A Refined Denominator Bounding Algorithm for Multivariate Linear Difference Equations

Manuel Kauers*
RISC
Johannes Kepler University
4040 Linz (Austria)
mkauers@risc.jku.at

Carsten Schneider†
RISC
Johannes Kepler University
4040 Linz (Austria)
cschneid@risc.jku.at

ABSTRACT

We continue to investigate which polynomials can possibly occur as factors in the denominators of rational solutions of a given partial linear difference equation. In an earlier article we have introduced the distinction between periodic and aperiodic factors in the denominator, and we have given an algorithm for predicting the aperiodic ones. Now we extend this technique towards the periodic case and present a refined algorithm which also finds most of the periodic factors.

Categories and Subject Descriptors

I.1.2 [**Computing Methodologies**]: Symbolic and Algebraic Manipulation—*Algorithms*

General Terms

Algorithms

Keywords

Difference Equations, Rational Solutions

1. INTRODUCTION

The usual approach for finding rational solutions of linear difference equations with polynomial coefficients is as follows. First one constructs a nonzero polynomial Q such that for any solution $y = p/q$ of the given equation (p, q coprime) we must have $q \mid Q$. Such a polynomial Q is called a denominator bound for the equation. Next, the denominator bound is used to transform the given equation into a new equation with the property that a polynomial P solves the new equation if and only if the rational function $y = P/Q$ solves the original equation. Thus the knowledge of a denominator bound reduces rational solving to polynomial solving.

The first algorithm for finding a denominator bound Q was given by Abramov in 1971 [1, 2, 5]. During the past forty years, other algorithms were found [14, 11, 7, 9, 4] and the technique was generalized to matrix equations [3, 6] as well as to equation over function fields [15, 8, 16]. Last year [12] we made a first step towards a denominator bounding algorithm for equations in several variables (PLDEs). We found that some factors of the denominator are easier to predict than others. We called a polynomial periodic if it has a nontrivial gcd with one of its shifts, and aperiodic otherwise. For example, the polynomial $2n - 3k$ is periodic because shifting it twice in k and three times in n leaves it fixed. We say that it is periodic in direction $(3, 2)$. An example for an aperiodic polynomial is $nk + 1$. The main result of last year's paper was an algorithm for determining aperiodic denominator bounds for PLDEs, i.e., we can find Q such that whenever $y = \frac{p}{uq}$ solves the given equation, p and q are coprime, and q is aperiodic, then $q \mid Q$.

The present paper is a continuation of this work. We now turn to periodic factors and study under which circumstances a slightly adapted version of last year's algorithm can also predict periodic factors of the denominator. We propose an algorithm which finds the periodic factors for almost all directions. Every equation has however some directions which our algorithm does not cover. But if, for instance, we have a system of two equations and apply our algorithm to each of them, then the two bounds can under favorable circumstances (which can be detected algorithmically) be combined to a denominator bound which provably contains all the factors that can possibly occur in the denominator of any solution of the system. This was not possible before. So while until now we were just able to compute in all situations some factors, we can now also find in some situations all factors.

Despite this progress, we must confess that our results are still of a somewhat academic nature because denominator bounds in which some factors are missing are not really enough for solving equations. And even when a full denominator bound is known, it still remains to find the polynomial solutions of a PLDE, and nobody knows how to do this—the corresponding problem for differential equations is undecidable. But in practice, we can heuristically choose a degree bound for finding polynomial solutions, and knowing parts of the possible denominators is certainly better than knowing nothing, and the more factors we know, the better. Apart

*Supported by the Austrian FWF grant Y464-N18 and the EU grant PITN-GA-2010-264564.

†Supported by the Austrian FWF grant P20347-N18 and the EU grant PITN-GA-2010-264564.

ISSAC'11, June 8–11, 2011, San Jose, California, USA.

from this, we find it interesting to see how far the classical univariate techniques carry in the multivariate setting, and we would be curious to see new ideas leading towards algorithms which also find the factors that we still miss.

2. PREPARATIONS

Let $\mathbb{K}$ be a field of characteristic zero. We consider polynomials and rational functions in the r variables $n_1, \ldots, n_r$ with coefficients in $\mathbb{K}$. For each variable n_i, let N_i denote the shift operator mapping n_i to $n_i + 1$ and leaving all other variables fixed, so that

$$N_i q(n_1, \ldots, n_r) = q(n_1, \ldots, n_{i-1}, n_i + 1, n_{i+1}, \ldots, n_r)$$

for every rational function q. Whenever it seems appropriate, we will use multiindex notation, writing for instance $\mathbf{n}$ instead of $n_1, \ldots, n_r$ or $N^{\mathbf{i}}$ for $N_1^{i_1} N_2^{i_2} \cdots N_r^{i_r}$.

We consider equations of the form

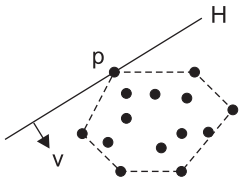
$$\sum_{\mathbf{s} \in S} a_{\mathbf{s}} N^{\mathbf{s}} y = f \tag{1}$$

where $S \subseteq \mathbb{Z}^r$ is finite and nonempty, $f \in \mathbb{K}[\mathbf{n}]$ and $a_{\mathbf{s}} \in \mathbb{K}[\mathbf{n}] \setminus \{0\}$ $(\mathbf{s} \in S)$ are given, and y is an unknown rational function. The set S is called the *support* of the equation. Our goal is to determine the polynomials $p \in \mathbb{K}[\mathbf{n}]$ which may possibly occur in the denominator of a solution y, or at least to find many factors of p.

We recall the following definitions and results from our previous paper [12]. By convention, we understand that gcds are monic, so that saying "$\gcd(u, v) = 1$" is the same as saying "u and v are coprime". Also by convention, when writing a rational function $y \in \mathbb{K}(\mathbf{n})$ as a quotient $y = p/q$, we mean to say that p and q are in $\mathbb{K}[\mathbf{n}]$ and $\gcd(p, q) = 1$.

Definition 1. *Let $p, q, d \in \mathbb{K}[\mathbf{n}]$.*

1. *The set* $\mathrm{Spread}(p, q) := \{\, \mathbf{i} \in \mathbb{Z}^r : \gcd(p, N^{\mathbf{i}} q) \neq 1 \,\}$ *is called the* spread *of p and q. For short, we write* $\mathrm{Spread}(p) := \mathrm{Spread}(p, p)$.
2. *The number* $\mathrm{Disp}_k(p, q) := \max\{\, |i_k| : (i_1, \ldots, i_r) \in \mathrm{Spread}(p, q) \,\}$ *is called the* dispersion *of p and q with respect to $k \in \{1, \ldots, r\}$. (We set $\max A := -\infty$ if A is empty and $\max A := \infty$ if A is unbounded.)*
3. *The polynomial p is called* aperiodic *if* $\mathrm{Spread}(p)$ *is finite, and* periodic *otherwise.*
4. *The polynomial d is called an* aperiodic denominator bound *for equation (1) if $d \neq 0$ and every solution y can be written as $\frac{a}{ub}$ for some $a, b, u \in \mathbb{K}[\mathbf{n}]$ where u is periodic and $b \mid d$.*
5. *A point $\mathbf{p} \in S \subseteq \mathbb{Z}^r \subseteq \mathbb{R}^r$ is called a* corner point *of S if there exists a vector $\mathbf{v} \in \mathbb{R}^r$ such that $(\mathbf{s} - \mathbf{p}) \cdot \mathbf{v} > 0$ for all $\mathbf{s} \in S \setminus \{\mathbf{p}\}$. Such a vector $\mathbf{v}$ is then called an* inner vector, *and the affine hyperplane $H := \{\mathbf{x} \in \mathbb{R}^r : (\mathbf{x} - \mathbf{p}) \cdot \mathbf{v} = 0\}$ is called a* border plane *for S.*



In the univariate case ($r = 1$), slightly different definitions are circulating in the literature. Our "denominator bound" corresponds most closely to what Abramov [1] calls "universal denominator" and to the reciprocal of what van Hoeij [11] calls a rational function which "bounds the denominator".

Theorem 1. *Let $p, q \in \mathbb{K}[\mathbf{n}]$.*

1. *If p is irreducible, then* $\mathrm{Spread}(p)$ *is a submodule of $\mathbb{Z}^r$ and p is aperiodic if and only if* $\mathrm{Spread}(p) = \{0\}$.
2. *If p and q are irreducible, then there exists $\mathbf{s} \in \mathbb{Z}^r$ such that $\mathbf{s} + \mathrm{Spread}(p, q)$ is a submodule of $\mathbb{Z}^r$. This submodule has the property that whenever $m \in \mathbb{Z} \setminus \{0\}$ and $\mathbf{y} \in \mathbb{Z}^r$ are such that the module contains $m\mathbf{y}$, then it also contains $\mathbf{y}$.*
3. $\mathrm{Spread}(p, q) = \bigcup_{u,v} \mathrm{Spread}(u, v)$, *where the union is taken over all pairs (u, v) where u is a monic irreducible factor of p and v is a monic irreducible factor of q.*
4. *There is an algorithm for computing* $\mathrm{Spread}(p, q)$.
5. *There is an algorithm for computing an aperiodic denominator bound for (1) given the support S and the coefficients $a_{\mathbf{s}}$ $(\mathbf{s} \in S)$.*

Throughout the rest of this paper, we will only consider submodules $M \subseteq \mathbb{Z}^r$ with the property quoted in Thm. 1.2: if $m \in \mathbb{Z} \setminus \{0\}$ and $\mathbf{y} \in \mathbb{Z}^r$ are such that $m\mathbf{y} \in M$, then also $\mathbf{y} \in M$. For lack of better names, let us call these submodules *good*. Note that a submodule $M \subseteq \mathbb{Z}^r$ is good if and only if $\mathbb{Z}^r / M$ is torsion free.

3. DENOMINATOR BOUNDS MODULO A PRESCRIBED MODULE

Our goal in this section is to determine the factors whose spread is contained in some prescribed set $W \subseteq \mathbb{Z}^r$. Under suitable assumptions about W such factors must pop up in the coefficients of the equation (cf. Lemma 2 below) and under stronger assumptions we can also give a bound on the dispersion between them (cf. Theorem 2 below). Using these two results we obtain a denominator bound relative to W (cf. Theorem 3 and Algorithm 1) below. In the next section, we then propose an algorithm which combines the denominator bounds with respect to several sets W. It turns out that by considering only finitely many sets W one can obtain a denominator bound with respect to infinitely many sets W.

Definition 2. *Let $W \subseteq \mathbb{Z}^r$ with $0 \in W$. A polynomial $d \in \mathbb{K}[\mathbf{n}] \setminus \{0\}$ is called a denominator bound of (1) with respect to W if for every solution $y = p/q \in \mathbb{K}(\mathbf{n})$ of (1) and every irreducible factor u of q with multiplicity $m \in \mathbb{N}$ such that* $\mathrm{Spread}(u) \subseteq W$ *we have $u^m \mid d$.*

Typically, W will be a good submodule of $\mathbb{Z}^r$ or a finite union of such modules. The definition reduces to the notion of aperiodic denominator bound when $W = \{0\}$. In the other extreme, when $W = \mathbb{Z}^r$ then d is a "complete" denominator bound: it contains all the factors, periodic or not, that can possibly occur in the denominator of a solution y of (1). In general, d predicts all aperiodic factors in the denominator of a solution as well as the periodic factors whose spread is contained in W.

Denominator bounds with respect to different submodules can be combined as follows.

LEMMA 1. *Let $W_1, \dots, W_m$ be good submodules of $\mathbb{Z}^r$, and let $d_1, \dots, d_m$ be denominator bounds of (1) with respect to $W_1, \dots, W_m$, respectively. Then $d := \operatorname{lcm}(d_1, \dots, d_m)$ is a denominator bound with respect to $W := W_1 \cup \dots \cup W_m$.*

PROOF. Let u be an irreducible factor of the denominator of some solution of (1) and suppose that $U := \operatorname{Spread}(u) \subseteq W$. It suffices to show that then $U \subseteq W_k$ for some k, because then it follows that $u \mid d_k \mid d$, as desired.

We show that if U contains some vector $\mathbf{x} \notin W_1$, then $U \subseteq W_2 \cup \dots \cup W_m$. Applying the argument repeatedly proves that $U \subseteq W_k$ for some k.

If $U \cap W_1 = \{0\}$, then $U \subseteq W_2 \cup \dots \cup W_m$ is obvious. If not, let $\mathbf{y} \in U \cap W_1$ be a nonzero vector. We show that $\mathbf{y} \in W_2 \cup \dots \cup W_m$. Since U is a submodule of $\mathbb{Z}^r$, we have $\mathbf{x} + \alpha\mathbf{y} \in U$ for all $\alpha \in \mathbb{Z}$. By assumption $U \subseteq W_1 \cup \dots \cup W_m$, so each such $\mathbf{x} + \alpha\mathbf{y}$ must belong to at least one module W_ℓ ($\ell = 1, \dots, m$). It cannot belong to W_1 though, because together with $\mathbf{y} \in W_1$ this would imply $\mathbf{x} \in W_1$, which is not the case. Therefore: For every $\alpha \in \mathbb{Z}$ there exists $\ell \in \{2, \dots, m\}$ such that $\mathbf{x} + \alpha\mathbf{y} \in W_\ell$.

Since $\mathbb{Z}$ is infinite and m is finite, there must be some index $\ell \in \{2, \dots, m\}$ for which there are two different $\alpha_1, \alpha_2 \in \mathbb{Z}$ with $\mathbf{x} + \alpha_1\mathbf{y} \in W_\ell$ and $\mathbf{x} + \alpha_2\mathbf{y} \in W_\ell$. Since W_ℓ is also a submodule of $\mathbb{Z}^r$, it follows that $(\alpha_1 - \alpha_2)\mathbf{y} \in W_\ell$, and finally, because W_ℓ is good, $\mathbf{y} \in W_\ell \subseteq W_2 \cup \dots \cup W_m$, as claimed. □

The next result says that factors of denominators tend to leave traces in the coefficients of corner points of S.

LEMMA 2. *Let $y = p/q$ be a solution of (1), and let u be a monic irreducible factor of q. Let $\mathbf{p} \in S$ be a corner point of S with an inner vector $\mathbf{v} \in \mathbb{R}^r$ orthogonal to $\operatorname{Spread}(u)$ (meaning $\mathbf{w} \cdot \mathbf{v} = 0$ for all $\mathbf{w}$ in $\operatorname{Spread}(u)$). Then there exists $\mathbf{i} \in \mathbb{Z}^r$ such that $N^{\mathbf{i}}u \mid a_{\mathbf{p}}$.*

PROOF. Let $u_1, \dots, u_m$ be all the distinct monic irreducible factors of q with $\operatorname{Spread}(u, u_k) \neq 0$. Let $\mathbf{c}_k \in \operatorname{Spread}(u, u_k)$ for $k = 1, \dots, m$. Then $\gcd(u, N^{\mathbf{c}_k}u_k) \neq 1$, and therefore, since u and u_k are monic and irreducible, $u = N^{\mathbf{c}_k}u_k$ and $u_k = N^{-\mathbf{c}_k}u$.

For every $\mathbf{i} \in \mathbb{Z}^r$ we have

$$\begin{aligned}
\mathbf{i} \in \operatorname{Spread}(u, u_k) &\iff \gcd(u, N^{\mathbf{i}}u_k) \neq 1 \\
&\iff u = N^{\mathbf{i}}u_k \\
&\iff N^{\mathbf{i}-\mathbf{c}_k}u = u \\
&\iff \mathbf{i} - \mathbf{c}_k \in \operatorname{Spread}(u) \\
&\iff \mathbf{i} \in c_k + \operatorname{Spread}(u).
\end{aligned}$$

It follows that $\operatorname{Spread}(u, u_k) = \mathbf{c}_k + \operatorname{Spread}(u)$, and with Thm. 1.3 that

$$\operatorname{Spread}(u, q) = \bigcup_{k=1}^{m} (\mathbf{c}_k + \operatorname{Spread}(u)) = C + \operatorname{Spread}(u)$$

where $C = \{\mathbf{c}_1, \dots, \mathbf{c}_m\} \subseteq \operatorname{Spread}(u, q)$.

Let $k \in \{1, \dots, m\}$ be such that $\mathbf{v} \cdot \mathbf{c}_k$ is maximal. Rewrite (1) as

$$a_{\mathbf{p}}N^{\mathbf{p}}y = f - \sum_{\mathbf{s} \in S \setminus \{\mathbf{p}\}} a_{\mathbf{s}}N^{\mathbf{s}}y.$$

Because of $N^{-\mathbf{c}_k}u = u_k$, the factor $N^{\mathbf{p}-\mathbf{c}_k}u = N^{\mathbf{p}}u_k$ appears in the denominator of $N^{\mathbf{p}}y$. Suppose that it also appears in the denominator of some $N^{\mathbf{s}}y$ on the right hand side. Then

$$N^{\mathbf{p}-\mathbf{c}_k}u = N^{\mathbf{s}}u_j = N^{\mathbf{s}-\mathbf{c}_j}u$$

for some $j \in \{1, \dots, m\}$, hence $\mathbf{s} - \mathbf{p} + \mathbf{c}_k - \mathbf{c}_j \in \operatorname{Spread}(u)$. As $\mathbf{v}$ is orthogonal to $\operatorname{Spread}(u)$ by assumption, we have $\mathbf{v} \cdot (\mathbf{s} - \mathbf{p} + \mathbf{c}_k - \mathbf{c}_j) = 0$. On the other hand, $\mathbf{v} \cdot (\mathbf{s} - \mathbf{p}) > 0$, because $\mathbf{p}$ is a corner point of S with inner vector $\mathbf{v}$, and $\mathbf{v} \cdot \mathbf{c}_k \geq \mathbf{v} \cdot \mathbf{c}_j$ by the choice of k, so $\mathbf{v} \cdot (\mathbf{s} - \mathbf{p} + \mathbf{c}_k - \mathbf{c}_j) = \mathbf{v} \cdot (\mathbf{s} - \mathbf{p}) + \mathbf{v} \cdot \mathbf{c}_k - \mathbf{v} \cdot \mathbf{c}_j > 0$, a contradiction. It follows that $N^{\mathbf{p}-\mathbf{c}_k}u$ cannot appear in the denominator of $N^{\mathbf{s}}y$ for any $\mathbf{s} \in S \setminus \{\mathbf{p}\}$, therefore $N^{\mathbf{p}-\mathbf{c}_k}u \mid a_{\mathbf{p}}$. The claim follows with $\mathbf{i} = \mathbf{p} - \mathbf{c}_k$. □

The lemma tells us for which choices of $W \subseteq \mathbb{Z}^r$ something nontrivial may happen. Let us illustrate this with an example.

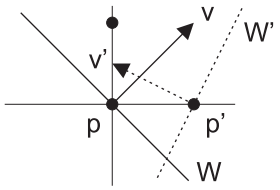
EXAMPLE 1. *The equation*

$$\begin{aligned}
&(4k - 2n + 1)(k + n + 1)y(n, k) \\
&\quad + (8k^2 + 2kn + k + 6n^2 + 13n + 6)y(n, k + 1) \\
&\quad - 2(6k^2 + 2kn + 13k + 2n^2 + n + 6)y(n + 1, k) = 0
\end{aligned}$$

has the solution $y = (n^2 + 2k^2)/(k + n + 1)$. Its denominator is periodic, $\operatorname{Spread}(k + n + 1) = \binom{1}{-1}\mathbb{Z}$. Lemma 2 predicts the appearance of $u := k + n + 1$ (or at least some shifted version of it) in the coefficient of $y(n, k)$, because for the choice $W := \operatorname{Spread}(u) = \binom{1}{-1}\mathbb{Z}$, the point $\mathbf{p} = \binom{0}{0} \in S$ admits the choice $\mathbf{v} = \binom{1}{1}$ in accordance with the requirements imposed by the lemma. Note that no factor of the form $N^iK^j(k+n+1)$ occurs in the coefficients of $y(n, k+1)$ or $y(n+1, k)$, which does not contradict the lemma, because the points $\binom{0}{1}$ and $\binom{1}{0}$ lie on a line parallel to W (meaning $\binom{0}{1} - \binom{1}{0} = \binom{-1}{1} \in W$). This has the consequence that for these points, there does not exist a vector $\mathbf{v}$ with the required property.

Conversely, the factor $u' := 4k - 2n + 1$ cannot possibly appear in the denominator of a solution, because for $W' := \operatorname{Spread}(u') = \binom{1}{2}\mathbb{Z}$ we can take $\mathbf{p}' = \binom{1}{0}$ and $\mathbf{v}' = \binom{-2}{1}$, and according to the lemma, some factor of the form $N^iK^j(4k - 2n + 1)$ would have to appear in the coefficient of $y(n+1, k)$.

More generally, for any nontrivial good submodule W'' of $\mathbb{Z}^2$ other than W, Lemma 2 excludes the possibility of periodic factors whose spread is contained in W'', because such factors would have to leave a trace in at least one of the coefficients of the equation.



In the previous example, we could thus determine all the interesting modules W by just looking at the spreads of the factors of the coefficients of the equation. The following example indicates that this is not always sufficient.

EXAMPLE 2. *The equation*

$$\begin{aligned}&(2k-3n^2-8n-5)y(n,k+1)\\&\quad+(k+3n^2+5n+4)y(n+1,k)\\&\quad-(5k-3n^2-11n-7)y(n+1,k+1)\\&\quad+(2k-3n^2-8n-3)y(n+2,k)=0\end{aligned}$$

also has the solution $y=(n^2+2k^2)/(k+n+1)$. *Its denominator* $k+n+1$ *does not appear in any of the coefficients of the equation. This is because for its spread* $W=\binom{1}{-1}\mathbb{Z}$ *there are no suitable* $\mathbf{p}\in S$ *and* $\mathbf{v}\in\mathbb{R}^2$ *matching the conditions of the lemma because the points* $\binom{1}{0},\binom{0}{1}$ *as well as the points* $\binom{2}{0},\binom{1}{1}$ *lie on a line parallel to* W.

In summary, in order for W to be the spread of a factor that can appear in the denominator of a solution of (1), W must be contained in the spread of some coefficient of the equation (as in Ex. 1) or it must be parallel to one of the faces in the convex hull of the support S (as in Ex. 2). For every equation, we can thus determine some finitely many good submodules of $\mathbb{Z}^r$ of codimension one such that each possibly occurring spread W is contained in at least one of them.

3.1 A Normalizing Change of Variables

Let $\mathbb{Z}^r=V\oplus W$ be a decomposition of $\mathbb{Z}^r$ into good submodules. Our goal is to obtain denominator bounds with respect to W by applying the algorithm from last year [12] to $V\cong\mathbb{Z}^r/W$. It turns out that this can be done provided that W is sufficiently nondegenerate. In order to formulate the precise conditions on W without too much notational overhead, it seems convenient to make a change of coordinates.

Let invertible matrices $A=((a_{i,j}))_{i,j=1}^r\in\mathbb{Q}^{r\times r}$ act on $\mathbb{K}(\mathbf{n})$ via

$$\begin{aligned}A\cdot y(n_1,\dots,n_r):=y\big(&a_{1,1}n_1+a_{1,2}n_2+\cdots+a_{1,r}n_r,\\&a_{2,1}n_1+a_{2,2}n_2+\cdots+a_{2,r}n_r,\\&\vdots\\&a_{r,1}n_1+a_{r,2}n_2+\cdots+a_{r,r}n_r\big).\end{aligned}$$

We obviously have $A\cdot(p+q)=(A\cdot p)+(A\cdot q)$ and $A\cdot(pq)=(A\cdot p)(A\cdot q)$ for all $p,q\in\mathbb{K}(\mathbf{n})$. It can be checked that we also have

$$A\cdot(N^{\mathbf{s}}y)=N^{A^{-1}\mathbf{s}}(A\cdot y)$$

for every $A\in\mathbb{Z}^{r\times r}$ with $|\det A|=1$ and every $\mathbf{s}\in\mathbb{Z}^r$ and every $y\in\mathbb{K}(\mathbf{n})$. It follows that $y\in\mathbb{K}(\mathbf{n})$ is a solution of (1) if and only if $\tilde{y}=A\cdot y$ is a solution of the transformed equation

$$\sum_{\mathbf{s}\in S}(A\cdot a_{\mathbf{s}})N^{A^{-1}\mathbf{s}}\tilde{y}=A\cdot f,$$

or equivalently of

$$\sum_{\mathbf{s}\in\tilde{S}}\tilde{a}_{\mathbf{s}}N^{\mathbf{s}}\tilde{y}=\tilde{f},$$

where $\tilde{S}=\{A^{-1}\mathbf{s}:s\in S\}$, $\tilde{a}_{\mathbf{s}}:=A\cdot a_{A\mathbf{s}}$ $(\mathbf{s}\in\tilde{S})$, and $\tilde{f}=A\cdot f$.

Now take $A\in\mathbb{Z}^{r\times r}$ with $|\det A|=1$ such that the first t rows of A^{-1} form a basis of V and the last $r-t$ rows of A^{-1} form a basis of W. Then the transformation just described maps the basis vectors of V to the first t unit vectors and the basis vectors of W to the last $r-t$ unit vectors. In other words, we can assume without loss of generality that V itself is generated by the first t unit vectors and W by the last $r-t$ unit vectors in $\mathbb{Z}^r$. We will make this assumption from now on, unless otherwise stated. Note that this convention implies for an irreducible polynomial $u\in\mathbb{K}[\mathbf{n}]$ that $\mathrm{Spread}(u)=W$ is equivalent to u being free of the variables $n_{t+1},n_{t+2},\dots,n_r$ and aperiodic as element of $\mathbb{K}[n_1,\dots,n_t]$.

From now on we will assume that W is a proper good submodule of $\mathbb{Z}^r$. This restriction is conform with our later application (see Algorithm 2) where we will choose $W:=\mathrm{Spread}(u)$ for some irreducible $u\in\mathbb{K}[\mathbf{n}]$; since $u\notin\mathbb{K}$, this implies $W\neq\mathbb{Z}^r$. By applying, if necessary, a suitable power of N_1 on both sides of the equation (1) we can further assume without loss of generality that $\min\{s_1:(s_1,\dots,s_r)\in S\}=0$, and we set $k:=\max\{s_1:(s_1,\dots,s_r)\in S\}$. Moreover, we may assume $k>0$: If $k=0$, the variable n_1 in problem (1) is in fact a constant. Hence we can move n_1 into the constant field $\mathbb{K}$, and we can rename the remaining variables accordingly. This reduction can occur at most $r-1$ times (otherwise this would imply $V=\{\mathbf{0}\}$ or equivalently $W=\mathbb{Z}^r$) and we eventually find a modified S with $k\geq 1$.

3.2 Bounding the Dispersion

With this transformation w.r.t. a proper good submodule W of $\mathbb{Z}^r$ and under the assumption that the extreme points (2) of S have certain properties, Theorem 2 below explains how one can bound the dispersion w.r.t. n_1 ($\mathrm{Disp}_1(u)$ as defined in Def. 1.2 in Section 2) of all factors u with $\mathrm{Spread}(u)\in W$ that occur in the denominator of a solution of (1). This result is a refinement of Lemma 2 from [12].

LEMMA 3. *Let* $u,v\in\mathbb{K}[\mathbf{n}]\setminus\{0\}$ *with* $\mathrm{Spread}(u)\subseteq W$ *and* $\mathrm{Spread}(v)\subseteq W$. *Then there is at most one* $(s_1,\dots,s_t)\in\mathbb{Z}^r$ *s.t. there is* $(s_{t+1},\dots,s_r)\in\mathbb{Z}^{r-t}$ *with* $N^{(s_1,\dots,s_r)}u=v$.

PROOF. Take $\mathbf{s},\mathbf{s}'$ with $N^{\mathbf{s}}u=v=N^{\mathbf{s}'}u$. As $N^{\mathbf{s}-\mathbf{s}'}u=u$, it follows $\mathbf{s}-\mathbf{s}'\in W=\{0\}^t\times\mathbb{Z}^{r-t}$, and thus the first t components of $\mathbf{s},\mathbf{s}'$ agree. □

By the transformation in Section 3.1 it follows that for any irreducible $u\in\mathbb{K}[\mathbf{n}]$ with $\mathrm{Spread}(u)\subseteq W$ we have that $\mathrm{Disp}_1(u)$ is bounded. As a consequence, we have $s\in\mathbb{N}\cup\{-\infty\}$ for the s defined in (3) below.

THEOREM 2. *Let*

$$\begin{aligned}A&=\{(s_1,\dots,s_r)\in S:s_1=0\},\\B&=\{(s_1,\dots,s_r)\in S:s_1=k\}.\end{aligned}\tag{2}$$

Suppose that no two elements of A *agree in the first* t *coordinates, and that the same is true for* B. *Let* $a'_{\mathbf{i}}$ *be those polynomials which contain all irreducible factors* u *of* $a_{\mathbf{i}}$ *with* $\mathrm{Spread}(u)\subseteq W$. *Let*

$$s:=\max\{\mathrm{Disp}_1(a'_{\mathbf{s}},N_1^{-k}a'_{\mathbf{t}}):\mathbf{s}\in A\text{ and }\mathbf{t}\in B\}.\tag{3}$$

Then for any solution $y=p/q\in\mathbb{K}(\mathbf{n})$ *of* (1) *and any irreducible factors* u,v *of* q *with* $\mathrm{Spread}(u),\mathrm{Spread}(v)\subseteq W$ *we have* $\mathrm{Disp}_1(u,v)\leq s$.

PROOF. As S is not empty, A,B are nonempty. W.l.o.g. we may assume that the minimal element of A w.r.t. lexicographic order is the zero vector.

Suppose that there are irreducible factors u, v of q with $\mathrm{Spread}(u) \subseteq W$, $\mathrm{Spread}(v) \subseteq W$ and $d := \mathrm{Disp}_1(u, v)$ such that $d > s$; take such u, v such that d is maximal (since there are only finitely many factors u, v in q and $\mathrm{Disp}_1(u, v)$ is bounded, this is possible). W.l.o.g., we assume that $\gcd(v, N^{\mathbf{d}}u) \neq 1$ where the first entry in $\mathbf{d} \in \mathbb{Z}$ is d (otherwise we interchange u and v). Consider all the factors $N^{\mathbf{u}}u$ and $N^{\mathbf{v}}v$ occurring in q where the first entry in $\mathbf{u}$ and $\mathbf{v}$ is 0. Note that by Lemma 3 there are only finitely many choices of the first t components, so we can choose two such factors from q where the first t components of $\mathbf{u}$ are minimal and the first t components of $\mathbf{v}$ are maximal w.r.t. lexicographic order; these factors are denoted by u', v' respectively; note that $\gcd(v', N^{\mathbf{d}'}u') \neq 1$ for some $\mathbf{d}' \in \mathbb{Z}$ where the first entry is d.

• First suppose that u' divides one of the polynomials $a_{\mathbf{m}}$ with $\mathbf{m} \in A$. In this case we choose the polynomial $a_{\mathbf{w}}$ with $\mathbf{w} = (w_1, \ldots, w_r) \in B$ such that $(w_2, \ldots, w_t)$ is maximal w.r.t. lexicographic order (uniqueness is guaranteed by the assumption that no two elements from B agree in the first t components). We can write (1) in the form

$$N^{\mathbf{w}}y = \frac{1}{a_{\mathbf{w}}}\Big(f - \sum_{\mathbf{s}\in S\setminus\{\mathbf{w}\}} a_{\mathbf{s}}N^{\mathbf{s}}y\Big). \tag{4}$$

Now observe that the factor $N^{\mathbf{w}}v'$ does not occur in the denominator of any $N^{\mathbf{s}}y$ with $\mathbf{s} \in S \setminus \{\mathbf{w}\}$:

1. Suppose that there is $\mathbf{s} \in S \setminus B$ such that $N^{\mathbf{w}}v'$ occurs in $N^{\mathbf{s}}q$, i.e., $N^{\mathbf{w}-\mathbf{s}}v'$ is a factor of q. Since the first component of $\mathbf{w}$ is k ($\mathbf{w} \in B$) and the first component of $\mathbf{s}$ is smaller than k ($\mathbf{s} \notin B$), the first component of $\mathbf{w} - \mathbf{s}$ is positive. Moreover, since $\gcd(v', N^{\mathbf{d}'}u') \neq 1$, the factors v' and $N^{\mathbf{w}-\mathbf{s}}v'$ of q have distance larger than d in the first component; a contradiction to the maximality of d. Thus, if $N^{\mathbf{w}}v'$ is a factor in the denominator of $N^{\mathbf{s}}y$ with $\mathbf{s} \in S$, it follows that $\mathbf{s} \in B$.
2. Suppose that there is $\mathbf{s} \in B$ with $\mathbf{w} \neq \mathbf{s}$ such that $N^{\mathbf{w}}v'$ is a factor of $N^{\mathbf{s}}q$. Then $N^{\mathbf{w}-\mathbf{s}}v'$ is a factor of q. Since the first component of the vectors in B is k, but the first t components in total cannot be the same for two different vectors of B, it follows that the first entry in $\mathbf{w} - \mathbf{s}$ is zero and at least one of the others is non-zero; in particular, by the maximality assumption on $\mathbf{w}$ the first non-zero entry is positive. Hence we find $\mathbf{v}' = (0, v'_2, \ldots, v'_r) := \mathbf{v} + \mathbf{w} - \mathbf{s}$ such that $N^{\mathbf{v}'}v$ is a factor of q and such that $(v'_2, \ldots, v'_t)$ is larger than $(v_2, \ldots, v_t)$ w.r.t. lexicographic ordering; a contradiction to the choice of the vector $\mathbf{v}$.

Since $f, a_{\mathbf{s}} \in \mathbb{K}[\mathbf{n}]$ and $N^{\mathbf{w}}v'$ does not occur in the denominators of $N^{\mathbf{s}}y$ for any $\mathbf{s} \in S \setminus \{\mathbf{w}\}$, also the common denominator of the rational function $f - \sum_{\mathbf{s}\in S\setminus\{\mathbf{w}\}} a_{\mathbf{s}}N^{\mathbf{s}}y$ does not contain the factor $N^{\mathbf{w}}v'$. Finally, $N^{\mathbf{w}}v'$ cannot be a factor of $a_{\mathbf{w}}$: Since $\mathbf{m} \in A$, $\mathbf{w} \in B$ and $s < d$, we have $\mathrm{Disp}_1(a_{\mathbf{m}}, N_1^{-k}a_{\mathbf{w}}) < d$. However, $\gcd(u', N^{\mathbf{d}'}v') \neq 1$ and $u' \mid a_{\mathbf{m}}$; thus $N^{\mathbf{w}}v' \mid a_{\mathbf{m}}$ would imply that $N_1^{-k}N^{\mathbf{w}}v' \mid N_1^{-k}a_{\mathbf{m}}$ and thus (note that the first component in $\mathbf{w}$ is $k \geq 0$) it would follow $\mathrm{Disp}_1(a_{\mathbf{m}}, N_1^{-k}a_{\mathbf{w}}) \geq d$. Overall, the common denominator on the right side of (4) cannot contain the factor $N^{\mathbf{w}}v'$, and hence the denominator of $N^{\mathbf{w}}y$ is not divisible by $N^{\mathbf{w}}v'$. Thus the denominator of y, in particular q is not divisible by v'; a contradiction.

• Conversely, suppose that u' does not divide any of the polynomials $a_{\mathbf{s}}$ with $\mathbf{s} \in A$. Now let $\mathbf{w} = (0, w_2 \ldots, w_r) \in A$ such that $(w_2, \ldots, w_t)$ is minimal w.r.t. lexicographic ordering (again it is uniquely determined by the assumptions on A), and write (1) in the form (4); by our assumption stated in the beginning, $\mathbf{w}$ is just the zero vector $\mathbf{0}$. By analogous arguments as above (the roles of A and B, resp. u' and v', are exchanged) it follows that u' does not occur in the denominator of any $N^{\mathbf{s}}y$ with $\mathbf{s} \in S \setminus \{\mathbf{0}\}$. Hence as above, the common denominator of $f - \sum_{\mathbf{s}\in S\setminus\{\mathbf{0}\}} a_{\mathbf{s}}N^{\mathbf{s}}y$ does not contain the factor u'. Moreover, since u' does not divide any $a_{\mathbf{s}}$ from $\mathbf{s} \in A$, the factor u' does not occur in $a_{\mathbf{0}}$. In total, the factor u' is not part of the denominator on the right hand side of (4), but it is a factor of the denominator on the left hand side; a contradiction. □

The following example illustrates that Theorem 2 is not always applicable.

Example 3. *Fix* $W := \mathrm{Spread}(k + n + 1) = \binom{1}{-1}\mathbb{Z}$ *and take* $V = \binom{0}{1}\mathbb{Z}$. *The problem from Example 1 is normalized by the change of variables* $n \to k$ *and* $k \to n-k$ *(i.e., a basis transformation* $\left(\begin{smallmatrix}0 & 1\\ 1 & -1\end{smallmatrix}\right)$ *with determinant* -1 *is chosen) and one obtains* $V' = \binom{1}{0}\mathbb{Z}$ *and* $W' = \binom{0}{1}\mathbb{Z}$. *This gives the new equation*

$$\begin{aligned}&(n+1)(-6k+4n+1)y(n,k)\\ &\quad+(12k^2-14nk+12k+8n^2+n+6)y(n+1,k)\\ &-2(6k^2-10nk-12k+6n^2+13n+6)y(n+1,k+1)=0\end{aligned}$$

with the new structure set $S' = \{\binom{0}{0}, \binom{1}{0}, \binom{1}{1}\}$ *which now has the solution* $y = \frac{3k^2-4nk+2n^2}{n+1}$ *where the denominator consists of the factor* $n+1$ *with* $\mathrm{Spread}(n+1) = W'$. *As observed already in Example 1 one can predict the factor* $n+1$ *(up to a shift in* n*) by exploiting Lemma 2. However, one cannot apply Theorem 2. For* S' *we get the sets* $A = \{\binom{0}{0}\}$ *and* $B = \{\binom{1}{0}, \binom{1}{1}\}$ *where in* B *the two vectors are the same in the first component but differ in the second component.*

3.3 Denominator Bounding Theorem

We are now working towards a denominator bounding theorem (Thm. 3 below) which says that if we rewrite the equation (1) into a new equation whose support contains some point $\mathbf{p}$ which is sufficiently far away from all the other points in the support, then we can read off a denominator bound from this new equation. We will need the following fact, which appears literally as Theorem 3 in [12] (with W, S' renamed to R^-, R^+ here in order to avoid a name clash with the meaning of W in the present paper).

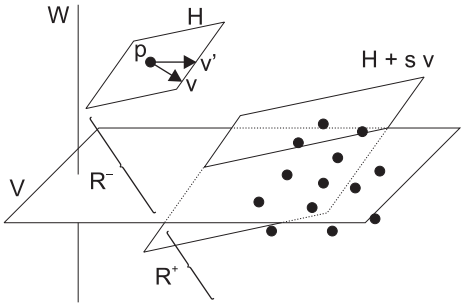
Lemma 4. *Let* $\mathbf{p}$ *be a corner point of* S *with border plane* H *and inner vector* $\mathbf{v}$. *Then for every* $s > 0$ *there exist finite sets*

$$R^- \subseteq \mathbb{Z}^r \cap \bigcup_{0\leq e\leq s} (H + e\mathbf{v}) \text{ and } R^+ \subseteq \mathbb{Z}^r \cap \bigcup_{e>s} (H + e\mathbf{v}),$$

and polynomials $b, b_{\mathbf{i}} \in \mathbb{K}[\mathbf{n}]$ *such that for any solution* $y \in \mathbb{K}(\mathbf{n})$ *of* (1) *we have*

$$N^{\mathbf{p}}y = \frac{b + \sum_{\mathbf{i}\in R^+} b_{\mathbf{i}}N^{\mathbf{i}}y}{\prod_{\mathbf{i}\in R^-} N^{\mathbf{i}-\mathbf{p}}a_{\mathbf{p}}}. \tag{5}$$

The sets R^- and R^+ and the polynomials $b, b_{\mathbf{i}}$ can be computed for a given s, S, $\mathbf{p}$, and $\mathbf{v}$ by Algorithm 2 from [12]. The next theorem provides a denominator bound with respect to W. It is an adaption of Theorem 4 from [12] to the present situation. We continue to assume the normalization $V = \mathbb{Z}^t \times \{0\}^{r-t}$, $W = \{0\}^t \times \mathbb{Z}^{r-t}$. The following figure illustrates the situation. The vector $\mathbf{v}$ is orthogonal to H but not necessarily to W, while the vector $\mathbf{v}'$ is orthogonal to W but not necessarily to H. Relation (5) separates $\mathbf{p}$ from the points in R^+ which are all below the plane $H + s\mathbf{v}$. The points in R^- are all between H and $H + s\mathbf{v}$.



THEOREM 3. *Let $s \in \mathbb{N} \cup \{-\infty\}$ be such that for any solution $y = p/q \in \mathbb{K}(\mathbf{n})$ of (1) and any irreducible factors u, v of q with $\mathrm{Spread}(u), \mathrm{Spread}(v) \subseteq W$ we have $\mathrm{Disp}_1(u, v) \le s$. Let $\mathbf{p}$ be a corner point of S for which there is an inner vector $\mathbf{v} = (v_1, \ldots, v_r)$ with $v_1 \ge 1$ as well as an inner vector $\mathbf{v}'$ orthogonal to W. For these choices of s, $\mathbf{p}$, and $\mathbf{v}$, let R^-, R^+, b, $b_{\mathbf{i}}$ be as in Lemma 4. Let $a'_{\mathbf{p}}$ be the polynomial consisting of all the factors of $a_{\mathbf{p}}$ whose spread is contained in W. Then*

$$d := \prod_{\mathbf{s} \in R^-} N^{\mathbf{s}-2\mathbf{p}} a'_{\mathbf{p}} \tag{6}$$

is a denominator bound of (1) with respect to W.

PROOF. Let $y = p/q \in \mathbb{K}(\mathbf{n})$ be a solution of (1) and let u be an irreducible factor of q with multiplicity m and $\mathrm{Spread}(u) \subseteq W$. We have to show $u^m \mid d$. Lemma 2 applied to $\mathbf{p}$ and $\mathbf{v}'$ implies that there is some $\mathbf{i} \in \mathbb{Z}^r$ with $u' \mid q$ and $u' := N^{\mathbf{i}} u \mid a_{\mathbf{p}}$. By the choice of s we have $\mathrm{Disp}_1(u', u) \le s$.

Lemma 4 implies the representation

$$N^{\mathbf{p}} y = \frac{b + \sum_{\mathbf{i} \in R^+} b_{\mathbf{i}} N^{\mathbf{i}} y}{\prod_{\mathbf{i} \in R^-} N^{\mathbf{i}-\mathbf{p}} a_{\mathbf{p}}}.$$

Because of $v_1 > 1$, every $\mathbf{i} \in R^+$ differs from $\mathbf{p}$ in the first coordinate by more than s. This implies that $N^{\mathbf{p}} u$ and hence that $N^{\mathbf{p}} u^m$ cannot appear in the denominator of $N^{\mathbf{i}} y$ for any $\mathbf{i} \in R^+$. But it does appear in the denominator of $N^{\mathbf{p}} y$, so it must appear as well in the denominator of the right hand side. The only remaining possibility is thus $N^{\mathbf{p}} u^m \mid \prod_{\mathbf{i} \in R^-} N^{\mathbf{i}-\mathbf{p}} a_{\mathbf{p}}$, and hence

$$u^m \mid \prod_{\mathbf{i} \in R^-} N^{\mathbf{i}-2\mathbf{p}} a_{\mathbf{p}}.$$

Because of $\mathrm{Spread}(u') = \mathrm{Spread}(u) \subseteq W$, it follows that $u^m \mid d$. □

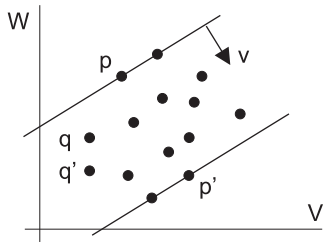
3.4 A Denominator Bounding Algorithm

We now combine Theorems 2 and 3 to an algorithm for computing a denominator bound with respect to an arbitrary given W in situations where these theorems are applicable.

DEFINITION 3. *Let $\mathbf{p}, \mathbf{p}'$ be corner points of S and W some submodule of $\mathbb{Z}^r$.*

1. *The point $\mathbf{p}$ is called* useless *for W if there is an edge $(\mathbf{p}, \mathbf{s})$ in the convex hull of S with $\mathbf{p} - \mathbf{s} \in W$.*
2. *The pair $(\mathbf{p}, \mathbf{p}')$ is called* opposite *if there is a vector $\mathbf{v}$ such that $(\mathbf{s} - \mathbf{p}) \cdot \mathbf{v} \ge 0$ and $(\mathbf{p}' - \mathbf{s}) \cdot \mathbf{v} \ge 0$ for all $\mathbf{s} \in S$. Such a $\mathbf{v}$ is called a* witness vector *for the pair $(\mathbf{p}, \mathbf{p}')$.*
3. *The pair $(\mathbf{p}, \mathbf{p}')$ is called* useful *for W if it is opposite and neither $\mathbf{p}$ nor $\mathbf{p}'$ is useless for W.*

In the illustration below, the pair $(\mathbf{p}, \mathbf{p}')$ is opposite, with $\mathbf{v}$ being a witness vector. It is even a useful pair, because neither $\mathbf{p}$ nor $\mathbf{p}'$ is an endpoint of the edge of the convex hull of S which is parallel to W. In contrast, the corner point $\mathbf{q}$ is useless, because the edge $(\mathbf{q}, \mathbf{q}')$ is parallel to W.



The definition of a useful pair is made in such a way that when a change of variables as described in Section 3.1 is applied which maps a witness vector of the pair to the first axis, then the sets A and B from Theorem 2 are such that $\mathbf{p} \in A$, $\mathbf{p}' \in B$ (because of the oppositeness), no two elements of A agree in the first $r - \dim W$ coordinates (because $\mathbf{p}$ is not useless), and the same is true for B (because $\mathbf{p}'$ is not useless).

Whether a pair $(\mathbf{p}, \mathbf{p}') \in S^2$ is useful or not can be found out by making an ansatz for the coefficients of a witness vector and solving the system of linear inequalities from the definition. The pair is useful if and only if this system is solvable, and in this case, any solution gives rise to a witness vector.

If for a given good submodule W we have found a useful pair, then we can compute a denominator bound with respect to W by the following algorithm.

ALGORITHM 1. Input: *An equation of the form (1), a proper good submodule W of $\mathbb{Z}^r$, a useful pair $(\mathbf{p}, \mathbf{p}')$ of S for W.* Output: *A denominator bound for (1) with respect to W.*

Set $t := r - \dim W$.
Choose $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_t \in \mathbb{Z}^r$ such that $\mathbf{v}_1$ is a witness vector for $(\mathbf{p}, \mathbf{p}')$ and $\mathbb{Z}^r = V \oplus W$ where V is the module generated by these vectors.
Perform a change of variables as described in Section 3.1 such that $\mathbf{v}_i$ becomes the ith unit vector in $\mathbb{Z}^r$, W becomes $\{0\}^t \times \mathbb{Z}^{r-t}$.
Determine A, B as in Theorem 2.
Compute $s \in \mathbb{N} \cup \{-\infty\}$ as defined in Theorem 2.
Choose an inner vector $\mathbf{v} \in \mathbb{R}^r$ for $\mathbf{p}$.
Compute R^- as defined in Lemma 4.
Compute d as defined in Theorem 3.
Apply the inverse change of variables to d, getting d'.
Return d'.

The following variations can be applied for further improvements:

1. If the dimension of V is greater than 1, there might be different choices of witness vectors. Choosing different versions in line 2 might lead to different denominator bounds of W, say, $d_1, \dots, d_k$. Then taking $d := \gcd(d_1, \dots, d_k)$ may produce sharper denominator bound for (1) w.r.t. W.
2. Choosing different inner vectors in line 10 might lead to different sets R^- to write (5) and hence gives rise to different denominator bounds in (6). Taking the gcd of these denominator bounds may produce a refined version.
3. The coefficients $a_{\mathbf{s}}$ with $\mathbf{s} \in S$ are often available in factorized form. Then also the denominator bounds are obtained in factorized form, and the gcd-computations reduce to comparisons of these factors and bookkeeping of their multiplicities.

4. A COMBINED DENOMINATOR BOUND

As mentioned earlier, when setting $W = \{0\}$, one is able to derive an aperiodic denominator bound for equation (1). In this particular case, for each corner point $\mathbf{p}$ there is an other corner point $\mathbf{p}'$ such that $(\mathbf{p}, \mathbf{p}')$ is useful for W. Hence applying Algorithm 1 for any useful pair leads to an aperiodic denominator bound. In particular, running through all corner points and taking the gcd for all these candidates leads to a rather sharp aperiodic denominator bound for equation (1) which coincides with the output given in our previous investigation [12].

In the other extreme, when setting $W = \mathbb{Z}^r$, a denominator bound for (1) w.r.t. W would lead to a complete denominator bound for equation (1). However, in this case, we will fail to find a useful pair $(\mathbf{p}, \mathbf{p}')$, and in particular our Algorithm 1 is not applicable.

Our goal is to find a simultaneous denominator bound with respect to all W to which Algorithm 1 is applicable, i.e., for all W from the set

$$U := \{W \text{ good submodule of } \mathbb{Z}^r \mid \exists\ (\mathbf{p}, \mathbf{p}') \text{ useful for } W\}.$$

In general, this is an infinite set. But we can make use of the observations made after Example 2. Using Lemma 2, it turns out that instead of looping through all these infinitely many modules W, it is sufficient to consider those W which appear as spread of some factor in the coefficient of $a_{\mathbf{p}}$.

This argument even works for all W in the larger set

$$O := \{W \text{ good submodule of } \mathbb{Z}^r \mid \exists\ (\mathbf{p}, \mathbf{p}') \text{ opposite with } \mathbf{p} \text{ not useless for } W\},$$

but since the $W \in O \setminus U$ do not satisfy the conditions of Theorem 2, we can only obtain partial information about their denominator bounds.

We propose the following algorithm.

ALGORITHM 2. Input: *An equation of the form* (1). Output: *A finite set of irreducible polynomials* $P = \{p_1, \dots, p_k\}$, *and a nonzero* $d \in \mathbb{K}[\mathbf{n}]$ *such that for every solution* $y = \frac{p}{q} \in \mathbb{K}(\mathbf{n})$ *of* (1) *and every irreducible factor* u *of* q *with multiplicity* m *exactly one of the following holds:*

1. $\text{Spread}(u) \in U$ *and* $u^m \mid d$,
2. $\text{Spread}(u) \in O \setminus U$ *and* $\exists\ \mathbf{s} \in \mathbb{Z}^r, p \in P : N^{\mathbf{s}} u = p$,
3. $\text{Spread}(u) \notin O$.

```
1  d := 1; P := {}; C := {p ∈ S : p corner point of S}
2  forall q ∈ C do
3    forall u | a_q irreducible do
4      W := Spread(u)
5      if W ∈ U then
6        Compute a denominator bound d_0 w.r.t. W
7              using an arbitrary useful pair for W.
8        d := lcm(d, d_0)
9      else if W ∈ O then
10       P := P ∪ {u}
11 return (P, d)
```

THEOREM 4. *The polynomial* d *computed by Algorithm 2 is a denominator bound with respect to any finite union of modules in* U.

PROOF. Let W be in U and $(\mathbf{p}, \mathbf{p}')$ be a useful pair with respect to W. Let $y = p/q$ be a solution of (1) and u be an irreducible factor of q with multiplicity m and $\text{Spread}(u) \subseteq W$. We have to show that $u^m \mid d$.

Since $\mathbf{p}$ is not useless, Lemma 2 implies that there is some $\mathbf{i} \in \mathbb{Z}^r$ with $N^{\mathbf{i}} u \mid a_{\mathbf{p}}$. This factor is going to be investigated in some iteration of the loop starting in line 3. The polynomial d_0 computed in this iteration is a denominator bound with respect to $\text{Spread}(N^{\mathbf{i}} u) = \text{Spread}(u)$. It follows that $u^m \mid d_0 \mid d$.

This proves the theorem when W itself is in U. If W is only a finite union of elements of U, the theorem follows from here by Lemma 1. □

For $W \in O \setminus U$, we can still apply Lemma 2 but Theorem 2 is no longer applicable. This prevents us from computing precise denominator bounds with respect to these W. However, using the set $P = \{p_1, \dots, p_k\}$ returned by the algorithm we can at least say that for every denominator q of a solution $y = p/q$ of (1) there exist $m \in \mathbb{N}$ and a finite set $S' \subseteq \mathbb{Z}^r$ such that

$$d \prod_{\substack{p \in P \\ \mathbf{s} \in S'}} N^{\mathbf{s}} p^m \tag{7}$$

is a multiple of every divisor of q whose spread is contained in some finite union of modules in O. Appropriate choices S' and m can be found for instance by making an ansatz. Note also that the set P is usually smaller than the set of all periodic factors that occur in the coefficients $a_{\mathbf{s}}$ of (1). This phenomenon was demonstrated already in the second part of Example 2.

Summarizing, some part of the denominator is out of reach, namely all those parts of the denominator w.r.t. the modules from

$$\{\, W \text{ submodule of } \mathbb{Z}^r \mid (\mathbf{p}, \mathbf{p}') \text{ opposite for } W, \text{ both } \mathbf{p} \text{ and } \mathbf{p}' \text{ are useless for } W \,\},$$

some part of the denominator can be given up to possible shifts and multiplicities, and some part of the denominator bound is given explicitly by d.

The following improvements can be utilized.

1. As a preprocessing step, one should compute an aperiodic denominator bound for the equation (1) as described above. What remains is to recover the periodic factors. As a consequence, one can neglect all

irreducible factors u which are aperiodic and one can apply Theorem 3 where all aperiodic factors are removed from the polynomials $a'_{\mathbf{p}}$.

2. Choosing different useful pairs for a module W in line 9 might lead to different choices of denominator bounds, and taking their gcd may give rise to sharper denominator bounds of (1) w.r.t. W.

5. DISCUSSION

Typically the set O will contain all the submodules of $\mathbb{Z}^r$. Only when the convex hull of S happens to have two parallel edges on opposite sides, as is the case in Example 2, then modules W parallel to this edge do not belong to O. The set U will never contain all the submodules of $\mathbb{Z}^r$. Precisely those modules W which are parallel to an edge of the convex hull of S do not belong to U. Since the convex hull of S contains only finitely many edges, U will in some sense still contain almost all the submodules of $\mathbb{Z}^r$.

Depending on the origin of the equation, it may be that there is some freedom in the structure set S. For example, by multivariate guessing [13] or by creative telescoping [17, 10, 16] one can systematically search for equations with a prescribed structure set. In such situations, one can try to search for an equation with a structure set for which U and O cover as many spaces as possible.

If two equations with different structure sets are available, it may be possible to combine the two denominator bounds obtained by Algorithm 2 to a denominator bound with respect to the full space $\mathbb{Z}^r$.

EXAMPLE 4. *Consider the following system of equations:*

$$\begin{aligned}
&-(k+n+1)(2k+3n+1)y(n,k)\\
&\quad+(k+n+4)(2k+3n+3)y(n,k+1)\\
&\qquad-(k+n+2)(2k+3n+4)y(n+1,k)\\
&\qquad\quad+(k+n+5)(2k+3n+6)y(n+1,k+1)=0,\\
&(n^2+n+1)(2k+3n+3)y(n,k+1)\\
&\quad-(n^2+5n+7)(2k+3n+4)y(n+1,k)\\
&\qquad-(n^2+3n+3)(2k+3n+8)y(n+1,k+2)\\
&\qquad\quad+(n^2+7n+13)(2k+3n+9)y(n+2,k+1)=0.
\end{aligned}$$

Algorithm 2 applied to the first equation returns

$$d=(n+k+1)(n+k+2)(n+k+3)(3n+2k+1)$$

as a denominator bound with respect to any W except $\binom{1}{0}\mathbb{Z}$ and $\binom{0}{1}\mathbb{Z}$. Applied to the second equation, it returns

$$d=(n^2+n+1)((n+1)^2+(n+1)+1)(3n+2k+1)$$

as a denominator bound with respect to any W except $\binom{1}{1}\mathbb{Z}$ and $\binom{1}{-1}\mathbb{Z}$. The least common multiple of the two outputs is a simultaneous denominator bound with respect to any W.

Indeed, the system has the solution

$$\frac{1}{(n+k+1)(n+k+2)(n+k+3)(n^2+n+1)((n+1)^2+(n+1)+1)(3n+2k+1)}.$$

There is no hope for an algorithm which computes for any given single equation a denominator bound with respect to the full space $\mathbb{Z}^r$. This is because there are equations whose solution space contains rational functions with no finite common denominator. For instance, for every univariate polynomial p, we have that $1/p(n+k)$ is a solution of the equation

$$y(n+1,k)-y(n,k+1)=0.$$

It would be interesting to characterize under which circumstances this happens, and to have an algorithm which finds a denominator bound with respect to $\mathbb{Z}^r$ in all other cases.

Acknowledgements. We thank all five referees for their careful reading and their critical comments.

6. REFERENCES

[1] S. A. Abramov. On the summation of rational functions. *Zh. vychisl. mat. Fiz*, pages 1071–1075, 1971.

[2] S. A. Abramov. Problems in computer algebra that are connected with a search for polynomial solutions of linear differential and difference equations. *Moscow Univ. Comput. Math. Cybernet.*, 3:63–68, 1989.

[3] S. A. Abramov and M. Barkatou. Rational solutions of first order linear difference systems. In *Proc. ISSAC'98*, pages 124–131, 1998.

[4] S. A. Abramov, A. Gheffar, and D. Khmelnov. Factorization of polynomials and gcd computations for finding universal denominators. In *Proc. CASC'10*, pages 4–18, 2010.

[5] S. A. Abramov and K. Yu. Kvashenko. Fast algorithms to search for the rational solutions of linear differential equations with polynomial coefficients. In *Proc. ISSAC'91*, pages 267–270, 1991.

[6] M. Barkatou. Rational solutions of matrix difference equations: The problem of equivalence and factorization. In *Proc. ISSAC'99*, pages 277–282, 1999.

[7] A. Bostan, F. Chyzak, T. Cluzeau, and B. Salvy. Low complexity algorithms for linear recurrences. In *Proc. ISSAC'06*, pages 31–39, 2006.

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

[9] W. Y. C. Chen, P. Paule, and H. L. Saad. Converging to Gosper's algorithm. *Adv. in Appl. Math.*, 41(3):351–364, 2008.

[10] F. Chyzak. An extension of Zeilberger's fast algorithm to general holonomic functions. *Discrete Mathematics*, 217:115–134, 2000.

[11] M. van Hoeij. Rational solutions of linear difference equations. In *Proc. ISSAC'98*, pages 120–123, 1998.

[12] M. Kauers and C. Schneider. Partial denominator bounds for partial linear difference equations. In *Proc. ISSAC'10*, pages 211–218, 2010.

[13] M. Kauers. Guessing handbook. Technical Report 09-07, RISC-Linz, 2009.

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

[15] M. Petkovšek. Hypergeometric solutions of linear recurrences with polynomial coefficients. *Journal of Symbolic Computation*, 14(2-3):243–264, 1992.

[16] C. Schneider. A collection of denominator bounds to solve parameterized linear difference equations in $\Pi\Sigma$-extensions. In *Proc. SYNASC'04*, pages 269–282, 2004.

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