (5.17), we have

$$f = \sum_{i=1}^{r} \Delta_{\tau_i}(h_i) = \sum_{i=1}^{r}\sum_{j=1}^{r} \Delta_{\sigma_j}(h_{i,j}) = \sum_{j=1}^{r} \Delta_{\sigma_j}\left(\sum_{i=1}^{r} h_{i,j}\right), \tag{5.18}$$

where the last equality follows from the linearity of Δ_{σ_j}. Thus f is $(\sigma_1, \ldots, \sigma_r)$-summable. Similarly, the other direction is also true. ∎

Theorem 5.8 (Theorem 1.6, restated)**.** *Let $f = a/d^j \in \mathbb{F}(\mathbf{x})$ be of the form (5.10). Let $\{\tau_i\}_{i=1}^r (1 \leq r < n)$ be a basis of G_d (take $\tau_1 = \mathbf{1}$, if $G_d = \{\mathbf{1}\}$). Then f is $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summable if and only if*

$$a = \Delta_{\tau_1}(b_1) + \cdots + \Delta_{\tau_r}(b_r)$$

for some $b_i \in \mathbb{F}(\hat{\mathbf{x}}_1)[x_1]$ with $\deg_{x_1}(b_i) < \deg_{x_1}(d)$ for all $1 \leq i \leq r$.

Proof. The sufficiency follows from the fact that $f = \sum_{i=1}^r \Delta_{\tau_i}(b_i/d^j)$ and Formula 5.7. For the necessity, we proceed by induction on n. If $n = 1$, then G_d is a trivial group and the univariate case follows from Lemma 5.4. If $n > 1$, suppose the inductive hypothesis is true for $n - 1$ as follows.

If $\{\theta_i\}_{i=1}^s$ is a basis of H_d, then f is $(\sigma_{x_1}, \ldots, \sigma_{x_{n-1}})$-summable if and only if $a = \sum_{i=1}^s \Delta_{\theta_i}(b_i)$ for some $b_i \in \mathbb{F}(\hat{\mathbf{x}}_1)[x_1]$ with $\deg_{x_1}(b_i) < \deg_{x_1}(d)$ for all $1 \leq i \leq s$.

Now we proceed by a case distinction according to the rank of G_d/H_d. If $\operatorname{rank}(G_d/H_d) = 0$, then $H_d = G_d$. The conclusion follows from Lemma 5.5 and the inductive hypothesis. If $\operatorname{rank}(G_d/H_d) = 1$, by Lemma 5.6, we may assume $\{\tau_i\}_{i=1}^r$ is a basis of G_d such that $H_d = \langle \tau_1, \ldots, \tau_{r-1} \rangle$ and $G_d/H_d = \langle \bar{\tau}_r \rangle$. In here, $\bar{\tau}_r$ represents the element $\tau_r H_d$ with $\tau_r \in G_d$. Then we can choose $\tau_r = \sigma_{x_1}^{-k_1} \cdots \sigma_{x_{n-1}}^{-k_{n-1}} \sigma_{x_n}^{k_n}$ such that k_n is a positive integer. Otherwise, replace τ_r by τ_r^{-1}. Since $\bar{\tau}_r$ is a generator of G_d/H_d, we have k_n is the smallest positive integer such that $\sigma_{x_n}^{k_n}(d) \sim_H d$.

By the decomposition (4.5), we can assume $f = \Delta_{x_1}(g_1) + \cdots + \Delta_{x_n}(g_n)$ with $g_i \in V_{[d]_G, j}$. In here, g_n can be decomposed as

$$g_n = \sum_{i=1}^{n-1} \Delta_{x_i}(u_i) + \sum_{\ell=0}^{k_n-1} \frac{\lambda_\ell}{\sigma_{x_n}^{\ell}(d)^j},$$

where $u_i \in \mathbb{F}(\mathbf{x})$ and $\lambda_\ell \in \mathbb{F}(\hat{\mathbf{x}}_1)[x_1]$ with $\deg_{x_1}(\lambda_\ell) < \deg_{x_1}(d)$. Then we have

$$f - \Delta_{x_n}\left(\sum_{\ell=0}^{k_n-1} \frac{\lambda_\ell}{\sigma_{x_n}^{\ell}(d)^j}\right) = \sum_{i=1}^{n-1} \Delta_{x_i}(h_i), \tag{5.19}$$

where $h_i = g_i + \Delta_{x_n}(u_i)$. Note that $\sigma_{x_n}^{k_n}(d) = \sigma_{x_1}^{k_1} \ldots \sigma_{x_{n-1}}^{k_{n-1}}(d)$ and apply the reduction formula (5.7) to simplify (5.19). We get

$$\tilde{f} := \sum_{\ell=0}^{k_n-1} \frac{\tilde{\lambda}_\ell}{\sigma_{x_n}^{\ell}(d)^j} = \sum_{i=1}^{n-1} \Delta_{x_i}(\tilde{h}_i), \tag{5.20}$$

where $\tilde{h}_i \in \mathbb{F}(\mathbf{x})$, $\tilde{\lambda}_0 = a+\lambda_0-\sigma_{x_1}^{-k_1}\ldots\sigma_{x_{n-1}}^{-k_{n-1}}\sigma_{x_n}(\lambda_{k_n-1})$ and $\tilde{\lambda}_\ell = \lambda_\ell-\sigma_{x_n}(\lambda_{\ell-1})$ for $1 \leq \ell \leq k_n-1$.

Note that $[d]_H, [\sigma_{x_n}(d)]_H, \ldots, [\sigma_{x_n}^{k_n-1}(d)]_H$ are distinct H-orbits due to the minimality of k_n. From the equation (5.20), $\tilde{f}$ is $(\sigma_{x_1}, \ldots, \sigma_{x_{n-1}})$-summable. So by Lemma 5.1, each $\frac{\tilde{\lambda}_\ell}{\sigma_{x_n}^\ell(d)^j}$ is $(\sigma_{x_1}, \ldots, \sigma_{x_{n-1}})$-summable for $0 \leq \ell \leq k_n - 1$. Let W denote the vector subspace of $\mathbb{F}(\mathbf{x})$ over $\mathbb{F}$ consisting of all elements in the form of $\sum_{i=1}^{r-1} \Delta_{\tau_i}(b_i)$ with $b_i \in \mathbb{F}(\hat{\mathbf{x}}_1)[x_1]$ and $\deg_{x_1}(b_i) < \deg_{x_1}(d)$. (If $r = 1$, take $W = \{0\}$.) If two rational functions $g, h \in \mathbb{F}(\mathbf{x})$ satisfy the property that $g - h \in W$, we say g, h are congruent modulo W, denoted by $g \equiv h \pmod{W}$. Since $H_d = H_{\sigma_{x_n}^\ell(d)}$, we apply the inductive hypothesis to conclude that

$$\begin{cases} 0 \equiv a + \lambda_0 - \sigma_{x_1}^{-k_1}\ldots\sigma_{x_{n-1}}^{-k_{n-1}}\sigma_{x_n}(\lambda_{k_n-1}) & \pmod{W} \\ 0 \equiv \lambda_1 - \sigma_{x_n}(\lambda_0) & \pmod{W} \\ \qquad\vdots & \\ 0 \equiv \lambda_{k_n-1} - \sigma_{x_n}(\lambda_{k_n-2}) & \pmod{W}. \end{cases} \tag{5.21}$$

Since W is G-invariant, it follows from the equations that

$$a \equiv \sigma_{x_1}^{-k_1}\ldots\sigma_{x_{n-1}}^{-k_{n-1}}\sigma_{x_n}^{k_n}(\lambda_0) - \lambda_0 \equiv \Delta_{\tau_r}(\lambda_0) \pmod{W}.$$

This completes the proof. ∎

Remark 5.9. *For the bivariate case with $n = 2$, Theorem 5.8 coincides with the known criterion in [36, Theorem 3.3]. In this case, $\operatorname{rank}(G_d) \leq 1$ and $H_d = \{\mathbf{1}\}$. If $\operatorname{rank}(G_d) = 0$, then a/d^j is $(\sigma_{x_1}, \sigma_{x_2})$-summable in $\mathbb{F}(\mathbf{x})$ if and only if $a = 0$. If $\operatorname{rank}(G_d) = 1$ and G_d is generated by $\tau = \sigma_{x_1}^{\ell_1}\sigma_{x_2}^{-\ell_2} \in G$ for some $\ell_2 \neq 0$, then a/d^j is $(\sigma_{x_1}, \sigma_{x_2})$-summable if and only if $a = \sigma_{x_1}^{\ell_1}\sigma_{x_2}^{-\ell_2}(b) - b$ for some $b \in \mathbb{F}(\hat{\mathbf{x}}_1)[x_1]$ with $\deg_{x_1}(b) < \deg_{x_1}(d)$.*

Example 5.10. *Let $f = 1/(x_1^s + \cdots + x_n^s) \in \mathbb{Q}(x_1, \ldots, x_n)$ with $s, n \in \mathbb{N} \setminus \{0\}$. Let G_d be the isotropy group of $d = x_1^s + \cdots + x_n^s$ in $G = \langle \sigma_{x_1}, \ldots, \sigma_{x_n} \rangle$. Decide the $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summability of f in $\mathbb{Q}(x_1, \ldots, x_n)$.*

(1) If $s = 1$ and $n = 1$, then $f = 1/x_1^s$. Since the isotropy group of x_1 in $\langle \sigma_{x_1} \rangle$ is $\{\mathbf{1}\}$, by Theorem 5.8, we get f is not (σ_{x_1})-summable.

(2) If $s = 1$ and $n > 1$, then d is irreducible. The rank of G_d is $n - 1$ and one basis is given by $\tau_1, \ldots, \tau_{n-1}$ with $\tau_i = \sigma_{x_i}\sigma_{x_{i+1}}^{-1}$ for $i = 1, \ldots, n - 1$. Since $1 = \tau_1(x_1) - x_1$, it follows that f is $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summable. In fact, we have

$$\frac{1}{x_1 + \cdots + x_n} = \Delta_{x_1}\left(\frac{x_1}{x_1 + \cdots + x_n}\right) + \Delta_{x_2}\left(\frac{-x_1 - 1}{x_1 + \cdots + x_n}\right).$$

This means f is $(\sigma_{x_1}, \sigma_{x_2})$-summable , so is $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summable.

(3) If $s > 1$ and $n = 2$, then $f = 1/(x_1^s + x_2^s) = \sum_{j=1}^s a_j/(x_1 - \beta_j x_2)$, where β_j's are distinct roots of $z^s = -1$ and $a_j = 1/s(\beta_j x_2)^{s-1}$. There exists $j \in \{1, \ldots, s\}$ such that $\beta_j \notin \mathbb{Z}$. Then for $d_j = x_1 - \beta_j x_2$, we have $G_{d_j} = \{\mathbf{1}\}$. So a_j/d_j is not $(\sigma_{x_1}, \sigma_{x_2})$-summable in $\mathbb{C}(x_1, x_2)$ and by Lemma 5.1, neither is f. Hencef is not $(\sigma_{x_1}, \sigma_{x_2})$-summable in $\mathbb{Q}(x_1, x_2)$. This result has appeared in [21, Example 3.8].

(4) If $s > 1$ and $n > 2$, then d is irreducible. Since $G_d = \{\mathbf{1}\}$, by Theorem 5.8, we get f is not $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summable.

Now we only need to transfer the $(\tau_1, \ldots, \tau_r)$-summability problem into the $(\sigma_{x_1}, \ldots, \sigma_{x_r})$-summability problem.

Proposition 5.11. *Let $\{\tau_i\}_{i=1}^r (1 \leq r \leq n)$ be a family of linearly independent elements in $G = \langle \sigma_{x_1}, \ldots, \sigma_{x_n} \rangle$. Then there exists an $\mathbb{F}$-automorphism ϕ of $\mathbb{F}(\mathbf{x})$ such that ϕ is a difference isomorphism between the difference fields $(\mathbb{F}(\mathbf{x}), \tau_i)$ and $(\mathbb{F}(\mathbf{x}), \sigma_{x_i})$ for all $i = 1, \ldots, r$. Therefore, for any $f \in \mathbb{F}(\mathbf{x})$, f is $(\tau_1, \ldots, \tau_r)$-summable in $\mathbb{F}(\mathbf{x})$ if and only if $\phi(f)$ is $(\sigma_{x_1}, \ldots, \sigma_{x_r})$-summable in $\mathbb{F}(\mathbf{x})$.*

Proof. Assume $\tau_i = \sigma_{x_1}^{a_{i,1}} \ldots \sigma_{x_m}^{a_{i,m}}$ with $a_{i,j} = 0$ if $j > n$ and write $\alpha_i = (a_{i,1}, \ldots, a_{i,m}) \in \mathbb{Z}^m$ viewed as a vector in $\mathbb{Q}^m$ for $i = 1, \ldots, r$. Then $\alpha_1, \ldots, \alpha_r$ are linearly independent over $\mathbb{Q}$. So we can find the other vectors $\alpha_{r+1}, \ldots, \alpha_m$ such that $\{\alpha_1, \ldots, \alpha_m\}$ forms a basis of $\mathbb{Q}^m$. Let $\alpha_i = (a_{i,1}, \ldots, a_{i,m})$ for $i = r+1, \ldots, m$ and $A = (a_{i,j}) \in \mathbb{Q}^{m \times m}$. Then A is an invertible matrix. Thus we define an $\mathbb{F}$-automorphism $\phi : \mathbb{F}(\mathbf{x}) \to \mathbb{F}(\mathbf{x})$ by

$$(\phi(x_1), \ldots, \phi(x_m)) := (x_1, \ldots, x_m)A.$$

Let $u_j := \phi(x_j) = \sum_{i=1}^m a_{i,j} x_i$ for all $1 \leq j \leq m$. Then ϕ satisfies the relation $\phi \circ \tau_i = \sigma_{x_i} \circ \phi$ for all $i = 1, \ldots, r$, which means the following diagrams

$$\begin{array}{ccc} \mathbb{F}(\mathbf{x}) & \xrightarrow{\phi} & \mathbb{F}(\mathbf{x}) \\ \downarrow{\scriptstyle \tau_1} & & \downarrow{\scriptstyle \sigma_1} \\ \mathbb{F}(\mathbf{x}) & \xrightarrow{\phi} & \mathbb{F}(\mathbf{x}) \end{array} \qquad \cdots \qquad \begin{array}{ccc} \mathbb{F}(\mathbf{x}) & \xrightarrow{\phi} & \mathbb{F}(\mathbf{x}) \\ \downarrow{\scriptstyle \tau_r} & & \downarrow{\scriptstyle \sigma_r} \\ \mathbb{F}(\mathbf{x}) & \xrightarrow{\phi} & \mathbb{F}(\mathbf{x}) \end{array}$$

are commutative. This is true since for any $f \in \mathbb{F}(x_1, \ldots, x_m)$, we have

$$\begin{aligned} \phi\left(\tau_i(f(x_1, \ldots, x_m)\right) &= \phi\left(f(x_1 + a_{i,1}, \ldots, x_m + a_{i,m})\right) \\ &= f(u_1 + a_{i,1}, \ldots, u_m + a_{i,m}) \end{aligned}$$

and

$$\begin{aligned} \sigma_{x_i}\left(\phi(f(x_1, \ldots, x_m)\right) &= \sigma_{x_i}\left(f\left(u_1, \ldots, u_m\right)\right) \\ &= f\left(u_1 + a_{i,1}, \ldots, u_m + a_{i,m}\right). \end{aligned}$$

It follows that

$$f = \sum_{i=1}^r \Delta_{\tau_i}(g_i) \iff \phi(f) = \sum_{i=1}^r \Delta_{x_i}(\phi(g_i)) \tag{5.22}$$

whenever $f, g_1, \ldots, g_r \in \mathbb{F}(\mathbf{x})$. This proves our assertion. ∎

Combining Theorem 5.8 and Proposition 5.11, the summability problem 2.4 in n variables can be reduced to that in fewer variables. So we can design the following recursive algorithm for testing $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summability of multivariate rational functions. Furthermore, the $(\tau_1, \ldots, \tau_n)$-summability problem can also be solved via the transformation in Proposition 5.11.

Algorithm 5.12 (Rational Summability Testing)**. IsSummable(**f**,** $[x_1, \ldots, x_n]$**).**
INPUT: a multivariate rational function $f \in \mathbb{F}(\mathbf{x})$ and a list $[x_1, \ldots, x_n]$ of variable names;
OUTPUT: certificates $g_1, \ldots, g_n$ for f if f is $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summable in $\mathbb{F}(\mathbf{x})$; false *otherwise.*

using shift equivalence testing and partial fraction decomposition, decompose f into $f = f_0 + \sum_{j \in \mathbb{N}^+} \sum_{[d]_G} f_{[d]_G, j}$ as in Equation (5.2).

apply the reduction to f_0 *and each nonzero component* $f_{[d]_G,j}$ *such that*

$$f = \Delta_{x_1}(g_1) + \cdots + \Delta_{x_n}(g_n) + r \text{ with } r = \sum_{i=1}^{I}\sum_{j=1}^{J_i} \frac{a_{i,j}}{d_i^j}, \tag{5.23}$$

where $a_{i,j}/d_i^j$ *is the remainder of* $f_{[d_i]_G,j}$ *described in Lemma 5.2.*

if $r = 0$, *then* **return** $g_1, \ldots, g_n$.

for $i = 1, \ldots, I$ **do**

  compute a basis $\tau_{i,1}, \ldots, \tau_{i,r_i}$ *for the isotropy group* G_{d_i} *of* d_i.

  for $j = 1, \ldots, J_i$ **do**

   if $n = 1$ *or* $G_{d_i} = \{\mathbf{1}\}$ *then*

    return false *if* $a_{i,j} \neq 0$.

   else

    find an $\mathbb{F}$*-automorphism* ϕ_i *of* $\mathbb{F}(\mathbf{x})$ *given in Proposition 5.11 such that* $\phi_i \circ \tau_{i,\ell} = \sigma_{x_\ell} \circ \phi_i$ *for* $\ell = 1, \ldots, r_i$.

    set $\tilde{a}_{i,j} = \phi_i(a_{i,j})$.

    IsSummable($\tilde{a}_{i,j}$, $[x_1, \ldots, x_{r_i}]$).

    if $\tilde{a}_{i,j}$ *is* $(\sigma_{x_1}, \ldots, \sigma_{x_{r_i}})$*-summable in* $\mathbb{F}(\mathbf{x})$, *let*

$$\tilde{a}_{i,j} = \Delta_{x_1}\left(\tilde{b}_{i,j}^{(1)}\right) + \cdots + \Delta_{x_{r_i}}\left(\tilde{b}_{i,j}^{(r_i)}\right); \tag{5.24}$$

    return false *otherwise.*

    applying ϕ_i^{-1} *to the previous equation yields that*

$$a_{i,j} = \Delta_{\tau_{i,1}}\left(b_{i,j}^{(1)}\right) + \cdots + \Delta_{\tau_{i,r_i}}\left(b_{i,j}^{(r_i)}\right), \tag{5.25}$$

    where $(b_{i,j}^{(1)}, \ldots, b_{i,j}^{(r_i)}) = (\phi_i^{-1}(\tilde{b}_{i,j}^{(1)}), \ldots, \phi_i^{-1}(\tilde{b}_{i,j}^{(r_i)}))$.

    using Formula 5.7 to compute $h_{i,j}^{(1)}, \ldots, h_{i,j}^{(n)} \in \mathbb{F}(\mathbf{x})$ *such that*

$$\frac{a_{i,j}}{d_i^j} = \sum_{\ell=1}^{r_i} \Delta_{\tau_{i,\ell}}\left(\frac{b_{i,j}^{(\ell)}}{d_i^j}\right) = \sum_{\ell=1}^{n} \Delta_{x_\ell}\left(h_{i,j}^{(\ell)}\right) \tag{5.26}$$

    update $g_\ell = g_\ell + h_{i,j}^{(\ell)}$ *for* $\ell = 1, \ldots, n$.

return $g_1, \ldots, g_n$.

Example 5.13. *Let* $G = \langle \sigma_x, \sigma_y, \sigma_z \rangle$ *and* $f = f_1 + f_2 + f_3 \in \mathbb{Q}(x, y, z)$ *be the same as in Example 4.9.*

1. *After the* $(\sigma_x, \sigma_y, \sigma_z)$*-reduction for* f_1, *see Example 5.3, we get*

$$f_1 = \Delta_x(u_1) + \Delta_y(v_1) + \Delta_z(w_1) + r_1 \text{ with } r_1 = \frac{2x - 1}{d_1}, \tag{5.27}$$

   where $u_1, v_1, w_1 \in \mathbb{Q}(x, y, z)$ *and* $d_1 = x^2 + 2xy + z^2$. *By Example 4.5.1, the isotropy group* $G_{d_1} = \{\mathbf{1}\}$ *is trivial. By Theorem 5.8, we see* r_1 *is not* $(\sigma_x, \sigma_y, \sigma_z)$*-summable because its numerator* $a_1 = 2x - 1$ *is not zero. Hence* f_1 *is not* $(\sigma_x, \sigma_y, \sigma_z)$*-summable.*

2. *For $f_2 = a_2/d_2$ with $a_2 = x+z$ and $d_2 = (x-3y)^2(y+z)+1$, we know from Example 4.5.2 that a basis of G_{d_2} is $\{\sigma_x^3\sigma_y\sigma_z^{-1}\}$. For any $\{\mu,\nu\} \subset \{x,y,z\}$, since the isotropy group of d_2 in $\langle\sigma_\mu,\sigma_\nu\rangle$ is trivial, we get that f_2 is not (σ_μ,σ_ν)-summable in $\mathbb{Q}(x,y,z)$. By Theorem 5.8, we see f_2 is $(\sigma_x,\sigma_y,\sigma_z)$-summable in $\mathbb{Q}(x,y,z)$ if and only if a_2 is (τ)-summable in $\mathbb{Q}(x,y,z)$ with $\tau = \sigma_x^3\sigma_y\sigma_z^{-1}$. Choose one $\mathbb{Q}$-automorphism ϕ_2 of $\mathbb{Q}(x,y,z)$ given in Proposition 5.11 as follows*

$$\phi_2(h(x,y,z)) = h(3x, x+y, -x+z),$$

for any $h \in \mathbb{Q}(x,y,z)$. Then $\phi_2 \circ \tau = \sigma_x \circ \phi_2$. Hence a_2 is (τ)-summable in $\mathbb{Q}(x,y,z)$ if and only if $\phi_2(a_2)$ is (σ_x)-summable in $\mathbb{Q}(x,y,z)$. Since

$$\phi_2(a_2) = 2x+z = \Delta_x((x-1)(x+z)) \tag{5.28}$$

is (σ_x)-summable, it follows that f_2 is $(\sigma_x,\sigma_y,\sigma_z)$-summable. In fact, applying ϕ_2^{-1} to Equation (5.28) yields that

$$a_2 = x+z = \Delta_\tau(b) \text{ with } b = \frac{1}{9}(x-3)(2x+3z).$$

By Formula 5.7, we have

$$f_2 = \Delta_\tau\left(\frac{b}{d_2}\right) = \Delta_x(u_2) + \Delta_y(v_2) + \Delta_z(w_2), \tag{5.29}$$

where $u_2 = \sum_{\ell=0}^{2} \sigma_x^\ell\sigma_y\sigma_z^{-1}\left(\frac{b}{d_2}\right)$, $v_2 = \sigma_z^{-1}\left(\frac{b}{d_2}\right)$ and $w_2 = -\sigma_z^{-1}\left(\frac{b}{d_2}\right)$.

3. *For $f_3 = a_3/d_3^2$ with $a_3 = y + z/(y^2+z-1) - 1/(y^2+z)$ and $d_3 = x+2y+z$, we know from Example 4.5.2 that a basis of G_{d_3} is $\{\tau_1,\tau_2\}$, where $\tau_1 = \sigma_x^2\sigma_y^{-1}$, $\tau_2 = \sigma_x\sigma_z^{-1}$. To decide the $(\sigma_x,\sigma_y,\sigma_z)$-summability of f_3, we construct a $\mathbb{Q}$-automorphism ϕ_3 of $\mathbb{Q}(x,y,z)$ such that $\phi_3\circ\tau_1 = \sigma_x\circ\phi_3$ and $\phi_3\circ\tau_2 = \sigma_y\circ\phi_3$ as follows*

$$\phi_3(h(x,y,z)) = h(2x+y, -x, -y+z),$$

for any $h \in \mathbb{Q}(x,y,z)$. Then it remains to decide the (σ_x,σ_y)-summability of

$$\phi_3(a_3) = -x + \frac{z-y}{\underbrace{x^2-y+z-1}_{\sigma_y(\tilde{d})}} - \frac{1}{\underbrace{x^2-y+z}_{\tilde{d}}}$$

in $\mathbb{Q}(x,y,z)$. So we use (σ_x,σ_y)-reduction to reduce $\phi_3(a_3)$ and obtain

$$\phi_3(a_3) = \Delta_x\left(\tilde{b}_1\right) + \Delta_y\left(\tilde{b}_2\right) + \frac{z-y}{x^2-y+z}, \tag{5.30}$$

where $\tilde{b}_1 = -\frac{1}{2}x(x-1)$ and $\tilde{b}_2 = \frac{z-y+1}{x^2-y+z}$. Since the isotropy group of $\tilde{d}$ in $\langle\sigma_x,\sigma_y\rangle$ is trivial, $\phi_3(a_3)$ is not (σ_x,σ_y)-summable. Hence f_3 is not $(\sigma_x,\sigma_y,\sigma_z)$-summable. Even so, in this case, using the above calculation, we can further decompose f_3 into a summable part and a remainder. Let us see how to do this. Starting from the decomposition (5.30) of $\phi_3(a_3)$ with respect to the (σ_x,σ_y)-summability problem, we apply ϕ_3^{-1} to both sides of this decomposition to obtain that

$$a_3 = \Delta_{\tau_1}(b_1) + \Delta_{\tau_2}(b_2) + \frac{z}{y^2+z}.$$

where $b_1 = \phi_3^{-1}(\tilde{b}_2) = -\frac{1}{2}y(y+1)$ *and* $b_2 = \phi_3^{-1}(\tilde{b}_2) = \frac{z+1}{y^2+z}$. *By Formula 5.7 with* $\tau = \tau_1, \tau_2$, *we have*

$$\begin{aligned} f_3 = \frac{a_3}{d_3^2} &= \Delta_{\tau_1}\left(\frac{b_1}{d_3^2}\right) + \Delta_{\tau_2}\left(\frac{b_2}{d_3^2}\right) + \underbrace{\frac{z}{(y^2+z)d_3^2}}_{r_3} \\ &= \Delta_x(u_3) + \Delta_y(v_3) + \Delta_z(w_3) + r_3, \end{aligned} \tag{5.31}$$

where $u_3 = \sum_{\ell=0}^{1} \sigma_x^\ell \sigma_y^{-1}\left(\frac{b_1}{d_3^2}\right) + \sigma_z^{-1}\left(\frac{b_2}{d_3^2}\right)$, $v_3 = -\sigma_y^{-1}\left(\frac{b_1}{d_3^2}\right)$ *and* $w_3 = -\sigma_z^{-1}\left(\frac{b_2}{d_3^2}\right)$.

4. *For* $f = f_1 + f_2 + f_3$, *from Example 4.9 we know* f_1, f_2, f_3 *are in distinct* $V_{[d]_G,j}$ *spaces. Since* f_1 *is not* $(\sigma_x, \sigma_y, \sigma_z)$*-summable, it follows from Lemma 5.1 that* f *is not* $(\sigma_x, \sigma_y, \sigma_z)$ *summable. Moreover, combining Equations (5.27), (5.29) and (5.31), we decompose* f *into*

$$f = \Delta_x(u) + \Delta_y(v) + \Delta_z(w) + r \text{ with } r = \frac{2x-1}{d_1} + \frac{z}{(y^2+z)d_3^2}, \tag{5.32}$$

where $u = \sum_{i=1}^{2} u_i$, $v = \sum_{i=1}^{2} v_i$ *and* $w = \sum_{i=1}^{2} w_i$ *are rational functions in* $\mathbb{Q}(x, y, z)$.

As we discussed in the above example, given a rational function $f \in \mathbb{F}(\mathbf{x})$, we can compute rational functions $g_1, \ldots, g_n, r \in \mathbb{F}(\mathbf{x})$ such that

$$f = \Delta_{x_1}(g_1) + \cdots + \Delta_{x_n}(g_n) + r$$

satisfying the property that f is $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summable if and only if $r = 0$. This process can be achieved by induction on n. However, this remainder r is not unique, which depends on the choice of difference isomorphisms ϕ_i. So how to choose a minimal remainder r is still an open problem.

6 Existence problem of telescopers

Similar to the summability problem, there are mainly two steps of solving the existence problem 2.2 of telescopers. First we use the orbital decomposition and Abramov's reduction to simplify the existence problem in Section 6.1. Then in Section 6.2, we use the exponent separation introduced in [19] to further reduce the existence problem to simple fractions and use the summability criteria in Section 5.2 to derive the existence criteria.

6.1 Orbital reduction for the existence of telescopers

Let f be a rational function in $\mathbb{K}(t, \mathbf{x})$, where $\mathbf{x} = \{x_1, \ldots, x_m\}$. Let n be an integer such that $1 \leq n \leq m$. We consider the existence problem of telescopers of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_n})$ for the rational function f in $\mathbb{K}(t, \mathbf{x})$. Let $G_t = \langle \sigma_t, \sigma_{x_1}, \ldots, \sigma_{x_n} \rangle$ be the free abelian group generated by the shift operators $\sigma_t, \sigma_{x_1}, \ldots, \sigma_{x_n}$. Taking $\mathbb{E} = \mathbb{K}(t, \hat{\mathbf{x}}_1)$ and $A = G_t$ in Equality (4.3), we get

$$V_{[d]_{G_t},j} = \operatorname{Span}_{\mathbb{E}}\left\{ \frac{a}{\tau(d)^j} \,\middle|\, a \in \mathbb{E}[x_1], \tau \in G_t, \deg_{x_1}(a) < \deg_{x_1}(d) \right\}. \tag{6.1}$$

Then f can be decomposed as

$$f = f_0 + \sum_j \sum_{[d]_{G_t}} f_{[d]_{G_t},j}, \tag{6.2}$$

where $f_0 \in V_0 = \mathbb{E}[x_1]$ and $f_{[d]_{G_t},j}$ are in distint $V_{[d]_{G_t},j}$ spaces. It induces the following orbital decomposition of $\mathbb{K}(t,\mathbf{x})$ with respect to the group G_t

$$\mathbb{K}(t,\mathbf{x}) = V_0 \bigoplus \left(\bigoplus_{j\in\mathbb{N}^+} \bigoplus_{[d]_{G_t}\in T_{G_t}} V_{[d]_{G_t},j} \right) \tag{6.3}$$

as a vector space over $\mathbb{K}(t,\hat{\mathbf{x}}_1)$. This orbital decomposition is G_t-invariant. Moreover for any L in $\mathbb{K}(t)\langle S_t\rangle$, if $f \in V_{[d]_{G_t},j}$, then $L(f) \in V_{[d]_{G_t},j}$. Note that such an operator L commutes with difference operator Δ_{x_i} for $i = 1,\ldots,n$. So by Remark 2.5 and the similar argument as in the proof of Lemma 5.1, we arrive at the following lemma.

Lemma 6.1. *Let $f \in \mathbb{K}(t,\mathbf{x})$. Then f has a telescoper of type $(\sigma_t;\sigma_{x_1},\ldots,\sigma_{x_n})$ in if and only if f_0 and each $f_{[d]_{G_t},j}$ have a telescoper of the same type for all $[d]_{G_t} \in T_{G_t}$ and $j \in \mathbb{N}^+$.*

Since $f_0 \in V_0 = \mathbb{K}(t,\hat{\mathbf{x}}_1)[x_1]$ is always (σ_{x_1})-summable, we have $L = 1$ is a telescoper for f_0. As for an element in $V_{[d]_{G_t},j}$, it can be written as

$$f = \sum_{\tau} \frac{a_\tau}{\tau(d)^j}, \tag{6.4}$$

where $\tau \in G_t$, $a_\tau \in \mathbb{K}(t,\hat{\mathbf{x}}_1)[x_1]$, $d \in \mathbb{K}[t,\mathbf{x}]$ with $\deg_{x_1}(a_\tau) < \deg_{x_1}(d)$ and d is irreducible in x_1 over $\mathbb{K}(t,\hat{\mathbf{x}}_1)$. Each $\tau \in G_t$ is in the form of $\tau = \sigma_t^{k_0}\sigma_{x_1}^{k_1}\cdots\sigma_{x_n}^{k_n}$ for some $k_0,k_1,\ldots,k_n \in \mathbb{Z}$. Using the $(\sigma_{x_1},\ldots,\sigma_{x_n})$-reduction formula (5.7), we get the following decomposition.

Lemma 6.2. *Let $f \in V_{[d]_{G_t},j}$ be in the form (6.4). Then we can decompose it into the form*

$$f = \sum_{i=1}^{n} \Delta_{x_i}(g_i) + r \text{ with } r = \sum_{\ell=0}^{\rho} \frac{a_\ell}{\sigma_t^\ell(\mu)^j}, \tag{6.5}$$

where $\rho \in \mathbb{N}$, $g_i \in \mathbb{K}(t,\mathbf{x})$, $a_\ell \in \mathbb{K}(t,\hat{\mathbf{x}}_1)[x_1]$, $\mu \in \mathbb{K}[t,\mathbf{x}]$, $\deg_{x_1}(a_\ell) < \deg_{x_1}(d)$, μ is in the same G_t-orbit as d, and $\sigma_t^\ell(\mu)$, $\sigma_t^{\ell'}(\mu)$ are not G-equivalent for $0 \le \ell \ne \ell' \le \rho$. Therefore. f has a telescoper of type $(\sigma_t;\sigma_{x_1},\ldots,\sigma_{x_n})$ if and only if r has a telescoper of the same type.

Example 6.3. *Let $\mathbb{K} = \mathbb{Q}$, $G_t = \langle\sigma_t,\sigma_x,\sigma_y,\sigma_z\rangle$ and $G = \langle\sigma_x,\sigma_y,\sigma_z\rangle$.*

1. *Consider the rational function f in $\mathbb{Q}(t,x,y,z)$ of the form*

$$f = \frac{2x-1}{d} + \frac{y}{\sigma_t(d)} + \frac{1}{\sigma_t^3\sigma_x\sigma_y\sigma_z(d)}$$

where $d = x^2 + 2xy + z^2 + t$. Then $f \in V_{[d]_{G_t},1}$ and applying $(\sigma_x,\sigma_y,\sigma_z)$-reduction formula to f yields that

$$f = \Delta_x(u_0) + \Delta_y(v_0) + \Delta_z(w_0) + \frac{2x-1}{d} + \frac{y}{\sigma_t(d)} + \frac{1}{\sigma_t^3(d)}, \tag{6.6}$$

where

$$u_0 = \frac{1}{\sigma_t^3\sigma_y\sigma_z(d)},\ v_0 = \frac{1}{\sigma_t^3\sigma_z(d)} \text{ and } w_0 = \frac{1}{\sigma_t^3(d)}.$$

Since there is no nonzero integer s such that $\sigma_t^s(d)$ and d are G-equivalent, the equation (6.6) gives a required decomposition for f in Lemma 6.2.

2. Consider the rational function f in $\mathbb{Q}(t,x,y,z)$ of the form

$$f = \frac{1}{t(t+y+2z)d} + \frac{y+z-1}{(t+3z)\sigma_t(d)} - \frac{y+z}{(t+3z)\sigma_t\sigma_x^3\sigma_y^2(d)},$$

where $d = 3y + (x+z)^2 + t$. Then $f \in V_{[d]_{G_t},1}$ and applying $(\sigma_x, \sigma_y, \sigma_z)$-reduction formula to f yields that

$$f = \Delta_x(u_0) + \Delta_y(v_0) + \Delta_z(w_0) + \frac{1}{t(t+y+2z)d} + \frac{1}{(t+3z)\sigma_t(d)}, \tag{6.7}$$

where

$$u_0 = -\sum_{\ell=0}^{2} \frac{y+z}{(t+3z)\sigma_t\sigma_x^\ell\sigma_y^2(d)}, \quad v_0 = -\sum_{\ell=0}^{1} \frac{y+\ell-2+z}{(t+3z)\sigma_t\sigma_y^\ell(d)} \text{ and } w_0 = 0.$$

We claim that the equation (6.7) gives a required decomposition for f in Lemma 6.2. Since the isotropy group of d in G_t is $G_{t,d} = \langle \sigma_t^3\sigma_y^{-1}, \sigma_x\sigma_z^{-1}\rangle$, the minimal positive integer s such that $\sigma_t^s(d)$ and d are G-equivalent is $s = 3$. So d and $\sigma_t(d)$ are not G-equivalent.

6.2 Criteria on the existence of telescopers

Combining Lemmas 6.1 and 6.2, we reduce the existence problem (2.2) to that for rational functions in the form

$$f = \sum_{i=0}^{I} \frac{a_i}{\sigma_t^i(d)^j}, \tag{6.8}$$

where $j \in \mathbb{N}\setminus\{0\}$, $a_i \in \mathbb{K}(t,\hat{\mathbf{x}}_1)[x_1]$, $d \in \mathbb{K}[t,\mathbf{x}]$, $\deg_{x_1}(a_i) < \deg_{x_1}(d)$ and d is irreducible such that $\sigma_t^i(d)$ and $\sigma_t^{i'}(d)$ are not G-equivalent for $0 \le i \ne i' \le I$.

Let $G_t = \langle \sigma_t, \sigma_{x_1}, \ldots, \sigma_{x_n}\rangle$ and $G = \langle \sigma_{x_1}, \ldots, \sigma_{x_n}\rangle$ be a subgroup of G_t. Let G_d and $G_{t,d}$ be the isotropy groups of the polynomial d in G and G_t, respectively. By Lemma 4.4, the quotient group $G_{t,d}/G_d$ is free and of rank 0 or 1.

In the case of $\operatorname{rank}(G_{t,d}/G_d) = 0$, the existence problem of telescopers is equivalent to the summability problem.

Lemma 6.4. *Let $f \in \mathbb{K}(t,\mathbf{x})$ be in the form (6.8). If $\operatorname{rank}(G_{t,d}/G_d) = 0$, then f has a telescoper of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_n})$ if and only if each $a_i/\sigma_t^i(d)^j$ is $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summable in $\mathbb{K}(t,\mathbf{x})$ for $0 \le i \le I$.*

Proof. Suppose that each $a_i/\sigma_t^i(d)^j$ is $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summable for $0 \le i \le I$. By the linearity of difference operators Δ_{x_i}, we see $L = \mathbf{1}$ is a telescoper for f. Conversely, assume that $L = \sum_{\ell=0}^{\rho} e_\ell S_t^\ell$ with $e_\ell \in \mathbb{K}(t)$ and $e_0 \ne 0$ is a telescoper of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_n})$ for f. Then we have

$$L(f) = \sum_{\ell=0}^{\rho}\sum_{i=0}^{I} e_\ell\sigma_t^\ell\left(\frac{a_i}{\sigma_t^i(d)^j}\right) = \sum_{\ell=0}^{I+\rho}\left(\frac{\sum_{i=0}^{\ell} e_i\sigma_t^i(a_{\ell-i})}{\sigma_t^\ell(d)^j}\right) \tag{6.9}$$

is $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summable, where $e_\ell = 0$ if $\ell > \rho$ and $a_i = 0$ if $i > I$. Since $\operatorname{rank}(G_{t,d}/G_d) = 0$, all $\sigma_t^\ell(d)$ with $\ell \in \mathbb{Z}$ are in distinct G-orbits. By Lemma 5.1, for any ℓ with $0 \le \ell \le \rho$, there exist $g_{\ell,1}, \ldots, g_{\ell,n} \in \mathbb{K}(t,\mathbf{x})$ such that

$$\frac{\sum_{i=0}^{\ell} e_i\sigma_t^i(a_{\ell-i})}{\sigma_t^\ell(d)^j} = \Delta_{x_1}(g_{\ell,1}) + \cdots + \Delta_{x_n}(g_{\ell,n}). \tag{6.10}$$

To show that each $a_i/\sigma_t^i(d)^j$ is $(\sigma_{x_1},\ldots,\sigma_{x_n})$-summable for $0 \le i \le I$, we proceed by induction. For $i=0$, substituting $\ell=0$ into (6.10), we get $a_0/d^j = \Delta_{x_1}(g_{0,1}/e_0)+\cdots+\Delta_{x_n}(g_{0,n}/e_0)$. Suppose we have $a_i/\sigma_t^i(d)^j$ is $(\sigma_{x_1},\ldots,\sigma_{x_n})$-summable for $i=0,\ldots,s-1$ with $s \le I$. Taking $\ell = s$ in Equation (6.10) yields that

$$\frac{a_s}{\sigma_t^s(d)^j} = \Delta_{x_1}\left(\frac{g_{s,1}}{e_0}\right)+\cdots+\Delta_{x_n}\left(\frac{g_{s,n}}{e_0}\right) - \frac{1}{e_0}\sum_{i=1}^{s} e_i\sigma_t^i\left(\frac{a_{s-i}}{\sigma_t^{s-i}(d)^j}\right).$$

By the inductive hypothesis, we have $a_{s-i}/\sigma_t^{s-i}(d)^j$ is $(\sigma_{x_1},\ldots,\sigma_{x_n})$-summable for $1 \le i \le s$. Note that $e_i \in \mathbb{K}(t)$ is free of $\mathbf{x}$. Due to the commutativity between σ_t and σ_{x_i} for $i=1,\ldots,n$, we get $\frac{1}{e_0}\sum_{i=1}^{s} e_i\sigma_t^i\left(\frac{a_{s-i}}{\sigma_t^{s-i}(d)^j}\right)$ is $(\sigma_{x_1},\ldots,\sigma_{x_n})$-summable. Hence $a_s/\sigma_t^s(d)^j$ is also $(\sigma_{x_1},\ldots,\sigma_{x_n})$-summable. ∎

Example 6.5. *Continue the Example 6.3.1 and write $f \in \mathbb{Q}(t,x,y,z)$ as*

$$f = \Delta_x(u_0)+\Delta_y(v_0)+\Delta_z(w_0)+r \text{ with } r = \frac{2x-1}{d}+\frac{y}{\sigma_t(d)}+\frac{1}{\sigma_t^3(d)},$$

where $u_0, v_0, w_0 \in \mathbb{Q}(t,x,y,z)$ and $d = x^2+2xy+z^2+t$. Note that the isotropy groups $G_{t,d} = G_d = \{\mathbf{1}\}$ are trivial. The first term $(2x-1)/d$ of r is not $(\sigma_x,\sigma_y,\sigma_z)$-summable in $\mathbb{Q}(t,x,y,z)$ by the similar reason as in Example 5.13.1. Since $\operatorname{rank}(G_{t,d}/G_d)=0$, we know from Lemma 6.4 that r does not have any telescoper of type $(\sigma_t;\sigma_x,\sigma_y,\sigma_z)$ and neither does f.

Lemma 6.6. *Let $f = \sum_{i=1}^{I} a_i/\sigma_t^i(d)^j \in \mathbb{K}(t,\mathbf{x})$ be in the form (6.8). If $\operatorname{rank}(G_{t,d}/G_d)=1$, then f has a telescoper of type $(\sigma_t;\sigma_{x_1},\ldots,\sigma_{x_n})$ if and only if each $a_i/\sigma_t^i(d)^j$ has a telescoper of the same type for $0 \le i \le I$.*

Proof. Sufficiency follows from Remark 2.5. The proof of necessity is a natural generalization from the trivariate case [19, lemma 5.3] to the multivariate case. Suppose $L = \sum_{i=0}^{\ell} e_i S_t^i \in \mathbb{K}(t)\langle S_t\rangle$ is a telescoper for f. Since $\operatorname{rank}(G_{t,d}/G_d)=1$, there is a minimal positive integer k_0 such that $\sigma_t^{k_0}(d) = \sigma_{x_1}^{k_1}\cdots\sigma_{x_n}^{k_n}(d)$ for some integers $k_1,\ldots,k_n$. In the expression (6.8), we require that $\sigma_t^i(d)$ and $\sigma_t^{i'}(d)$ are not G-equivalent for any $0 \le i \ne i' \le I$. By the minimality of k_0, we may assume $f = \sum_{i=0}^{k_0-1} a_i/\sigma_t^i(d)^j$. The k_0-exponent separation of L (see [19, Section 4]) is defined as follows

$$L = L_0 + L_1 + \cdots + L_{k_0-1},$$

where $L_i = \sum_{j=0}^{\ell} e_{jm+i}S_t^{jm+i}$ and $e_i = 0$ if $i > \ell$. Since $L(f)$ is $(\sigma_{x_1},\ldots,\sigma_{x_n})$-summable, by Lemma 5.1 each orbital component of $L(f)$ is summable. So we have

$$\begin{cases} L_0\dfrac{a_0}{d^j} + L_{k_0-1}\dfrac{a_1}{\sigma_t(d)^j} + \cdots + L_1\dfrac{a_{k_0-1}}{\sigma_t^{k_0-1}(d)^j} & \equiv 0 \\ L_1\dfrac{a_0}{d^j} + \quad L_0\dfrac{a_1}{\sigma_t(d)^j} + \cdots + L_2\dfrac{a_{k_0-1}}{\sigma_x^{k_0-1}(d)^j} & \equiv 0 \\ \qquad\qquad \cdots & \\ L_{k_0-1}\dfrac{a_0}{d^j} + L_{k_0-2}\dfrac{a_1}{\sigma_t(d)^j} + \cdots + L_0\dfrac{a_{k_0-1}}{\sigma_t^{k_0-1}(d)^j} & \equiv 0, \end{cases} \tag{6.11}$$

where $f \equiv 0$ means f is $(\sigma_{x_1},\ldots,\sigma_{x_n})$-summable in $\mathbb{K}(t,\mathbf{x})$. Taking

$$\mathcal{V} = \left[\frac{a_0}{d^j}, \frac{a_1}{\sigma_t(d)^j}, \ldots, \frac{a_{k_0-1}}{\sigma_t^{k_0-1}(d)^j}\right],$$

then Equation (6.11) can be written as

$$\mathcal{L}_{k_0} \cdot \mathcal{V} \equiv 0, \tag{6.12}$$

where

$$\mathcal{L}_{k_0} = \begin{bmatrix} L_0 & L_{k_0-1} & L_{k_0-2} & \cdots & L_1 \\ L_1 & L_0 & L_{k_0-1} & \cdots & L_2 \\ L_2 & L_1 & L_0 & \cdots & L_3 \\ \vdots & \vdots & \vdots & & \vdots \\ L_{k_0-1} & L_{k_0-2} & L_{k_0-3} & \cdots & L_0 \end{bmatrix}.$$

According to [19, Proposition 4.3], there exist non-zero operators $T_0, \ldots, T_{k_0-1} \in \mathbb{K}(t)\langle S_t\rangle$ and the matrix $\mathcal{M}$ over $\mathbb{K}(t)\langle S_t\rangle$ such that

$$\mathcal{M} \cdot \mathcal{L}_{k_0} = \operatorname{diag}(T_0, \cdots, T_{k_0-1}). \tag{6.13}$$

For each $0 \leq i \leq k_0 - 1$, we have T_i is a telescoper of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_n})$ for $a_i/\sigma_t^i(d)^j$, because $T_i \in \mathbb{K}(t)\langle S_t\rangle$ commutes with the difference operator s $\Delta_{x_1}, \ldots, \Delta_{x_n}$.

∎

Now we consider the existence problem of telescopers for simple fractions in the form

$$f = \frac{a}{d^j} \tag{6.14}$$

where $j \in \mathbb{N} \setminus \{0\}$, $a \in \mathbb{K}(t, \hat{\mathbf{x}}_1)[x_1]$, $d \in \mathbb{K}[t, \mathbf{x}]$, $\deg_{x_1}(a) < \deg_{x_1}(d)$ and d is irreducible such that $\operatorname{rank}(G_{t,d}/G_d) = 1$.

Theorem 6.7 (Theorem 1.7, restated). *Let $f \in \mathbb{K}(t, \mathbf{x})$ be as in (6.14). Let $\{\tau_0, \tau_1, \ldots, \tau_r\}(1 \leq r < n)$ be a basis of $G_{t,d}$ such that $G_{t,d}/G_d = \langle \bar{\tau}_0 \rangle$ and $\{\tau_1, \ldots, \tau_r\}$ is a basis of G_d (take $\tau_1 = \mathbf{1}$, if $G_d = \{\mathbf{1}\}$). If $\tau_0 = \sigma_t^{k_0}\sigma_{x_1}^{-k_1} \cdots \sigma_{x_n}^{-k_n}$, set $T_0 = S_t^{k_0} S_{x_1}^{-k_1} \cdots S_{x_n}^{-k_n}$. Then f has a telescoper of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_n})$ if and only if there exists a nonzero operator $L \in \mathbb{K}(t)\langle T_0\rangle$ such that*

$$L(a) = \Delta_{\tau_1}(b_1) + \cdots \Delta_{\tau_r}(b_r)$$

for some $b_i \in \mathbb{K}(t, \hat{\mathbf{x}}_1)[x_1]$ with $\deg_{x_1}(b_i) < \deg_{x_1}(d)$ for $1 \leq i \leq r$.

Proof. Firstly, suppose that $L_0 = \sum_{\ell=0}^{\rho} e_\ell T_0^\ell \in \mathbb{K}(t)\langle T_0\rangle$ is a nonzero operator such that $L_0(a) = \sum_{i=1}^{r} \Delta_{\tau_i}(b_i)$ for some $b_i \in \mathbb{K}(t, \hat{\mathbf{x}}_1)[x_1]$ with $\deg_{x_1}(b_i) < \deg_{x_1}(d)$. Set $L = \sum_{\ell=0}^{\rho} e_\ell S_t^{\ell k_0}$. Then

$$\begin{aligned} L(f) &= \sum_{\ell=0}^{\rho} \frac{e_\ell \sigma_t^{\ell k_0}(a)}{\sigma_t^{\ell k_0}(d)^j} = \sum_{\ell=0}^{\rho} \frac{e_\ell \sigma_t^{\ell k_0}(a)}{\sigma_{x_1}^{\ell k_1} \cdots \sigma_{x_n}^{\ell k_n}(d)^j} \\ &= \sum_{i=1}^{n} \Delta_{x_i}(g_i) + \frac{\sum_{\ell=0}^{\rho} e_\ell \sigma_t^{\ell k_0} \sigma_{x_1}^{-\ell k_1} \cdots \sigma_{x_n}^{-\ell k_n}(a)}{d^j} \quad \text{for some } g_i \in \mathbb{K}(t, \mathbf{x}) \\ &= \sum_{i=1}^{n} \Delta_{x_i}(g_i) + \frac{L_0(a)}{d^j} \qquad (6.15) \\ &= \sum_{i=1}^{n} \Delta_{x_i}(g_i) + \frac{1}{d^j} \sum_{i=1}^{r} (\tau_i(b_i) - b_i)) \\ &= \sum_{i=1}^{n} \Delta_{x_i}(g_i) + \sum_{i=1}^{r} \left(\tau_i\left(\frac{b_i}{d^j}\right) - \frac{b_i}{d^j} \right) \\ &= \sum_{i=1}^{n} \Delta_{x_i}(g_i + h_i) \quad \text{for some } h_i \in \mathbb{K}(t, \mathbf{x}). \qquad (6.16) \end{aligned}$$

The last equal sign follows from Formula 5.7.

Conversely, let L be a telescoper of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_n})$ for f. By the k_0-exponent separation (see [19, Section 4]) of L and Lemma 5.1, without loss of generality, we assume $L = \sum_{\ell=0}^{\rho} e_\ell S_t^{\ell k_0} \in \mathbb{K}(t)\langle S_t \rangle$ is a telescoper for f. Then

$$L\left(\frac{a}{d^j}\right) = \sum_{\ell=0}^{\rho} \frac{e_\ell \sigma_t^{\ell k_0}(a)}{\sigma_{x_1}^{\ell k_1} \cdots \sigma_{x_n}^{\ell k_n}(d)^j} = \sum_{i=1}^{n} \Delta_{x_i}(h_i) + \frac{1}{d^j} h \tag{6.17}$$

for some $h_1, \ldots, h_n, h \in \mathbb{K}(t, \mathbf{x})$ with

$$h = \sum_{\ell=0}^{\rho} e_\ell \sigma_t^{\ell k_0} \sigma_{x_1}^{-\ell k_1} \cdots \sigma_{x_n}^{-\ell k_n}(a) = \sum_{\ell=0}^{\rho} e_\ell \tau_0^\ell(a). \tag{6.18}$$

Since $L(a/d^j)$ is $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summable and $\{\tau_1, \ldots, \tau_r\}$ is a basis of G_d, by Theorem 5.8 with $\mathbb{F} = \mathbb{K}(t)$ we get

$$h = \Delta_{\tau_1}(b_1) + \ldots + \Delta_{\tau_r}(b_r) \tag{6.19}$$

for some $b_i \in \mathbb{K}(t, \hat{\mathbf{x}}_1)[x_1]$ with $\deg_{x_1}(b_i) < \deg_{x_1}(d)$ for $1 \leq i \leq r$. Combining Equations (6.18) and (6.19) yields that a has a telescoper $L_0 = \sum_{\ell=0}^{\rho} e_\ell T_0^\ell$ of type $(\tau_0; \tau_1, \ldots, \tau_r)$. ∎

Proposition 6.8. *Let $\tau \in G_t \setminus G$ and $f = a/b$ with $a, b \in \mathbb{K}[t, \mathbf{x}]$ and $\gcd(a, b) = 1$. Then there exist $e_0, \ldots, e_r \in \mathbb{K}(t)$, not all zero, such that $\sum_{i=0}^{r} e_i \tau^i(f) = 0$ if and only if $b = b_1 b_2$ with $b_1 \in \mathbb{K}[t]$ and $b_2 \in \mathbb{K}[t, \mathbf{x}]$ satisfying that $\tau(b_2) = b_2$.*

Proof. First we suppose $b = b_1 b_2$ with b_1, b_2 satisfying the above conditions. Then for any $i \in \mathbb{N}$,

$$\tau^i(f) = \frac{\tau^i(a)}{\tau^i(b_1 b_2)} = \frac{\tau^i(a)}{\tau^i(b_1) b_2} = \frac{\tau^i(a/b_1)}{b_2}. \tag{6.20}$$

Note that $b_1 \in \mathbb{K}[t]$ and the total degrees of the polynomials $\tau^i(a)$ in $\mathbf{x}$ are the same as that of a. Thus all shifts of a/b_1 lie in a finite dimensional linear space over $\mathbb{K}(t)$. So there exist $e_0, e_1, \ldots, e_r \in \mathbb{K}(t)$, not all zero, such that $\sum_{i=0}^{r} e_i \tau^i(a/b_1) = 0$. This implies $\sum_{i=0}^{r} e_i \tau^i(f) = 0$.

Conversely, suppose $\sum_{i=0}^{r} e_i \tau^i(f) = 0$. Let b_1 and b_2 be the content and primitive part of b as a polynomial in $\mathbf{x}$ over $\mathbb{K}(t)$. If $b_2 \in \mathbb{K}$, then we have done. Now we assume that $b_2 \notin \mathbb{K}$. Then all of its irreducible factors have positive total degree in $\mathbf{x}$. Assume that there exists an irreducible polynomial p such that $\tau(p) \neq p$. By Lemma 4.3, the quotient group $G_t/G_{t,p}$ is free, so is torsion free. So for any integer $i \neq 0$, $\tau^i(p) \neq p$. Among all of such irreducible factors of b_2, we can find one factor p such that $\tau^i(p) \nmid b_2$ for any integer $i < 0$. Let s be the largest integer such that $\tau^s(p) \mid b_2$. Then the irreducible polynomial $\tau^{r+s}(p)$ divides $\tau^r(b_2)$, but $\tau^{r+s}(p) \nmid \tau^i(b_2)$ for any $0 \leq i \leq r-1$. Otherwise $\tau^{r+s-i}(p) \mid b_2$, which contradicts the choice of s. Therefore we have $\sum_{i=0}^{r} e_i \tau^i(f) \neq 0$, since p depends on $\mathbf{x}$ and the coefficients e_i are in $\mathbb{K}(t)$. This leads to a contradiction. So every irreducible factor p of b_2 satisfies the property that $\tau(p) = p$. This implies that $\tau(b_2) = b_2$. ∎

Remark 6.9. *For the completeness of our induction method, we state the existence criterion in the bivariate case, i.e., $n = 1$. Let $G_t = \langle \sigma_t, \sigma_{x_1} \rangle$, $G = \langle \sigma_{x_1} \rangle$ and let $f \in \mathbb{K}(t, \mathbf{x})$ be in the form of (6.14) and $\operatorname{rank}(G_{t,d}/G_d) = 1$. Then there exists $\tau = \sigma_t^s \sigma_{x_1}^k \in G_{t,d}$ with $s > 0$ such that $G_{t,d}/G_d = \langle \bar{\tau} \rangle$. Since the degree of d in x_1 is positive, we have $G_d = \{\mathbf{1}\}$. By Theorem 6.7 and Proposition 6.8, we get f has a telescoper of type $(\sigma_t; \sigma_{x_1})$ if and only if $a = c/b$ with $c \in \mathbb{K}[t, \mathbf{x}]$, $b \in \mathbb{K}[t, \hat{\mathbf{x}}_1]$, $\gcd(b, c) = 1$, where b can be written as $b = b_1 b_2$ with $b_1 \in \mathbb{K}[t]$ and $b_2 \in \mathbb{K}[t, \hat{\mathbf{x}}_1]$ such that $\tau(b_2) = b_2$. Note that if $m = n = 1$, then $b \in \mathbb{K}[t]$. In this case, we get f always has a telescoper of type $(\sigma_t; \sigma_{x_1})$. This is the result in [6, Theorem 1] and [20, Theorem 4.11].*

Example 6.10. *Let $f = 1/(t^s + x_1^s + \cdots + x_n^s) \in \mathbb{Q}(t, x_1, \ldots, x_n)$ with $s, n \in \mathbb{N} \setminus \{0\}$. Then $d = t^s + x_1^s + \cdots + x_n^s$ is irreducible over $\mathbb{Q}$ if $n > 1$. Let $G_{t,d}$ and G_d be the isotropy group of d in $G_t = \langle \sigma_t, \sigma_{x_1}, \ldots, \sigma_{x_n} \rangle$ and $G = \langle \sigma_{x_1}, \ldots, \sigma_{x_n} \rangle$, respectively. Decide the existence of telescopers of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_n})$ for f.*

(1) If $s = 1$, then d is irreducible. Since $G_{t,d} = \langle \tau \rangle$ with $\tau = \sigma_t \sigma_{x_1}^{-1}$ and $G_d = \{\mathbf{1}\}$, we have $G_{t,d}/G_d = \langle \bar{\tau} \rangle$ and $\operatorname{rank}(G_{t,d}/G_d) = 1$. Observing that $\tau - 1$ is an annihilator of the numerator of f, by Theorem 6.7 we get f has a telescoper. Indeed $L(f) = \Delta_{x_1}(f) + \Delta_{x_2}(0) + \cdots + \Delta_{x_n}(0)$, where $L = S_t - 1$.

(2) If $s > 1$ and $n = 1$, then $f = 1/(t^s + x_1^s) = \sum_{j=1}^s a_j/(t - \beta_j x_1)$, where β_j's are distinct roots of $z^s = -1$ and $a_j = 1/s(\beta_j x_2)^{s-1}$. There exists $j \in \{1, \ldots, s\}$ such that $\beta^j \notin \mathbb{Z}$. Then for $d_j = t - \beta_j x_1$, we have $G_{t,d_j} = G_{d_j} = \{\mathbf{1}\}$. So a_j/d_j is not σ_{x_1}-summable in $\mathbb{C}(t, x_1)$ and neither is f. By Lemma 6.4, we get f does not have any telescoper of type (σ_t, σ_{x_1}) in $\mathbb{C}(t)\langle S_t \rangle$. Hence f does not have any telescoper of the same type in $\mathbb{Q}(t)\langle S_t \rangle$.

(3) If $s > 1$ and $n > 2$, then d is irreducible. Since $G_d = \{\mathbf{1}\}$, by Theorem 5.8, we get f is not $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summable. Since $G_{t,d} = \{\mathbf{1}\}$ and $\operatorname{rank}(G_{t,d}/G_d) = 0$, by Lemma 6.4, we get f does not have any telescoper.

Proposition 6.11. *Let $\{\tau_0, \tau_1, \ldots, \tau_r\}(1 \le r \le n)$ be a family of $\mathbb{Z}$-linearly independent elements in G_t such that $\tau_0 \in G_t \setminus G$ and $\{\tau_1, \ldots, \tau_r\} \subseteq G$. Then there exists a $\mathbb{K}$-automorphism φ of $\mathbb{K}(t, \mathbf{x})$ such that φ is a difference isomorphism between the difference fields $(\mathbb{K}(t, \mathbf{x}), \tau_0)$ and $(\mathbb{K}(t, \mathbf{x}), \sigma_t)$, and simultaneously a difference isomorphism between $(\mathbb{K}(t, \mathbf{x}), \tau_i)$ and $(\mathbb{K}(t, \mathbf{x}), \sigma_{x_i})$ for all $i = 1, \ldots, r$. Furthermore, for any $f \in \mathbb{K}(t, \mathbf{x})$, f has telescoper of type $(\tau_0; \tau_1, \ldots, \tau_r)$ if and only if $\varphi(f)$ has a telescoper of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_r})$.*

Proof. Let $\tau_i = \sigma_t^{a_{i,0}} \sigma_{x_1}^{a_{i,1}} \cdots \sigma_{x_m}^{a_{i,m}}$, where $a_{i,j} = 0$ if $j > n$. Then $\alpha_i = (a_{i,0}, a_{i,1}, \ldots, a_{i,m}) \in \mathbb{Q}^{m+1}$ for $i = 0, 1, \ldots, r$. Since $\alpha_0, \alpha_1, \ldots, \alpha_r$ are linearly independent over $\mathbb{Q}$, we can find vectors $\alpha_{r+1}, \ldots, \alpha_m \in \mathbb{Q}^{m+1}$ such that $\{\alpha_0, \alpha_1, \ldots, \alpha_m\}$ is a basis of $\mathbb{Q}^{m+1}$ over $\mathbb{Q}$. Write $\alpha_i = (a_{i,0}, a_{i,1}, \ldots, a_{i,m})$ for $i = r+1, \ldots, m$. Since $\tau_0 \in G_t \setminus G$ and $\{\tau_1, \ldots, \tau_r\} \subseteq G$, we have $a_{0,0} \neq 0$ and $a_{i,0} = 0$ for $i = 1, \ldots, r$. So we can further assume that $a_{i,0} = 0$ for $i = r+1, \ldots, m$. Let $A = (a_{i,j}) \in \mathbb{Q}^{(m+1)\times(m+1)}$ and then A is invertible. Let φ be a $\mathbb{K}$-automorphism of $\mathbb{K}(t, \mathbf{x})$ defined by

$$(\varphi(t), \varphi(x_1), \ldots, \varphi(x_m)) := (t, x_1, \ldots, x_m)A.$$

Then $\varphi(t) = a_{0,0} \cdot t$ and $\varphi(x_j) = a_{0,j} \cdot t + \sum_{i=1}^m a_{i,j} \cdot x_i$ for $j = 1, \ldots, m$. It can be checked that $\varphi \circ \tau_0 = \sigma_t \circ \varphi$ and$\varphi \circ \tau_i = \sigma_{x_i} \circ \varphi$ for $1 \le i \le r$. This means the following diagrams are commutative.

$$\begin{array}{ccc} \mathbb{K}(t,\mathbf{x}) & \xrightarrow{\varphi} & \mathbb{K}(t,\mathbf{x}) \\ \tau_0 \downarrow & & \downarrow \sigma_t \\ \mathbb{K}(t,\mathbf{x}) & \xrightarrow{\varphi} & \mathbb{K}(t,\mathbf{x}) \end{array} \qquad \cdots \qquad \begin{array}{ccc} \mathbb{K}(t,\mathbf{x}) & \xrightarrow{\varphi} & \mathbb{K}(t,\mathbf{x}) \\ \tau_i \downarrow & & \downarrow \sigma_{x_i} \\ \mathbb{K}(t,\mathbf{x}) & \xrightarrow{\varphi} & \mathbb{K}(t,\mathbf{x}) \end{array}$$

Note that $\varphi(\mathbb{K}(t)) \subseteq \mathbb{K}(t)$. It follows that

$$\sum_{\ell=0}^{\rho} e_\ell(t) \tau_0^\ell(f) = \sum_{i=1}^{r} \Delta_{\tau_i}(g_i) \quad \Longleftrightarrow \quad \sum_{\ell=0}^{\rho} e_\ell(a_{0,0}t) \sigma_t^\ell(\varphi(f)) = \sum_{i=1}^{r} \Delta_{x_i}(\varphi(g_i)),$$

whenever $e_\ell(t) \in \mathbb{K}(t)$ and $f, g_i \in \mathbb{K}(t, \mathbf{x})$. This completes our proof. ∎

Let $f = a/d^j$ be in the form (6.14) with $\operatorname{rank}(G_{t,d}/G_d) = 1$. By Theorem 6.7, there are two cases according to whether G_d is trivial or not. If $G_d = \{\mathbf{1}\}$, then a/d^j has a telescoper of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_n})$ if and only if there exists a nonzero operator $L \in \mathbb{K}(t)\langle T_0 \rangle$ such that $L(a) = 0$. This problem is solved by Proposition 6.8. If G_d is nontrivial, we can apply the transformation in Proposition 6.11 to reduce the existence problem of telescopers to that of fewer variables. Moreover, the general existence of telescopers of type $(\tau_0; \tau_1, \ldots, \tau_n)$ for rational functions has also been solved.

Algorithm 6.12 (Existence Testing of Telescopers). **IsTelescoperable(**f**,** $[x_1, \ldots, x_n]$**,** t**)**.
INPUT: a multivariate rational function $f \in \mathbb{K}(t, \mathbf{x})$, a set $\{x_1, \ldots, x_n\}$ of variable names and a varaible name t for telescoping;
OUTPUT: a telescoper L and its certificates $g_1, \ldots, g_n$ if f has a telescoper of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_n})$; false *otherwise.*

using shift equivalence testing and irreducible partial fraction decomposition, decompose f into $f = f_0 + \sum_{j \in \mathbb{N}^+} \sum_{[d]_{G_t}} f_{[d]_{G_t}, j}$ as in Equation (6.2).

apply the reduction to f_0 and each nonzero component $f_{[d]_{G_t}, j}$ such that

$$f = \Delta_{x_1}(g_1) + \cdots + \Delta_{x_n}(g_n) + r \text{ with } r = \sum_{i=1}^{I} \sum_{j=1}^{J_i} \sum_{\ell=0}^{s_{i,j}} \frac{a_{i,j,\ell}}{\sigma_t(d_i)^j}, \tag{6.21}$$

where $\sum_{\ell=0}^{s_{i,j}} \frac{a_{i,j,\ell}}{\sigma_t(d_i)^j}$ is the remainder of $f_{[d_i]_{G_t}, j}$ described in Lemma 6.2.

if $r = 0$, then **return** $L = \mathbf{1}$ *and $g_1, \ldots, g_n$.*

for $i = 1, \ldots, I$ **do**

  find elements $\tau_{i,0}, \tau_{i,1}, \ldots, \tau_{i,r_i} \in G_{t,d_i}$ such that $G_{t,d_i}/G_{d_i} = \langle \bar{\tau}_{i,0} \rangle$ and $\tau_{i,1}, \ldots, \tau_{i,r_i}$ form a basis for G_{d_i}.

  for $j = 1, \ldots, J_i$, $\ell = 1, \ldots, s_{i,j}$ **do**

    if $\operatorname{rank}(G_{t,d_i}/G_{d_i}) = 0$ *then*

      IsSummable($r_{i,j,\ell}$**,** $[x_1, \ldots, x_n]$**)**, *where $r_{i,j,\ell} := \frac{a_{i,j,\ell}}{\sigma_t(d_i)^j}$.*

      if $r_{i,j,\ell}$ is $(\sigma_{x_1}, \ldots, \sigma_{x_n})$-summable in $\mathbb{F}(\mathbf{x})$, let

$$r_{i,j,\ell} = \Delta_{x_1}\left(h_{i,j,\ell}^{(1)}\right) + \cdots + \Delta_{x_n}\left(h_{i,j,\ell}^{(n)}\right) \tag{6.22}$$

      and set $L_{i,j,\ell} = \mathbf{1}$; **return** false *otherwise.*

    if $\operatorname{rank}(G_{t,d_i}/G_{d_i}) = 1$ *then*

      choose $\tau_{i,0} = \sigma_t^{k_{i,0}} \sigma_{x_1}^{-k_{i,1}} \cdots \sigma_{x_n}^{-k_{i,n}}$ with $k_{i,0} > 0$.

      set $T_{i,0} = S_t^{k_{i,0}} S_{x_1}^{-k_{i,1}} \cdots S_{x_n}^{k_{i,n}}$.

      if $G_{d_i} = \{\mathbf{1}\}$ then

        using Proposition 6.8 to see whether there exists a nonzero operator $\bar{L}_{i,j,\ell}(t, T_{i,0}) \in \mathbb{K}(t)\langle T_{i,0} \rangle$ such that $\bar{L}_{i,j,\ell}(t, T_{i,0})(a_{i,j,\ell}) = 0$. If so, set $L_{i,j,\ell}(t, S_t) = \bar{L}_{i,j,\ell}(t, S_t^{k_{i,0}})$ and by Equation (6.15) we obtain

$$L_{i,j,\ell}\left(\frac{a_{i,j,\ell}}{\sigma_t^{\ell}(d_i)^j}\right) = \sum_{\lambda=1}^{n} \Delta_{x_\lambda}\left(h_{i,j,\ell}^{(\lambda)}\right) + \underbrace{\frac{\bar{L}_{i,j,\ell}(a_{i,j,\ell})}{\sigma_t^{\ell}(d_i)^j}}_{=0}; \tag{6.23}$$

        return false *otherwise.*

      else

find a $\mathbb{K}$-automorphism φ_i of $\mathbb{K}(t,\mathbf{x})$ given in Proposition 6.11 such that $\varphi_i \circ \tau_{i,0} = \sigma_t \circ \varphi_i$ and $\varphi_i \circ \tau_{i,\ell} = \sigma_{x_i} \circ \varphi_i$ for $\ell = 1, \ldots, r_i$.

set $\tilde{a}_{i,j,\ell} = \varphi_i(a_{i,j,\ell})$.

IsTelescoperable($\tilde{a}_{i,j,\ell}$, $[x_1, \ldots, x_{r_i}], t$).

if $\tilde{a}_{i,j,\ell}$ has a telescoper of type $(\sigma_t; \sigma_{x_1}, \ldots, \sigma_{x_{r_i}})$, let

$$\tilde{L}_{i,j,\ell}(t, S_t)(\tilde{a}_{i,j,\ell}) = \sum_{\lambda=1}^{r_i} \Delta_{x_\lambda}\left(\tilde{b}_{i,j,\ell}^{(\lambda)}\right); \tag{6.24}$$

return false *otherwise.*

apply φ_i^{-1} to both sides of the previous equation to get

$$\bar{L}_{i,j,\ell}(t, T_{i,0})(a_{i,j,\ell}) = \sum_{\lambda=1}^{r_i} \Delta_{\tau_{i,\lambda}}\left(b_{i,j,\ell}^{(\lambda)}\right), \tag{6.25}$$

where $\bar{L}_{i,j,\ell}(t, T_{i,0}) = \tilde{L}_{i,j,\ell}(t/k_{i,0}, T_{i,0})$ and $b_{i,j,\ell}^{(\lambda)} = \varphi_i^{-1}(\tilde{b}_{i,j,\ell}^{(\lambda)})$ for all $\lambda = 1, \ldots, r_i$.

set $L_{i,j,\ell}(t, S_t) = \tilde{L}_{i,j,\ell}(t, S_t^{k_{i,0}})$ and by Equations (6.15)and (6.16) we obtain

$$\begin{aligned} L_{i,j,\ell}\left(\frac{a_{i,j,\ell}}{\sigma_t^{\ell}(d_i)^j}\right) &= \sum_{\lambda=1}^{n} \Delta_{x_\lambda}\left(u_{i,j,\ell}^{(\lambda)}\right) + \frac{\tilde{L}_{i,j,\ell}(a_{i,j,\ell})}{\sigma_t^{\ell}(d_i)^j} \\ &= \sum_{\lambda=1}^{n} \Delta_{x_\lambda}\left(h_{i,j,\ell}^{(\lambda)}\right) \end{aligned} \tag{6.26}$$

for some $u_{i,j,\ell}^{(\lambda)}, h_{i,j,\ell}^{(\lambda)} \in \mathbb{K}(t,\mathbf{x})$.

let $L \in \mathbb{K}(t)\langle S_t\rangle$ be the LCLM of $L_{i,j,\ell}$ for all i, j, ℓ and write

$$L = R_{i,j,\ell} L_{i,j,\ell}.$$

update $g_\lambda = L(g_\lambda) + \sum_{i=1}^{I} \sum_{j=1}^{J_i} \sum_{\ell=1}^{s_{i,j}} R_{i,j,\ell}(h_{i,j,\ell}^{(\lambda)})$ for all $\lambda = 1, \ldots, n$.

return *L and $g_1, \ldots, g_n$.*

Example 6.13. *Let $\mathbb{K} = \mathbb{Q}$ and $f \in \mathbb{Q}(t, x, y, z)$. Consider the existence of telescoper of type $(\sigma_t; \sigma_x, \sigma_y, \sigma_z)$ for f. Let $G_t = \langle \sigma_t, \sigma_x, \sigma_y, \sigma_z\rangle$ and $G = \langle \sigma_x, \sigma_y, \sigma_z\rangle$.*

1. *For $f = \frac{1}{(t+1)(t+2z)d}$ with $d = (t - 3y + x)^2(t + y)(t + z) + 1$, we find a basis of the isotropy group $G_{t,d}$ is $\{\tau_0\}$, where $\tau_0 = \sigma_t \sigma_x^{-4} \sigma_y^{-1} \sigma_z^{-1}$. Then $G_{t,d}/G_d = \langle \bar{\tau}_0\rangle$. Since $\operatorname{rank}(G_{t,d}/G_d) = 1$ and $G_d = \{\mathbf{1}\}$ is a trivial group, we know from Theorem 6.7 that f has a telescoper of type $(\sigma_t; \sigma_x, \sigma_y, \sigma_z)$ if and only if there exists a nonzero operator $L_0 \in \mathbb{Q}(t)\langle T_0\rangle$ with $T_0 = S_t S_x^{-4} S_y^{-1} S_z^{-1}$ such that*

   $$L_0(a) = 0, \text{ where } a = fd = \frac{1}{(t+1)(t+2z)}.$$

   Note that the prime part of the denominator $b = (t + 1)(t + 2z)$ of a with respect to variables $\{x, y, z\}$ is $b_2 = t + 2z$ and $\tau_0(b_2) \neq b_2$. By Proposition 6.8, there does not exist any operator $L_0 \in \mathbb{Q}(t)\langle T_0\rangle$ such that $L_0(a) = 0$. So f does not have any telescoper of type $(\sigma_t; \sigma_x, \sigma_y, \sigma_z)$.

2. *For $f = \frac{1}{(t+1)d}$ with d being the same as in Example 6.13.1, it is easy to check that for $a = \frac{1}{t+1}$,*

$$L_0(a) = 0 \text{ with } L_0 = T_0 - \frac{t+1}{t+2}, \tag{6.27}$$

where $T_0 = S_t S_x^{-4} S_y^{-1} S_z^{-1}$. So by Theorem 6.7, f has a telescoper L of type $(\sigma_t; \sigma_x, \sigma_y, \sigma_z)$. In fact, we can take $L = S_t - \frac{t+1}{t+2}$. Then

$$\begin{aligned} L(f) &= \frac{\sigma_t(a)}{\sigma_t(d)} - \frac{t+1}{t+2} \cdot \frac{a}{d} = \frac{\sigma_t(a)}{\sigma_x^4 \sigma_y \sigma_z(d)} - \frac{t+1}{t+2} \cdot \frac{a}{d} \\ &= \Delta_x(u) + \Delta_y(v) + \Delta_z(w) + \underbrace{\frac{\tau_0(a) - ((t+1)/(t+2))a}{d}}_{=L_0(a)/d=0} \\ &= \Delta_x(u) + \Delta_y(v) + \Delta_z(w), \end{aligned}$$

where $u = \sum_{\ell=0}^{3} \frac{\sigma_t(a)}{\sigma_x^\ell \sigma_y \sigma_z(d)}$, $v = \frac{\sigma_t(a)}{\sigma_z(d)}$, and $w = \frac{\sigma_t(a)}{d}$. Additionally, this is a non-trivial example in two senses. Firstly, since $G_d = \{\mathbf{1}\}$, this rational function f is not $(\sigma_x, \sigma_y, \sigma_z)$-summable in $\mathbb{Q}(t, x, y, z)$. Secondly, for any $\{\mu, \nu\} \subset \{x, y, z\}$, since the isotropy group of d in $\langle \sigma_t, \sigma_\mu, \sigma_\nu \rangle$ is trivial and f is not (σ_μ, σ_ν)-summable, by Lemma 6.4, f does not have any telescoper in $\mathbb{Q}(t)\langle S_t \rangle$ of type $(\sigma_t; \sigma_\mu, \sigma_\nu)$.

3. *Continue the Example 6.3.2 and write f in the form*

$$f = \Delta_x(u_0) + \Delta_y(v_0) + \Delta_z(w_0) + r_1 + r_2,$$

where $u_0, v_0, w_0 \in \mathbb{Q}(t, x, y, z)$ and $r_1 = \frac{1}{t(t+y+2z)d}$, $r_2 = \frac{1}{(t+3z)\sigma_t(d)}$ with $d = 3y + (x+z)^2 + t$.

   (i) *For $r_1 = a_1/d$ with $a_1 = 1/(t(t+y+2z))$, we find a basis of $G_{t,d}$ is $\{\tau_0, \tau_1\}$, where $\tau_0 = \sigma_t^3 \sigma_y^{-1}$, $\tau_1 = \sigma_x \sigma_z^{-1}$. Then by Theorem 6.7, r_1 has a telescoper of type $(\sigma_t; \sigma_x, \sigma_y, \sigma_z)$ if and only if a_1 has a telescoper of type $(\tau_0; \tau_1)$. Choose one $\mathbb{Q}$-automorphism ϕ_1 of $\mathbb{Q}(t, x, y, z)$ given in Proposition 6.11 as follows*

$$\phi_1(h(t, x, y, z)) = h(3t, x, -t + y, -x + z),$$

   for any $h \in \mathbb{Q}(x, y, z)$. Then $\phi_1 \circ \tau_0 = \sigma_t \circ \phi_1$ and $\phi_1 \circ \tau_1 = \sigma_x \circ \phi_1$. So a_1 has a telescoper of type $(\tau_0; \tau_1)$ if and only if $\phi_1(a_1)$ has a telescoper of type $(\sigma_t; \sigma_x)$. A direct calculation yields that

$$\phi_1(a_1) = \frac{1}{3t\underbrace{(2t + y - 2x + 2z)}_{\tilde{d}}}.$$

   Again consider the isotropy group of $\tilde{d}$ in $\langle \sigma_t, \sigma_x \rangle$, which is generated by $\tilde{\tau}_0 = \sigma_t \sigma_x^2$. Since $(\tilde{\tau}_0 - \frac{t}{t+1})(\frac{1}{3t}) = 0$, by the similar argument as in Example 6.13.2, we see $\phi_1(a_1)$ has a telescoper $\tilde{L}_1 \in \mathbb{Q}(t)\langle S_t \rangle$ of type $(\sigma_t; \sigma_x)$ and in particular we find

$$\tilde{L}_1(t, S_t)(\phi_1(a_1)) = \Delta_x(\tilde{b}_1) \tag{6.28}$$

   with $\tilde{L}_1 = S_t - \frac{t}{t+1}$, $\tilde{b}_1 = -\frac{1}{3(t+1)(2t+y-2x+2+2z)}$. So by Theorem 6.7, r_1 has a telescoper $L \in \mathbb{Q}(t)\langle S_t \rangle$ of type $(\sigma_t; \sigma_x, \sigma_y, \sigma_z)$. In fact, we can find an explicit expression for L. Applying ϕ_1^{-1} to Equation (6.28) yields that

$$\bar{L}_1(t, T_0)(a_1) = \Delta_{\tau_1}(b_1),$$

where $T_0 = S_t^3 S_y^{-1}$, $\bar{L}_1(t, T_0) = \tilde{L}_1(\frac{t}{3}, T_0) = T_0 - \frac{t}{t+3}$, $b_1 = \phi_1^{-1}(\tilde{b}_1) = -\frac{1}{(t+3)(t+y+2z+2)}$. *Let* $L_1(t, S_t) = \bar{L}_1(t, S_t^3) = S_t^3 - \frac{t}{t+3}$. *Then we have*

$$L_1(r_1) = \frac{\sigma_t^3(a_1)}{\sigma_t^3(d)} - \frac{t}{t+3} \cdot \frac{a_1}{d} = \frac{\sigma_t^3(a_1)}{\sigma_y(d)} - \frac{t}{t+3} \cdot \frac{a_1}{d}$$
$$= \Delta_x(0) + \Delta_y(v_1) + \Delta_z(0) + \frac{\bar{L}_1(a_1)}{d} \text{ with } v_1 = \frac{\sigma_t^3 \sigma_y^{-1}(a_1)}{d}$$

and using Formula 5.7 with $\tau = \tau_1$*, we get*

$$\frac{\bar{L}_1(a_1)}{d} = \Delta_{\tau_1}\left(\frac{b_1}{d}\right) = \Delta_x(u_1) + \Delta_y(0) + \Delta_z(w_1)$$

with $u_1 = \sigma_z^{-1}\left(\frac{b_1}{d}\right)$ *and* $w_1 = -\sigma_z^{-1}\left(\frac{b_1}{d}\right)$. *Hence* L_1 *is a telescoper of type* $(\sigma_t; \sigma_x, \sigma_y, \sigma_z)$ *for* r_1 *and*

$$L_1(r_1) = \Delta_x(u_1) + \Delta_y(v_1) + \Delta_z(w_1). \tag{6.29}$$

(ii) Similarly, for $r_2 = a_2/\sigma_t(d)$ *with* $a_2 = 1/(t+3z)$*, applying the algorithm* IsTelescoperable *to* r_2*, the result is true and we obtain*

$$L_2(r_2) = \Delta_x(u_2) + \Delta_y(v_2) + \Delta_z(w_2), \tag{6.30}$$

where $L_2 = S_t^3 - 1$, $u_2 = \sigma_z^{-1}\left(\frac{b_2}{\sigma_t(d)}\right)$, $v_2 = \frac{\sigma_t^3\sigma_y^{-1}(a_2)}{\sigma_t(d)}$ *and* $w_2 = -\sigma_z^{-1}\left(\frac{b_2}{\sigma_t(d)}\right)$ *with* $b_2 = -\frac{1}{t+3z+3}$.

(iii) For $r = r_1 + r_2$*, using LCLM algorithm to compute the least common multiple* L *of* L_1, L_2 *in* $\mathbb{Q}(t)\langle S_t\rangle$*, we obtain*

$$L = R_1 L_1 = R_2 L_2 = S_t^6 - \frac{2(t+3)}{t+6} S_t^3 + \frac{t}{t+6}$$

with $R_1 = S_t^3 - \frac{t+3}{t+6}$ *and* $R_2 = S_t^3 - \frac{t}{t+6}$. *Then*

$$L(r) = \Delta_x(u) + \Delta_y(v) + \Delta_z(w),$$

where $u = \sum_{i=1}^2 R_i(u_i)$, $v = \sum_{i=1}^2 R_i(v_i)$ *and* $u = \sum_{i=1}^2 R_i(w_i)$ *are rational functions in* $\mathbb{Q}(t, x, y, z)$. *Updating* $u = u + L(u_0)$, $v = v + L(v_0)$ *and* $w = w + L(w_0)$*, we get*

$$L(f) = \Delta_x(u) + \Delta_y(v) + \Delta_z(w).$$

So L *is a telescoper of type* $(\sigma_t; \sigma_x, \sigma_y, \sigma_z)$ *for* f.

References

[1] Sergei A. Abramov. On the summation of rational functions. *USSR Computational Mathematics and Mathematical Physics*, 11(4):324–330, 1971.

[2] Sergei A. Abramov. The rational component of the solution of a first order linear recurrence relation with rational right hand side. *Ž. Vyčisl. Mat. i Mat. Fiz.*, 15(4):1035–1039, 1090, 1975.

[3] Sergei A. Abramov. Indefinite sums of rational functions. In *ISSAC '95: Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation*, pages 303–308, New York, NY, USA, 1995. ACM.

[4] Sergei A. Abramov. Rational solutions of linear difference and q-difference equations with polynomial coefficients. In *ISSAC '95: Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation*, pages 285–289, New York, NY, USA, 1995. ACM.

[5] Sergei A. Abramov. When does Zeilberger's algorithm succeed? *Adv. in Appl. Math.*, 30(3):424–441, 2003.

[6] Sergei A. Abramov and Ha Quang Le. A criterion for the applicability of Zeilberger's algorithm to rational functions. *Discrete Math.*, 259(1-3):1–17, 2002.

[7] Sergei A. Abramov, Ha Quang Le, and Ziming Li. Univariate ore polynomial rings in computer algebra. *J. of Mathematical Sci.*, 131(5):5885–5903, 2005.

[8] Sergei A. Abramov and Mark van Hoeij. A method for the integration of solutions of ore equations. In *ISSAC '97: Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*, pages 172–175, New York, NY, USA, 1997. ACM.

[9] George E. Andrews and Peter Paule. Some questions concerning computer-generated proofs of a binomial double-sum identity. *J. Symbolic Comput.*, 16(2):147–151, August 1993.

[10] J. Marshall Ash and Stefan Catoiu. Telescoping, rational-valued series, and zeta functions. *Transactions of the American Mathematical Society*, 357(8):3339–3358, 2005.

[11] Joseph Bernšteĭn. Modules over a ring of differential operators. An investigation of the fundamental solutions of equations with constant coefficients. *Funkcional. Anal. i Priložen.*, 5(2):1–16, 1971.

[12] Jérémy Berthomieu, Jean-Charles Faugère, and Ludovic Perret. Polynomial-time algorithms for quadratic isomorphism of polynomials: the regular case. *J. Complexity*, 31(4):590–616, 2015.

[13] Johannes Blümlein, Sebastian Klein, Carsten Schneider, and Flavia Stan. A symbolic summation approach to Feynman integral calculus. *J. Symbolic Comput.*, 47(10):1267–1289, 2012.

[14] Charles Bouillaguet, Pierre-Alain Fouque, and Amandine Véber. Graph-theoretic algorithms for the "isomorphism of polynomials" problem. In *Advances in cryptology—EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Comput. Sci.*, pages 211–227. Springer, Heidelberg, 2013.

[15] Peter Bürgisser, Michael Clausen, and M. Amin Shokrollahi. *Algebraic complexity theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1997. With the collaboration of Thomas Lickteig.

[16] Shaoshi Chen, Frédéric Chyzak, Ruyong Feng, Guofeng Fu, and Ziming Li. On the existence of telescopers for mixed hypergeometric terms. *J. Symbolic Comput.*, 68:1–26, 2015.

[17] Shaoshi Chen, Lixin Du, Rong-Hua Wang, and Chaochao Zhu. On the existence of telescopers for rational functions in three variables. *Journal of Symbolic Computation*, 104:494–522, 2021.

[18] Shaoshi Chen, Lixin Du, and Chaochao Zhu. Existence problem of telescopers for rational functions in three variables: The mixed cases. In *Proceedings of the 2019 on International Symposium on Symbolic and Algebraic Computation*, ISSAC '19, pages 82–89, New York, NY, USA, 2019. ACM.

[19] Shaoshi Chen, Qing-Hu Hou, George Labahn, and Rong-Hua Wang. Existence problem of telescopers: beyond the bivariate case. In *ISSAC '16: Proceedings of the 2016 on International Symposium on Symbolic and Algebraic Computation*, pages 167–174, New York, NY, USA, 2016. ACM.

[20] Shaoshi Chen and Michael F. Singer. Residues and telescopers for bivariate rational functions. *Adv. Appl. Math.*, 49(2):111–133, August 2012.

[21] Shaoshi Chen and Michael F. Singer. On the summability of bivariate rational functions. *J. of Algebra*, 409:320–343, 2014.

[22] William Y. C. Chen, Qing-Hu Hou, and Yan-Ping Mu. Applicability of the q-analogue of Zeilberger's algorithm. *J. Symbolic Comput.*, 39(2):155–170, 2005.

[23] William Y. C. Chen, Qing-Hu Hou, and Yan-Ping Mu. A telescoping method for double summations. *J. Comput. Appl. Math.*, 196(2):553–566, 2006.

[24] Xi Chen, Neeraj Kayal, and Avi Wigderson. Partial derivatives in arithmetic complexity and beyond. *Found. Trends Theor. Comput. Sci.*, 6(1-2):front matter, 1–138 (2011), 2010.

[25] Zeev Dvir, Rafael Mendes de Oliveira, and Amir Shpilka. Testing equivalence of polynomials under shifts. In *Automata, languages, and programming. Part I*, volume 8572 of *Lecture Notes in Comput. Sci.*, pages 417–428. Springer, 2014.

[26] Zeev Dvir, Rafael Mendes de Oliveira, and Amir Shpilka. Testing equivalence of polynomials under shifts. *Electron. Colloquium Comput. Complex*, 21:3, 2014.

[27] Jean-Charles Faugère and Ludovic Perret. Polynomial equivalence problems: algorithmic and theoretical aspects. In *Advances in cryptology—EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Comput. Sci.*, pages 30–47. Springer, Berlin, 2006.

[28] Keith O. Geddes, Stephanie R. Czapor, and George Labahn. *Algorithms for Computer Algebra*. Kluwer Academic Publishers, Boston, MA, 1992.

[29] Ralph William Gosper, Jr. Decision procedure for indefinite hypergeometric summation. *Proc. Nat. Acad. Sci. U.S.A.*, 75(1):40–42, 1978.

[30] Dima Grigoriev and Marek Karpinski. A zero-test and an interpolation algorithm for the shifted sparse polynominals. In Gérard D. Cohen, Teo Mora, and Oscar Moreno, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 10th International Symposium, AAECC-10, San Juan de Puerto Rico, Puerto Rico, May 10-14, 1993, Proceedings*, volume 673 of *Lecture Notes in Computer Science*, pages 162–169. Springer, 1993.

[31] Dima Yu. Grigoriev and Lakshman Y. N. Algorithms for computing sparse shifts for multivariate polynomials. In A. H. M. Levelt, editor, *ISSAC '95: Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation: July 10–12, 1995, Montréal, Canada*, ISSAC -PROCEEDINGS- 1995, pages 96–103, pub-ACM:adr, 1995. ACM Press.

[32] Dmitry Grigoriev. Testing shift-equivalence of polynomials using quantum machines. In *ISSAC '96: Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation*, pages 49–54, New York, NY, USA, 1996. ACM.

[33] Dmitry Grigoriev. Testing shift-equivalence of polynomials by deterministic, probabilistic and quantum machines. *Theoret. Comput. Sci.*, 180(1-2):217–228, 1997.

[34] Joshua A. Grochow, Youming Qiao, and Gang Tang. Average-case algorithms for testing isomorphism of polynomials, algebras, and multilinear forms. In *38th International Symposium on Theoretical Aspects of Computer Science*, volume 187 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages Art. No. 38, 17. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2021.

[35] Charlotte Hardouin and Michael F. Singer. Differential Galois theory of linear difference equations. *Math. Ann.*, 342(2):333–377, 2008.

[36] Qing-Hu Hou and Rong-Hua Wang. An algorithm for deciding the summability of bivariate rational functions. *Adv. in Appl. Math.*, 64:31–49, 2015.

[37] Ravindran Kannan and Achim Bachem. Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix. *SIAM J. Comput.*, 8(4):499–507, 1979.

[38] Michael Karr. Summation in finite terms. *J. Assoc. Comput. Mach.*, 28(2):305–350, 1981.

[39] Michael Karr. Theory of summation in finite terms. *J. Symbolic Comput.*, 1(3):303–315, 1985.

[40] Manuel Kauers and Carsten Schneider. Partial denominator bounds for partial linear difference equations. page 211–218, 2010.

[41] Neeraj Kayal. Algorithms for arithmetic circuits. *Electron. Colloquium Comput. Complex*, 17:73, 2010.

[42] Neeraj Kayal. Affine projections of polynomials [extended abstract]. In *STOC'12—Proceedings of the 2012 ACM Symposium on Theory of Computing*, pages 643–661. ACM, New York, 2012.

[43] Donald E. Knuth. *The art of computer programming. Vol. 2*. Addison-Wesley, Reading, MA, 1998. Seminumerical algorithms, Third edition [of MR0286318].

[44] Y. N. Lakshman and B. David Saunders. On computing sparse shifts for univariate polynomials. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, ISSAC '94, page 108–113, New York, NY, USA, 1994. Association for Computing Machinery.

[45] Y. N. Lakshman and B. David Saunders. Sparse shifts for univariate polynomials. *Appl. Algebra Engrg. Comm. Comput.*, 7(5):351–364, 1996.

[46] Laura Felicia Matusevich. Rational summation of rational functions. *Beiträge zur Algebra und Geometrie*, 41:531–536, 2000.

[47] Jacques Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two new families of asymmetric algorithms. In Ueli Maurer, editor, *Advances in Cryptology — EUROCRYPT '96*, pages 33–48, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg.

[48] Peter Paule. Greatest factorial factorization and symbolic summation. *J. Symbolic Comput.*, 20(3):235–268, 1995.

[49] Marko Petkovšek, Herbert S. Wilf, and Doron Zeilberger. $A = B$. A. K. Peters Ltd., Wellesley, MA, 1996. With a foreword by Donald E. Knuth.

[50] Roberto Pirastu and Volker Strehl. Rational summation and Gosper-Petkovšek representation. *J. Symbolic Comput.*, 20(5-6):617–635, 1995. Symbolic computation in combinatorics (Ithaca, NY, 1993).

[51] Mikio Sato. Theory of prehomogeneous vector spaces (algebraic part)—the English translation of Sato's lecture from Shintani's note. *Nagoya Math. J.*, 120:1–34, 1990. Notes by Takuro Shintani, Translated from the Japanese by Masakazu Muro.

[52] Nitin Saxena. Progress on polynomial identity testing. *Bull. Eur. Assoc. Theor. Comput. Sci. EATCS*, (99):49–79, 2009.

[53] Nitin Saxena. Progress on polynomial identity testing-II. In *Perspectives in computational complexity*, volume 26 of *Progr. Comput. Sci. Appl. Logic*, pages 131–146. Birkhäuser/Springer, Cham, 2014.

[54] Carsten Schneider. *Symbolic Summation in Difference Fields*. PhD thesis, J. Kepler University Linz, 2001.

[55] Carsten Schneider. Symbolic summation assists combinatorics. *Sém. Lothar. Combin.*, 56:Art. B56b, 36, 2006/07.

[56] Carsten Schneider. Parameterized telescoping proves algebraic independence of sums. *Ann. Comb.*, 14(4):533–552, 2010.

[57] Carsten Schneider and Johannes Blümlein, editors. *Computer algebra in quantum field theory*. Texts and Monographs in Symbolic Computation. Springer, Vienna, 2013. Integration, summation and special functions.

[58] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, 1980, October.

[59] Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Foundations and Trends® in Theoretical Computer Science*, 5(3–4):207–388, 2010.

[60] Volker Strassen. Algebraic complexity theory. In *Handbook of theoretical computer science, Vol. A*, pages 633–672. Elsevier, Amsterdam, 1990.

[61] Joachim von zur Gathen. Algebraic complexity theory. In *Annual review of computer science, Vol. 3*, pages 317–347. Annual Reviews, Palo Alto, CA, 1988.

[62] Joachim von zur Gathen and Gerhard Jürgen. *Modern Computer Algebra*. Cambridge University Press, Cambridge, second edition, 2003.

[63] Herbert S. Wilf and Doron Zeilberger. Rational functions certify combinatorial identities. *J. Amer. Math. Soc.*, 3(1):147–158, 1990.

[64] Herbert S. Wilf and Doron Zeilberger. An algorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities. *Invent. Math.*, 108(3):575–633, 1992.

[65] Doron Zeilberger. A holonomic systems approach to special functions identities. *J. Comput. Appl. Math.*, 32:321–368, 1990.

[66] Doron Zeilberger. The method of creative telescoping. *J. Symbolic Comput.*, 11(3):195–204, 1991.

[67] R. Zippel. Probabilistic algorithms for sparse polynomials. In *ISSAC '79: Proc. Int'l. Symp. on Symbolic and Algebraic Computation,* Lecture Notes in Computer Science, Vol. 72. Springer-Verlag, 1979. Zippel discusses probabilistic methods for testing polynomial identities and properties of systems of polynomials.

[68] Richard Zippel. *Effective polynomial computation.* Kluwer Academic Publishers, Boston-Dordrecht-London, 1993.