On n-Dimensional Sequences. I *

GRAHAM NORTON
Centre for Communications Research, University of Bristol, UK

July 19, 2001

Abstract

Let R be a commutative ring and let $n \geq 1$. We study $\Gamma(s)$, the generating function and $\mathrm{Ann}(s)$, the ideal of characteristic polynomials of s, an n-dimensional sequence over R.

We express $f(X_1, \ldots, X_n) \cdot \Gamma(s)(X_1^{-1}, \ldots, X_n^{-1})$ as a partitioned sum. That is, we give (i) a 2^n-fold "border" partition (ii) an explicit expression for the product as a 2^n-fold sum; the support of each summand is contained in precisely one member of the partition. A key summand is $\beta_0(f, s)$, the "border polynomial" of f and s, which is divisible by $X_1 \cdots X_n$.

We say that s is *eventually rectilinear* if the elimination ideals $\mathrm{Ann}(s) \cap R[X_i]$ contain an $f_i(X_i)$ for $1 \leq i \leq n$. In this case, we show that $\mathrm{Ann}(s)$ is the ideal quotient $(\sum_{i=1}^{n}(f_i) : \beta_0(f, s)/(X_1 \cdots X_n))$.

When R and $R[[X_1, X_2, \ldots, X_n]]$ are factorial domains (e.g. R a principal ideal domain or $\mathbb{F}[X_1, \ldots, X_n]$), we compute *the monic generator* γ_i of $\mathrm{Ann}(s) \cap R[X_i]$ from known $f_i \in \mathrm{Ann}(s) \cap R[X_i]$ or from a finite number of 1-dimensional linear recurring sequences over R. Over a field $\mathbb{F}$ this gives an $O(\prod_{i=1}^{n} \delta\gamma_i^3)$ algorithm to compute an $\mathbb{F}$-basis for $\mathrm{Ann}(s)$.

1 Introduction

Linear recurring sequences (lrs) have a long and useful history; see for example Cerlienco *et al.* (1987), Zierler (1959) and the works cited there. Sequences over the integers and over finite fields are applied *inter alia* in the Analysis of Algorithms (Greene & Knuth (1982)), Telecommunications (McEliece (1987)), Coding Theory (Peterson & Weldon (1972), Fitzpatrick & Norton (1991)) and Cryptography (Rueppel (1986)).

Applications of more general sequences have also appeared in the recent literature: sequences over $\mathbb{Z}/4\mathbb{Z}$ (Boztaş, Hammons and Kumar (1992)), over the Gaussian integers (Fan & Darnell (1994))

*Dedicated to Professor Peter J. Hilton on his retirement. Research supported by Science and Engineering Research Council Grant GR/H15141. Current addresses: Dept. Mathematics, University of Queensland, Brisbane 4072, ghn@maths.uq.edu.au.

and 2-dimensional lrs over a field (i.e. lrs indexed by $\mathbb{N}^2$); see for example Homer & Goldmann (1985) and the works cited there, Lin & Liu (1988), Prabhu & Bose (1982) and Sakata (1978, 1981, 1990), Fitzpatrick & Norton (1990), Chabanne & Norton (1994)), Norton (1995a).

We consider n-dimensional (n-D) sequences over an arbitrary commutative ring R, where $n \geq 1$. In Section 2 we set up our basic framework and develop some preliminary properties of (i) the ideal $\mathrm{Ann}(s)$ of characteristic polynomials and (ii) $\Gamma(s)$, the generating function of an n-D sequence s. Section 3 begins with a certain "border" partition and studies the resulting decomposition of the product $f(X_1, \ldots, X_n) \cdot \Gamma(s)(X_1^{-1}, \ldots, X_n^{-1})$. Finally, some properties of $\Gamma(s)$ and $\mathrm{Ann}(s)$ for an "eventually rectilinear (EVR)" sequence are given in Section 4.

In more detail, we study sequences over R indexed *negatively* i.e. by $-\mathbb{N}^n$. The traditional approach to studying $\Gamma(s)$ and $\mathrm{Ann}(s)$ is to index sequences by $\mathbb{N}^n$ and to regard $\Gamma(s)$ as an element of the power series ring $R[[X_1, \ldots, X_n]]$; in this way, $R[X_1, \ldots, X_n]$ acts by *left*-shifting. This approach complicates the theory and proofs unnecessarily however. For example, it forces use of the reciprocal f^* of a polynomial f (for $f^*\Gamma(s)$ to be in the power series ring), resulting in a characteristic polynomial f being characterized in terms of $\Gamma(s)$, its degree and f^*. Compare also Corollaries 2.9, 2.12 and 3.9, 3.10 below.

Instead, we let $f \circ s$ denote $f \in R[X_1, \ldots, X_n]$ acting on s by *right-shifting* (defined in Section 2) and let $\mathrm{Ann}(s)$ denote the annihilator ideal of s with respect to right-shifting. We use the ring of Laurent series $R((X_1^{-1}, \ldots, X_n^{-1}))$ — rather than power series — as the ambient ring. This is a much more natural approach: the ring of Laurent series contains $R[X_1, \ldots, X_n]$ *as standard* $R[X_1, \ldots, X_n]$*-submodule*, as well as the product $f \cdot \Gamma(s)$.

Section 2 defines a partial order on $\mathbb{Z}^n$ and generalizes standard interval notation to $\mathbb{Z}^n$. We give the basic definitions, various examples of n-D lrs, define EVR sequences and give some preliminary results relating $\mathrm{Ann}(s)$ and $\Gamma(s)$. For example, we show that $\Gamma(f \circ s)$ is a summand of $f \cdot \Gamma(s)$.

In Section 3, we define the border partition and the "border polynomial" $\beta_0(f, s)$ of f and s, a key summand of $f \cdot \Gamma(s)$, which is divisible by $X_1 \cdots X_n$. The remaining $2^n - 2$ summands are "border Laurent series". We also show how these border summands can be rewritten using a generalized Newton divided difference operator. Section 3 concludes with our decomposition formula for $f \cdot \Gamma(s)$.

Section 4 concentrates on EVR sequences over commutative rings, characterizing their generating functions and exhibiting $\mathrm{Ann}(s)$ as an ideal quotient. This requires looking at the elimination ideals $\mathrm{Ann}(s) \cap R[X_i]$, $(1 \leq i \leq n)$ via some ancillary results on 1-D sequences and 1-D "associated sequences".

We call R *potential* if for all $n \geq 1, R[[X_1, X_2, \ldots, X_n]]$ is a factorial — unique factorisation — domain. In this case, we show that the above elimination ideals have a unique *monic generator*, and give two ways of finding them: Theorem 4.13 and Corollary 4.16. We also generalize a result

of Cerlienco & Piras (1991) to sequences over potential domains (Theorem 4.18).

Finally, we show that if s is EVR with $f_i \in \mathrm{Ann}(s) \cap R[X_i]$, then $\mathrm{Ann}(s)$ is the ideal quotient $(\sum_{i=1}^{n}(f_i) \ : \ \beta_0(f,s)/(X_1 \cdots X_n))$. Algorithm 4.22 below shows how to compute the corresponding basis for $\mathrm{Ann}(s)$. There are known methods (Buchberger (1985) and Cox *et al.* (1991)) for finding a basis of an ideal quotient. The former yields a linear system of size $\prod_{i=1}^{n} \delta\gamma_i$ and the latter yields a groebner basis for $\mathrm{Ann}(s)$ (with respect to the lexicographic term order).

Our original goals were two-fold: to try and simplify the Commutative Algebra used in some early papers on the structure of 2-D cyclic codes (Imai & Arakaki (1974), Ikai, Kosako & Kojima (1975, 1976), Imai (1977), Sakata (1978, 1981)) and secondly, to better understand Sakata (1988). It seemed that this would be helped by undertaking a fundamental study of n-D sequences *per se*. (Even though our principal application is the case $n = 2$, we found that formulating and proving our results *for all* $n \geq 1$ improved and simplified the theory.) For some preliminary applications of this work to n-D cyclic codes and their duals, see Norton (1995a). An application to simplified encoding of n-D cyclic codes was presented in Norton (1995b).

We would suggest that the use of right-shifting and $R((X_1^{-1}, \ldots, X_n^{-1}))$ sharpens and simplifies the theory of both finite and linear recurring sequences: (i) Theorem 4.19 generalizes the treatment of rectilinear sequences over a field studied in Fitzpatrick & Norton (1990) to EVR sequences over an arbitrary commutative ring and does not require the "Reduction Lemma" of Fitzpatrick & Norton (1990) (ii) a *division-free* analogue of the Berlekamp-Massey algorithm in $R((X^{-1}))$, which computes a "minimal realization" $(f, \beta_0(f,s))$ of a finite sequence s over a domain R appears in Norton (1994), together with some new applications of minimal realization (iii) a theory of division-free minimal realizations of a finite n-D sequence over a domain will appear in Norton (1995d); *cf.* Sakata (1988, 1990).

The results of this paper have been applied in Chabanne & Norton (1994). In fact, the n-D key equation (*loc. cit.*, Theorem 2.4) is a special case of Corollary 4.14 over a finite field: f_i is the error-locator X_i-polynomial and $\beta_0(\prod_{i=1}^{n} f_i, s)/(X_1 \cdots X_n)$ is the error-evaluator polynomial. Indeed, the minimal realization algorithm of Norton (1994) applied to the 1-D version of our key equation gives a simpler way of decoding a t-error correcting Reed-Solomon code in at most $t(10t+1)$ multiplications, without using Forney's procedure to compute the error magnitudes for example, Norton (1995c). It seems likely that our work will also apply to decoding geometric Goppa codes.

Finally, our approach was partly suggested by the formulation for 1-D sequences given in Ferrand (1988), which uses $R((X))$ as the ambient ring. We note that $\mathbb{F}((X^{-1}))$, where $\mathbb{F}$ denotes a field, was used in Welch & Scholtz (1979) in the context of decoding BCH codes, and in Niedereiter (1988).

1.1 Notation

In general, we use lower case Roman letters for elements, Greek letters for functions and short names for sets. $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$.

Notation	**Meaning**
$\mathbf{n}$	$\{1, 2, \ldots, n\}$.
π_i	Projection of $\mathbb{Z}^n$ onto the i^{th} component, $i \in \mathbf{n}$.
X^a	Monomial $X_1^{a_1} X_2^{a_2} \ldots X_n^{a_n}$, where $a_i \in \mathbb{Z}, i \in \mathbf{n}$.
$\widehat{\mathbf{X}}_i$	Variables $X_1, X_2, \ldots, X_n$, excluding $X_i, i \in \mathbf{n}$.
P_n	Polynomials over R in $X_1, \ldots, X_n$.
L_n	Laurent series over R in $X_1^{-1}, \ldots, X_n^{-1}$.
S_n	Power series over R in $X_1^{-1}, \ldots, X_n^{-1}$.
$\delta_i g$	Degree of $g \in L_n$ as Laurent series in $X_i^{-1}, i \in \mathbf{n}$.
δg	Degree of $g \in L_n$ i.e. an n-vector.
$S^n(R)^-$	n-dimensional sequences over R, indexed by $-\mathbb{N}^n$.
$f \circ s$	Polynomial f acting on sequence s by shifting.
$\beta_0(f, s)$	Border polynomial of f and s.
$\mathrm{Ann}(s)$	Characteristic ideal of s.
$\gamma(s)$	Primitive generator of $\mathrm{Ann}(s)$, $s \in S^1(R)^-$, R factorial.
$s^{(i,*)}$	s regarded as an element of $S^1(R[[\widehat{\mathbf{X}}_i^{-\mathbf{1}}]])^-$.
$\Gamma(s)$	Generating function of s, as element of S_n.

We equate sums and products over the empty set to 0 and 1 respectively.

2 Preliminaries

2.1 $\mathbb{Z}^n$

Throughout the paper, $n \geq 1$ and $\mathbf{n} = \{1, 2, \ldots, n\}$. Addition and negation in $\mathbb{Z}^n$ are componentwise; thus we can write $-\mathbb{N}^n = (-\mathbb{N})^n$. We let $\mathbf{0}, \mathbf{1}$ be the points in $\mathbb{Z}^n$ with all components $0, 1$ respectively.

For $i \in \mathbf{n}$, $\pi_i : \mathbb{Z}^n \to \mathbb{Z}$ is the projection onto the i^{th} factor; for $a \in \mathbb{Z}^n$, we also write a_i for $\pi_i a$.

$\mathbb{Z}^n$ is *partially ordered* by the relation $\leq$ on each component: $a \leq b$ iff $a_i \leq b_i$ *for all* $i \in \mathbf{n}$; $a \geq b$ is synonymous with $b \leq a$. We write $a \not\geq b$ to mean that $a \geq b$ is false, that is, *for some* $i \in \mathbf{n}$, $a_i < b_i$.

We generalize the usual interval notation in $\mathbb{Z}$ to describe certain subsets of $\mathbb{Z}^n$:
for $a, b \in \mathbb{Z}^n$,

$$(-\infty, a] = \{c \in \mathbb{Z}^n \ : \ c \leq a\} \text{ and } [a, \infty) = \{c \in \mathbb{Z}^n \ : \ a \leq c\}$$

$$[a, b] = \{c \in \mathbb{Z}^n \ : \ a \leq c \leq b\} = \prod_{i=1}^{n} [a_i, b_i]$$

$$(a, b] = \{c \in \mathbb{Z}^n \ : \ a \not\geq c \leq b\} = (-\infty, b] \setminus (-\infty, a]$$

$$[a, b) = \{c \in \mathbb{Z}^n \ : \ a \leq c \not\geq b\} = [a, \infty) \setminus [b, \infty).$$

2.2 Polynomials and Laurent series

R is a commutative ring with $1 \neq 0$ and P_n denotes the ring of R-polynomials in $X_1, \ldots, X_n$; L_n denotes the ring of Laurent series in $X_1^{-1}, \ldots, X_n^{-1}$, which contains P_n. Indeed, L_n is a P_n-module which has P_n as standard P_n-submodule, where the action of X_i is *a shift to the right.* $S_n \subseteq L_n$ denotes the ring of R-power series in $X_1^{-1}, \ldots, X_n^{-1}$.

For $a \in \mathbb{Z}^n$, we abbreviate $X_1^{a_1} X_2^{a_2} \ldots X_n^{a_n}$ to X^a. For $i \in \mathbf{n}$, $\widehat{\mathbf{X}}_i$ denotes the variables $X_1, \ldots, X_n$, excluding X_i.

For $G \in L_n \setminus \{0\}$, G_a denotes a coefficient of G, and $\mathrm{Supp}(G) = \{a \in \mathbb{Z}^n : G_a \neq 0\}$ is called the *support* of G; $\mathrm{Supp}(0) = \emptyset$. If $G \in L_n$ and $A \subseteq \mathbb{Z}^n$, then $G|A = \sum_{a \in A \cap \mathrm{Supp}(G)} G_a X^a$.

We use the (exponential) valuation on $R((X^{-1}))$, which extends the degree function on $R[X]$. For convenience, we also denote it by δ; $\delta 0 = -\infty$. Thus for $G \in R((X^{-1})) \setminus \{0\}$, $\delta G = \max \mathrm{Supp}(G)$ and for $G, H \in R((X^{-1})), \delta(GH) \leq \delta G + \delta H$.

For $G \in L_n$ and $i \in \mathbf{n}$, we let $\delta_i G$ be the i^{th} *partial degree* of G, that is, the degree of G regarded as a Laurent series in X_i^{-1}; δG is the n-vector with components $\delta_i G$. We have $\mathrm{Supp}(G) \subseteq (-\infty, \delta G]$.

The letter f will always mean an element of P_n and we write $f = f(X) = \sum_{a \in \mathrm{Supp}(f)} f_a \ X^a$.

$\mathrm{Supp}(f) \subseteq [\mathbf{0}, \delta f]$, and so for $a \in \mathrm{Supp}(f)$, $\delta f - a$ is a well-defined point in $\mathbb{N}^n$. If $f \neq 0$, the reciprocal of f is $f^* = X^{\delta f} \ f(X^{-\mathbf{1}}) = \sum_{a \in \mathrm{Supp}(f)} f_a \ X^{\delta f - a}$ and $0^* = 0$. It is easy to verify that $f = X^{\delta f - \delta f^*} f^{**}$.

2.3 Linear recurring sequences

$S^n(R)^-$ denotes the set of functions $-\mathbb{N}^n \to R$ i.e. the set of R-sequences indexed by $-\mathbb{N}^n$; the value $s(a)$ is written s_a. *The letter s will always denote a sequence in $S^n(R)^-$*, and to avoid trivial cases, we assume that s is non-zero. With addition and scalar product defined componentwise, $S^n(R)^-$ becomes a unitary R-module. Further, the unit sequence and the Hadamard product make $S^n(R)^-$ into a commutative R-algebra with 1. In particular, its ideals are algebra ideals. There is

a *right* shift action of P_n on $S^n(R)^-$ given by

$$\left(\sum_{\mathbf{0}\le a\le \delta f} f_a X^a \circ s\right)_b = \sum_{\mathbf{0}\le a\le \delta f} f_a s_{b-a}$$

where $b \le \mathbf{0}$. This makes $S^n(R)^-$ into a P_n-module.

DEFINITION 2.1 *The* annihilator or characteristic ideal *of (characteristic polynomials) of s is* $\mathrm{Ann}(s) = \{f \in P_n : f \circ s = 0\}$. *We say that s is a* (homogeneous) n-dimensional linear recurring sequence (n-D lrs) *if* $\mathrm{Ann}(s) \neq \{0\}$.

EXAMPLE 2.2 *(a) Let $a \ge \mathbf{0}$. Then $s_b = 0$ for $b \le -a \iff X^a \in \mathrm{Ann}(s)$.*

(b) Let $r \in R \setminus \{0\}$, $a \le \mathbf{0}$ and $s_a = r^{-\sum_{i=1}^n a_i}$. Then $X - r^n \in \mathrm{Ann}(s)$.

(c) If $s \in S^2(R)^-$ then $s_{a-1,b} = s_{a,b} = s_{a,b-1}$ for $a, b \le \mathbf{0} \iff X_1 - 1, X_2 - 1 \in \mathrm{Ann}(s)$.

(d) We say that s is n-periodic *if for some $d \ge \mathbf{1}$, $s_{a-d_i} = s_a$ for all $a \le \mathbf{0}$ and $i \in \mathbf{n}$ i.e. s is n-periodic iff for some $d \ge \mathbf{1}$, $X_i^{d_i} - 1 \in \mathrm{Ann}(s)$ for all $i \in \mathbf{n}$; s is* eventually n-periodic *if for some $d \ge \mathbf{1}$, $e \ge \mathbf{0}$, $X_i^{e_i}(X_i^{d_i} - 1) \in \mathrm{Ann}(s)$ for all $i \in \mathbf{n}$.*

We now generalize the notion of a rectilinear n-D lrs over a field $\mathbb{F}$ from Fitzpatrick & Norton (1990). (Recall that s is rectilinear if for all $i \in \mathbf{n}$, there is an $f_i \in \mathrm{Ann}(s) \cap \mathbb{F}[X_i]$ with $\delta f_i \ge 1$ and $f_i(0) \neq 0$.)

DEFINITION 2.3 *We say that s is* eventually rectilinear *(EVR) if for all $i \in \mathbf{n}$, there is an $f_i \in \mathrm{Ann}(s) \cap R[X_i]$ with $\delta f_i \ge 1$.*

If R is a domain and s is non-zero, then s is EVR $\iff \mathrm{Ann}(s) \cap R[X_i] \neq \{0\}$ for all $i \in \mathbf{n}$.

EVR sequences include 1-D lrs over a commutative ring, eventually periodic lrs (Nerode (1958)), rectilinear lrs over a field (Fitzpatrick & Norton (1990)) and "n-linearly recursive functions over a field" (Cerlienco & Piras (1991)). If s is EVR and $g \in P_n$, then $g \circ s$ is EVR since $f \circ (g \circ s) = (fg) \circ s = g \circ (f \circ s)$.

EXAMPLE 2.4 *(a) Let $s \in S^2(R)^-$ satisfy $s_{0,j} = 1$ for $j \le 0$ and $s_{i,j} = 0$ otherwise. Then $X_1,\ X_2 - 1 \in \mathrm{Ann}(s)$, so that s is EVR. It is easy to check that $\mathrm{Ann}(s) \cap R[X_1] = (X_1)$, so that s is not rectilinear.*

(b) Let $s' \in S^2(R)^-$ satisfy $s'_{a,b} = 1$ if $a = b$ and $s'_{a,b} = 0$ otherwise. Then $X_1X_2 - 1 \in \mathrm{Ann}(s')$ but $\mathrm{Ann}(s') \cap R[X_i] = \{0\}$ for $i = 1,\ 2$:

if $f = \sum_{a=0}^{\delta f} f_a X_1^a \in R[X_1]$ and $f \circ s' = 0$ then for $0 \le b \le \delta f$,

$$f_b = \sum_{a=0}^{\delta f} f_a s'_{-a,-b} = \left(\sum_{a=0}^{\delta f} f_a X_1^a \circ s'\right)_{0,-b} = 0.$$

Similarly, $\mathrm{Ann}(s') \cap R[X_2] = \{0\}$. *Thus* s' *is* not *EVR. In particular, a 2-D lrs over GF(2) need not be 2-periodic (in contrast to the 1-D situation).*

In the literature, the standard approach to n-D lrs is to regard $S^n(R) = \{s : \mathbb{N}^n \to R\}$ as a P_n-module via *left* shifting (which we also denote by $\circ$):

$$\left(\sum_{\mathbf{0} \le a \le \delta f} f_a X^a \circ s \right)_b = \sum_{\mathbf{0} \le a \le \delta f} f_a s_{b+a}$$

where $b \ge \mathbf{0}$.

PROPOSITION 2.5 *The map* $^- : S^n(R) \to S^n(R)^-$ *given by* $(s^-)_a = s_{-a}$ *for* $a \le \mathbf{0}$ *is a* P_n*-module map.*

PROOF. Let $s \in S^n(R)$, $b \le \mathbf{0}$ and $f = \sum_{\mathbf{0} \le a \le \delta f} f_a X^a \in P_n$. Then

$$(f \circ s)^-_b = (f \circ s)_{-b} = \sum_{\mathbf{0} \le a \le \delta f} f_a s_{-b+a} = \sum_{\mathbf{0} \le a \le \delta f} f_a s^-_{b-a} = (f \circ s^-)_b$$

so that $(f \circ s)^- = f \circ s^-$. It is trivial that $^-$ preserves addition, so $^-$ is a P_n-module map. □

There is an obvious two-sided inverse of $^-$, so that $S^n(R)^-$ and $S^n(R)$ are isomorphic P_n-modules, s is an lrs iff s^- is an lrs, and $^-$ induces an isomorphism of $\mathrm{Ann}(s)$ and $\mathrm{Ann}(s^-)$.

2.4 $\mathrm{Ann}(s)$ and generating functions

The *generating function* of s is

$$\Gamma(s) = \sum_{a \le \mathbf{0}} s_a X^a \in S_n.$$

Strictly speaking, the definition of $\Gamma(s)$ should incorporate a linear (total) ordering on $-\mathbb{N}^n$; this has been omitted since the enumeration will either be clear or not used. Thus for Example 2.4, $\Gamma(s) = X_2/(X_2 - 1)$ and $\Gamma(s') = X_1X_2/(X_1X_2 - 1)$.

Since $\delta(f\Gamma(s)) \le \delta f$, we have $\mathrm{Supp}(f\Gamma(s)) \subseteq (-\infty, \delta f]$.

PROPOSITION 2.6 $(f\Gamma(s))|(-\infty,\mathbf{0}] = \Gamma(f \circ s)$.

PROOF. If $a \le \mathbf{0}$ and $f = \sum_{\mathbf{0} \le b \le \delta f} f_b X^b$, then $(f\Gamma(s))_a = \sum_{\mathbf{0} \le b \le \delta f} f_b s_{a-b} = (f \circ s)_a$. □

We note that Lemma 4.1 of Fitzpatrick & Norton (1990) is an analogue of the preceding result for left-shifting.

PROPOSITION 2.7 *The following are equivalent:*

(a) $f \in \mathrm{Ann}(s)$

(b) $(f\Gamma(s))|(-\infty,\mathbf{0}] = 0$

(c) $\mathrm{Supp}(f\Gamma(s)) \subseteq (\mathbf{0},\delta f]$

(d) $\exists G \in L_n$ *such that* $f\Gamma(s) = XG$ *and* $\mathrm{Supp}(G) \subseteq (-\mathbf{1},\ \delta f - \mathbf{1}]$.

PROOF. We omit the proof that (a) $\iff$ (b) $\iff$ (c). (c) $\iff$ (d): It is a straightforward exercise that $\mathrm{Supp}(f\Gamma(s)) \subseteq (\mathbf{0},\delta f] \iff \mathrm{Supp}(X^{-\mathbf{1}} f\Gamma(s)) \subseteq (-\mathbf{1},\delta f - \mathbf{1}]$. □

Setting $n = 1$ in Proposition 2.7, we obtain a simple characterization of $\mathrm{Ann}(s)$ which does not use δf or the reciprocal of f (*cf.* Niederreiter (1988), Lemmas 1, 2 when R is a field):

COROLLARY 2.8 *Let* $s \in S^1(R)^-$. *Then* $f \in \mathrm{Ann}(s) \iff f\Gamma(s) \in XR[X]$.

COROLLARY 2.9 *Let* s *be an lrs. Then* $\Gamma(s) = XG/f$ *for some non-zero* $f \in \mathrm{Ann}(s)$ *and* $G \in L_n$ *such that* $\mathrm{Supp}(G) \subseteq (-\mathbf{1},\ \delta f - \mathbf{1}]$.

Conversely, if f *is monic,* $G \in L_n$ *and* $\mathrm{Supp}(G) \subseteq (\text{-}\mathbf{1},\ \delta f - \mathbf{1}]$, *then* $XG/f \in S_n$ *and* s *defined by* $\Gamma(s) = XG/f$ *is an lrs with* $f \in \mathrm{Ann}(s)$.

PROOF. If f is monic, then $u = X^{-\delta f} f$ is a unit in S_n. Writing $G = \sum_{a\in(-\mathbf{1},\delta f-\mathbf{1}]} G_a X^a$, we obtain

$$XGu = f \sum_{a\in(-\mathbf{1},\delta f-\mathbf{1}]} G_a\ X^{a+\mathbf{1}-\delta f} = f \sum_{b\in(-\delta f,\mathbf{0}]} G_{b-\mathbf{1}+\delta f}\ X^b = fH$$

say, where $H \in S_n$ and so $XG/f = H/u \in S_n$. The result now follows from Proposition 2.7. □

"Rational lrs" are an important special case of Corollary 2.9:

DEFINITION 2.10 *We will say that* s *is a* rational *lrs if for some* $f \in P_n \setminus \{0\},\ f \cdot \Gamma(s) \in XP_n$.

Certainly every 1-D lrs is rational, but this fails for $n \geq 2$: if $G(X_1^{-1}) \in S_1$ is not a rational function, $f \in P_n$, $\delta f \geq \mathbf{1}$, and s is defined by $\Gamma(s) = \widehat{\mathbf{X}}_1 G/f$, then $f \in \mathrm{Ann}(s)$, but s is not rational. Example 2.4(b) shows that for $n \geq 2$, not all rational lrs are EVR. We will see in Theorem 4.9 below that EVR lrs are always rational.

For completeness, we now give an analogue of Corollary 2.9 for sequences indexed by $\mathbb{N}^n$ which use left-shifting (Corollary 2.12 below). This analogue could have been deduced from Propositions 2.5, 2.7 and an analogue of Proposition 2.7, but it is easier to appeal directly to the definitions:

LEMMA 2.11 *Let* $a \geq \mathbf{0}$ *and* $s : \mathbb{N}^n \to R$ *(so that* $\Gamma(s) \in R[[X]]$*). Then*

$$X^a f^* \in \mathrm{Ann}(s) \iff \mathrm{Supp}(f\Gamma(s)) \subseteq [\mathbf{0}, a + \delta f).$$

In particular, if $\mathrm{Supp}(f\Gamma(s)) \subseteq [\mathbf{0},\delta f)$, *then* $f^* \in \mathrm{Ann}(s)$.

PROOF. For any $b \geq \mathbf{0}$,

$$\begin{aligned}(X^a f^* \circ s)_b &= \left(\sum_{c\in\mathrm{Supp}(f)} f_c X^{a+\delta f-c} \circ s\right)_b \\ &= \sum_{c\in\mathrm{Supp}(f)} f_c s_{b+a+\delta f-c} = (f\Gamma(s))_{a+b+\delta f}\end{aligned}$$

and so

$$X^a f^* \in \mathrm{Ann}(s) \iff (f\Gamma(s))|[a+\delta f,\infty) = 0 \iff \mathrm{Supp}(f\Gamma(s)) \subseteq [\mathbf{0}, a+\delta f).$$

□

COROLLARY 2.12 *Let* $s : \mathbb{N}^n \to R$ *be an lrs. Then* $\Gamma(s) = G/f^*$ *for some non-zero* $f \in \mathrm{Ann}(s)$ *and* $G \in R[[X]]$ *such that* $\mathrm{Supp}(G) \subseteq [\mathbf{0},\ \delta f)$.

Conversely, suppose that $f(\mathbf{0}) = 1$ *and* $G \in R[[X]]$ *satisfies* $\mathrm{Supp}(G) \subseteq [\mathbf{0},d)$ *for some* $d \in \mathbb{N}^{\mathbf{n}} \setminus \{\mathbf{0}\}$. Define $m \in \mathbb{N}^n$ by

$$\pi_i m = \max\{0, d_i - \delta_i f\}.$$

If s is the n-D lrs with $\Gamma(s) = G/f$ and $a \geq m$, then $X^a f^* \in \mathrm{Ann}(s)$.

PROOF. The first part is an easy consequence of Lemma 2.11 applied to $f = X^{\delta f-\delta f^*}(f^*)^*$.

For the converse, if $a \geq m$, then $a \geq \mathbf{0}$ and $d \leq a+\delta f$. Therefore $[\mathbf{0},d) \subseteq [\mathbf{0},a+\delta f)$, so the result follows from Lemma 2.11. □

Here, rational lrs correspond to $\Gamma(s) = g/f^*$, where $f, g \in P_n$, $\delta f \geq \mathbf{1}$ and $\delta g \leq \delta f - \mathbf{1}$; in this case, we can take $d = \delta g + \mathbf{1}$ in Corollary 2.12. If in addition $n = 1$ in Corollary 2.12, we obtain Fitzpatrick & Norton (1995), Theorem 4.1.

3 A decomposition formula for $f \cdot \Gamma(s)$

3.1 The border partition

For $d \geq \mathbf{1}$, $(-\infty,d] = \prod_{i=1}^n (-\infty,d_i]$ and so

$$\beta(-\infty,d] = \prod_{i=1}^n \{(-\infty,0],[1,d_i]\}$$

is a partition of $(-\infty,d]$. We will abbreviate $\beta(-\infty,d]$ to β when d is understood.

It is convenient to use binary notation to index the 2^n members of the product partition $\beta(-\infty, d]$: for $0 \leq k \leq 2^n - 1$, we write the (n-bit) binary representation of k with the most significant bit $b_n(k)$ of k on the right (so that the bit ordering is the same as the ordering of the components of $\mathbb{Z}^n$) and index the k^{th} member $\beta_k(-\infty, d]$ of $\beta(-\infty, d]$ by

$$b_i(k) = 1 \text{ iff } \pi_i(\beta_k(-\infty, d]) = (-\infty, 0].$$

For example, if $n = 2$, $\beta_0 = \beta_{00} = [1, d_1] \times [1, d_2]$, $\beta_1 = \beta_{10} = [1, d_1] \times (-\infty, d_2]$, $\beta_2 = \beta_{01} = (-\infty, d_1] \times [1, d_2]$ etc.; notice that $\beta_0 \cup \beta_1 \cup \beta_2$ "borders" $\beta_3 = (-\infty, \mathbf{0}]$ in $(-\infty, d]$.

We will call $\bigcup\{\beta_k(-\infty, d] \ : 0 \leq k < 2^n - 1\}$ the *border* of $(-\infty, \mathbf{0}]$ in $(-\infty, d]$ and $\beta(-\infty, d]$ the *border partition* of $(-\infty, d]$.

3.2 The border polynomial

DEFINITION 3.1 *Let $\delta f \geq \mathbf{1}$ and let β be the border partition of $(-\infty, \delta f]$. For $0 \leq k \leq 2^n - 1$, we define $\beta_k(f, s) \in L_n$ by*

$$\beta_k(f, s) = (f \cdot \Gamma(s)) \mid \beta_k.$$

PROPOSITION 3.2 *Let $\delta f \geq \mathbf{1}$ and let β be the border partition of $(-\infty, \delta f]$. Then*

$$f \cdot \Gamma(s) = \sum_{k=0}^{2^n - 1} \beta_k(f, s)$$

where $\mathrm{Supp}(\beta_k(f, s)) \subseteq \beta_k$ *for* $0 \leq k \leq 2^n - 1$ *and* $\beta_{2^n - 1}(f, s) = \Gamma(f \circ s)$.

PROOF. This follows immediately from the fact that β is a partition of $(-\infty, \delta f]$ and from Proposition 2.6. □

Since $\beta_0(f, s) \in P_n$, we call it the *border polynomial* of f and s. We will express $\beta_0(f, s)$ in terms of s and generalized Newton divided differences of f. Recall Newton's divided difference operator ν for $n = 1$:

$\nu : R[X] \to R[X]$ is $\nu f = (f - f_0)/X$, and for $a \geq 1$, ν^a is defined iteratively by $\nu^0 f = f$ and $\nu^a = \nu\nu^{a-1}$. It is easy to see that if $d \geq 1$ and $f = f_0 + f_1 X + \ldots + f_d X^d$, then for $0 \leq a \leq d$,

$$\nu^a f = f_a \ + \ f_{a+1} \ X + \ldots + \ f_d X^{d-a} = \sum_{b=a}^{d} f_b X^{b-a}$$

whereas $\nu^a f = 0$ if $a > \delta f$. Thus $\delta(\nu^a f) = \delta f - a$ if $0 \leq a \leq \delta f$.

DEFINITION 3.3 *For $n \geq 1$, $a \geq \mathbf{0}$ and $f \in P_n$, we define*

$$\nu^a f = (f \mid [a, \delta f]) \, / X^a.$$

Clearly $\nu^{\mathbf{0}} f = f$ and the numerator is divisible by X^a. Indeed, if $\mathbf{0} \leq a \leq \delta f$, then $\nu^a f = \sum_{a \leq b \leq \delta f} f_b X^{b-a}$ and $\delta(\nu^a f) \leq \delta f - a$. For example, if $\delta f = (2,3)$ then

$$\nu^{(1,1)} f = f_{1,1} + f_{1,2} X_2 + f_{2,1} X_1 + f_{1,3} X_2^2 + f_{2,2} X_1 X_2 + f_{2,3} X_1 X_2^2.$$

On the other hand, if $a \geq \delta f + \mathbf{1}$, then $\nu^a f = 0$. When $n = 1$, ν^a coincides with Newton's operator.

LEMMA 3.4 *If $\delta f \geq \mathbf{1}$, then*

$$\beta_0(f,s) = X \sum_{\mathbf{0} \leq a \leq \delta f - \mathbf{1}} s_{-a}\ \nu^{a+\mathbf{1}} f.$$

PROOF.

$$\begin{aligned}
\beta_0(f,s) &= \sum_{\mathbf{1} \leq a \leq \delta f} \left(f\Gamma(s)\right)_a X^a \\
&= \sum_{\mathbf{1} \leq a \leq \delta f} \left(\sum_{a \leq b \leq \delta f} f_b s_{a-b} \right) X^a \\
&= \sum_{\mathbf{1} \leq a \leq \delta f} \left(\sum_{\mathbf{0} \leq c \leq \delta f - a} f_{a+c} s_{-c} X^a \right) \\
&= \sum_{\mathbf{0} \leq c \leq \delta f - \mathbf{1}} s_{-c} \left(\sum_{\mathbf{1} \leq a \leq \delta f - c} f_{a+c} X^a \right) \\
&= \sum_{\mathbf{0} \leq c \leq \delta f - \mathbf{1}} s_{-c} \left(\sum_{c+\mathbf{1} \leq d \leq \delta f} f_d X^{d-c} \right) \\
&= X \sum_{\mathbf{0} \leq c \leq \delta f - \mathbf{1}} s_{-c} \left(\sum_{c+\mathbf{1} \leq d \leq \delta f} f_d X^{d-(c+\mathbf{1})} \right) \\
&= X \sum_{\mathbf{0} \leq c \leq \delta f - \mathbf{1}} s_{-c}\ \nu^{c+\mathbf{1}} f.
\end{aligned}$$

□

Setting $n = 1$, we obtain the following result (*cf.* Ferrand (1988), Section 1.3):

COROLLARY 3.5 *If $n = 1$ and $\delta f \geq 1$, then*

$$f\Gamma(s) = X \sum_{a=0}^{\delta f - 1} s_{-a}\ \nu^{a+1} f\ + \Gamma(f \circ s).$$

3.3 The Border Laurent Series

We have determined the summands $\beta_k(f,s)$ of $f \cdot \Gamma(s)$ in Proposition 3.2 for $k = 0,\ 2^n - 1$. In this subsection, we determine the remaining summands (when $n \geq 2$).

If $0 < k < 2^n - 1$, then for some $i, j,\ 1 \le i, j \le n,\ b_i(k) = 0$ and $b_j(k) = 1$, so that for these $i, j,\ \beta_k(f,s)$ involves polynomials in X_i and power series in X_j^{-1}. For this reason, we call $\{\beta_k(f,s) \ : \ 0 < k < 2^n - 1\}$ the *border Laurent series of f and s*.

In order to discuss these series, we need to extend some of our earlier definitions:

$\mathbf{i}$ denotes a subset of $\mathbf{n} = \{1, 2, \ldots, n\}$ with cardinality $|\mathbf{i}|$ and $\mathbf{i}' = \mathbf{n} \setminus \mathbf{i}$; $\mathbf{i} \ll \mathbf{n}$ means that $\mathbf{i}$ is a *proper* subset of $\mathbf{n}$. If $\mathbf{i} \ll \mathbf{n}$ and $a \in \mathbb{N}^{\mathbf{i}}$, $X_{\mathbf{i}}^a$ has the obvious meaning and for $1 \le i \le n$, we write X_i for $X_{\{i\}}$. We let $\pi_{\mathbf{i}}$ be the projection of $\mathbb{Z}^n$ onto $\mathbb{Z}^{\mathbf{i}}$. If $a \in \mathbb{Z}^{\mathbf{i}}$ and $a' \in \mathbb{Z}^{\mathbf{i}'}$, then (a, a') is the unique element of $\mathbb{Z}^n$ with $\pi_{\mathbf{i}}(a, a') = a$ and $\pi_{\mathbf{i}'}(a, a') = a'$. Lastly, for $\delta f \ge \mathbf{1},\ \delta_{\mathbf{i}} f = \pi_{\mathbf{i}} \delta f$.

DEFINITION 3.6 *Let $n \ge 2$ and $\mathbf{i} \ll \mathbf{n}$.*

*(a) For $a \in -\mathbb{N}^{\mathbf{i}}$, the a-*section *of s is $s^{(a)} \in S^{|\mathbf{i}'|}(R)$ given by*

$$s^{(a)}_{a'} = s_{(a,a')}$$

for $a' \in -\mathbb{N}^{\mathbf{i}'}$.

*(b) For $\mathbf{0} \le a \le \delta_{\mathbf{i}} f$, the a-*section *of f is $f^{(a)} \in R[X_{\mathbf{i}'}]$ given by*

$$f^{(a)}(X_{\mathbf{i}'}) = \sum_{\mathbf{0}' \le a' \le \delta_{\mathbf{i}'} f} f_{(a,a')} X_{\mathbf{i}'}^{a'}.$$

Clearly $\delta f^{(a)} \le \delta_{\mathbf{i}'} f$ and for $\mathbf{0}' \le a' \le \delta(f^{(a)}),\ f^{(a)}_{a'} = f_{(a,a')}$.

We will simplify the main result of this subsection by using the following technical definition:

DEFINITION 3.7 *Let $n \ge 2$ and $\delta f \ge \mathbf{1}$. For $\mathbf{i} \ll \mathbf{n}$, let $\delta = \delta_{\mathbf{i}} f$ and $\delta' = \delta_{\mathbf{i}'} f$. We will write the sum of "cross-products of sections"*

$$X_{\mathbf{i}'} \sum_{\mathbf{0} \le a \le \delta} \ \sum_{\mathbf{0}' \le a' \le \delta' - \mathbf{1}'} \left(\nu^{a'+\mathbf{1}'} f^{(a)}\right)(X_{\mathbf{i}'}) \cdot \Gamma\left(X_{\mathbf{i}}^a \circ s^{(-a')}\right)(X_{\mathbf{i}}^{-\mathbf{1}})$$

as $\beta_{\mathbf{i}}^{\times}(f,s)(X_{\mathbf{i}}^{-\mathbf{1}}, X_{\mathbf{i}'})$ for short.

Notice that $\beta_{\mathbf{i}}^{\times}(f,s)(X_{\mathbf{i}}^{-\mathbf{1}}, X_{\mathbf{i}'}) \in L_n$. In fact it belongs to $(R[X_{\mathbf{i}'}])\,[[X_{\mathbf{i}}^{-\mathbf{1}}]]$. We will also abbreviate $\beta_{\mathbf{i}}^{\times}(f,s)(X_{\mathbf{i}}^{-\mathbf{1}}, X_{\mathbf{i}'})$ to $\beta_{\mathbf{i}}^{\times}(f,s)$.

For $n = 2$ and continuing the notation of the definition, $\mathbf{i} = \{1\}$ or $\{2\}$, and

$$\beta_{\{1\}}^{\times}(f,s)(X_1^{-1}, X_2) = X_2 \sum_{a=0}^{\delta} \sum_{a'=0}^{\delta'-1} \left(\nu^{a'+1} f^{(a)}\right)(X_2) \cdot \Gamma\left(X_1^a \circ s^{(-a')}\right)(X_1^{-1})$$

$$\beta_{\{2\}}^{\times}(f,s)(X_2^{-1}, X_1) = X_1 \sum_{a=0}^{\delta} \sum_{a'=0}^{\delta'-1} \left(\nu^{a'+1} f^{(a)}\right)(X_1) \cdot \Gamma\left(X_2^a \circ s^{(-a')}\right)(X_2^{-1})$$

where ν denotes the usual divided difference operator.

For $0 < k < 2^n - 1$, we define $\mathbf{i}(k) = \{i \in \mathbf{n} \ : \ b_i(k) = 1\} \ll \mathbf{n}$. Thus if $\delta f \ge \mathbf{1}$, $\mathbf{i}(k)$ is the set of i for which $\pi_i \beta_k(-\infty, \delta f]$ is infinite.

THEOREM 3.8 *Let $n \geq 2$, $0 < k < 2^n - 1$, and let $\mathbf{i} = \mathbf{i}\,(k)$. Then for $\delta f \geq \mathbf{1}$, the k^{th} border Laurent series of f and s is*

$$\beta_k(f,s) = \beta^{\times}_{\mathbf{i}}(X_{\mathbf{i}}^{\mathbf{-1}}, X_{\mathbf{i}'}).$$

PROOF.

$$\begin{aligned}
\beta_k(f,s) &= \sum_{(a,a')\in\beta_k(-\infty,\delta f]\cap \mathrm{Supp}(f\Gamma)} (f\Gamma)_{(a,a')}\, X^{(a,a')} \\
&= \sum_{a\leq \mathbf{0},\ \mathbf{1}'\leq a'\leq \delta'} \left(\sum_{(a,a')\leq b\leq(\delta,\delta')} f_b\ s_{(a,a')-b} \right) X^{(a,a')} \\
&= \sum_{a\leq \mathbf{0},\ \mathbf{1}'\leq a'\leq \delta'} \left(\sum_{(\mathbf{0},\mathbf{0}')\leq(c,c')\leq(\delta,\delta')-(a,a')} f_{(a,a')+(c,c')}\ s_{-(c,c')} \right) X^{(a,a')} \\
&= \sum_{a\leq \mathbf{0},\ \mathbf{0}'\leq c'\leq \delta'-\mathbf{1}'} \left(\sum_{\mathbf{0}\leq c\leq \delta-a,\ \mathbf{1}'\leq a'\leq \delta'} f_{(a,a')+(c,c')}\ s_{-(c,c')} \right) X_{\mathbf{i}}^{a} X_{\mathbf{i}'}^{a'} \\
&= \sum_{d\leq \mathbf{0},\ \mathbf{0}'\leq c'\leq \delta'-\mathbf{1}'} \left(\sum_{\mathbf{0}\leq c\leq \delta-d,\ c'+\mathbf{1}'\leq d'\leq \delta'} f_{(c+d,d')}\ s_{-(c,c')} \right) X_{\mathbf{i}}^{d} X_{\mathbf{i}'}^{d'-c'} \\
&= X_{\mathbf{i}'} \sum_{d\leq \mathbf{0},\ \mathbf{0}'\leq e'\leq \delta'-\mathbf{1}'} \left(\sum_{d\leq e\leq \delta,\ e'+\mathbf{1}'\leq d'\leq \delta'} f_{(e,d')} X_{\mathbf{i}'}^{d'}\ s_{(d-e,e')} \right) X_{\mathbf{i}}^{d} \\
&= X_{\mathbf{i}'} \sum_{\mathbf{0}\leq e\leq \delta,\ \mathbf{0}'\leq e'\leq \delta'-\mathbf{1}'} \left(\sum_{d\leq \mathbf{0},\ e'+\mathbf{1}'\leq d'\leq \delta'} f_{(e,d')} X_{\mathbf{i}'}^{d'-(e'+\mathbf{1}')}\ s_{(d-e,e')} X_{\mathbf{i}}^{d} \right) \\
&= X_{\mathbf{i}'} \sum_{\mathbf{0}\leq e\leq \delta,\ \mathbf{0}'\leq e'\leq \delta'-\mathbf{1}'} \left(\sum_{e'+\mathbf{1}'\leq d'\leq \delta'} f_{d'}^{(e)} X_{\mathbf{i}'}^{d'-(e'+\mathbf{1}')} \right) \cdot \left(\sum_{d\leq \mathbf{0}} \left(X_{\mathbf{i}}^{e} \circ s^{(-e')} \right)_d X_{\mathbf{i}}^{d} \right) \\
&= X_{\mathbf{i}'} \sum_{\mathbf{0}\leq e\leq \delta,\ \mathbf{0}'\leq e'\leq \delta'-\mathbf{1}'} \left(\nu^{e'+\mathbf{1}'} f^{(e)} \right)(X_{\mathbf{i}'}) \cdot \Gamma\left(X_{\mathbf{i}}^{e} \circ s^{(-e')} \right)(X_{\mathbf{i}}^{\mathbf{-1}}) \\
&= \beta^{\times}_{\mathbf{i}}(X_{\mathbf{i}}^{\mathbf{-1}}, X_{\mathbf{i}'}).
\end{aligned}$$

□

Let $\delta f \geq \mathbf{1}$. To simplify the notation, we let

$$\beta^{\times}_{\mathbf{i}(0)}(f,s) = X \sum_{\mathbf{0}\leq a\leq \delta f-\mathbf{1}} s_{-a}\ \nu^{a+\mathbf{1}} f,$$

which is just $\beta_0(f,s)$ by Lemma 3.4.

COROLLARY 3.9 *Let $\delta f \geq \mathbf{1}$.*

(a)

$$f\cdot\Gamma(s) = \sum_{k=0}^{2^n-2} \beta^{\times}_{\mathbf{i}(k)}(f,s) + \Gamma(f\circ s)$$

where $\mathrm{Supp}(\beta^{\times}_{\mathbf{i}(k)}(f,s)) \subseteq \beta_k(-\infty, \delta f]$ *for* $0 \le k \le 2^n - 2$.

(b) $f \in \mathrm{Ann}(s)$ *if, and only if*

$$\Gamma(s) = \left(\sum_{k=0}^{2^n-2} \beta^{\times}_{\mathbf{i}(k)}(f,s) \right) / f.$$

(c) If f *is monic,* $G \in L_n$ *and* $\mathrm{Supp}(G) \subseteq (\mathbf{-1}, \delta f - \mathbf{1}]$*, then* $XG/f \in S_n$ *and* s *defined by* $\Gamma(s) = XG/f$ *is an lrs with* $f \in \mathrm{Ann}(s)$*, and* $XG = \sum_{k=0}^{2^n-2} \beta^{\times}_{\mathbf{i}(k)}(f,s)$.

PROOF. These are immediate consequences of Proposition 2.6, Corollary 2.9, Lemma 3.4 and Theorem 3.8. □

We now state an analogue of the previous corollary for sequences $\mathbb{N}^n \to R$ and left-shifting. In this case, $\prod_{i=1}^{n} \{[-\delta_i f, -1], [0, \infty)\}$ is to be used as the "border partition" $\{\beta_k[-\delta f, \infty) : 0 \le k \le 2^n - 1\}$ of $[-\delta f, \infty)$.

COROLLARY 3.10 *Let* $\delta f \ge \mathbf{1}$*. If* $s : \mathbb{N}^n \to R$ *(so that* $\Gamma(s) \in R[[X]]$*), then*

(a)

$$f^*\Gamma(s) = \sum_{k=0}^{2^n-2} \beta^{\star}_{\mathbf{i}(k)}(f,s) + X^{\delta f}\Gamma(f \circ s)$$

where

$$\beta^{\star}_{\mathbf{i}(0)}(f,s) = X^{\delta f}\ \beta^{\times}_{\mathbf{i}(0)}(f,s)(X^{-\mathbf{1}}) \text{ and } \beta^{\star}_{\mathbf{i}(k)}(f,s) = X^{\delta f}\beta^{\times}_{\mathbf{i}(k)}(f,s)(X_{\mathbf{i}}, X_{\mathbf{i}'}^{-\mathbf{1}})$$

for $0 \le k \le 2^n - 2$ *and* $\mathrm{Supp}(\beta^{\star}_{\mathbf{i}(k)}) \subseteq \{a + \delta f \ : \ a \in \beta_k[-\delta f, \infty)\}$ *for* $0 \le k \le 2^n - 2$.

(b) If $f \in \mathrm{Ann}(s)$*, then*

$$\Gamma(s) = \left(\sum_{k=0}^{2^n-2} \beta^{\star}_{\mathbf{i}(k)}(f,s) \right) / f^*$$

where $\beta^{\star}_{\mathbf{i}(0)}(f,s) \in P_n$*. In fact,* $\delta\beta^{\star}_{\mathbf{i}(0)}(f,s) \le \delta f - \mathbf{1}$ *and* $\beta^{\star}_{\mathbf{i}(0)}(f,s) = X^{\delta f - \delta\beta_0(f,s)}\beta_0(f,s)^*$.

(c) If f *is monic and* $G \in R[[X]]$ *satisfies* $\mathrm{Supp}(G) \subseteq [\mathbf{0}, \delta f)$*, then* s *defined by* G/f^* *is an lrs with* $f \in \mathrm{Ann}(s)$ *and*

$$G = \sum_{k=0}^{2^n-2} \beta^{\star}_{\mathbf{i}(k)}(f,s).$$

PROOF. These are straightforward consequences of the previous result. □

4 EVR sequences

4.1 1-D sequences

It is convenient to begin with some results on 1-D sequences.

PROPOSITION 4.1 *Let* $s \in S^1(R)^-$ *and* $\delta f \geq 1$.

(a) $f\Gamma(s) = \beta_0(f,s) + \Gamma(f \circ s)$

(b) $f \in \mathrm{Ann}(s) \Longleftrightarrow f\Gamma(s) = \beta_0(f,s)$

(c) If $f \in \mathrm{Ann}(s)$, *then* $\mathrm{Ann}(s) = (f : \beta_0(f,s)/X)$.

PROOF. (a): This is immediate from Proposition 3.2.

(b): $f \in \mathrm{Ann}(s) \Longleftrightarrow f \circ s = 0 \Longleftrightarrow \Gamma(f \circ s) = 0 \Longleftrightarrow f\Gamma(s) = \beta_0(f,s)$.

(c): If $g \in \mathrm{Ann}(s)$, then $g\beta_0(f,s) = gf\Gamma(s) = \beta_0(g,s)f$, so that $g \in (f : \beta_0(f,s)/X)$. Conversely, if $g\beta_0(f,s)/X = hf$ for some $h \in R[X]$, then $g\Gamma(s) = g\beta_0(f,s)/f = Xh$ and so by Corollary 2.8, $g \in \mathrm{Ann}(s)$. □

The next result is a considerable generalization of Theorem 1 of Prabhu & Bose (1982) and Theorem 4.11 of Fitzpatrick & Norton (1995), both of which use left-shifting.

LEMMA 4.2 *Let* R *be a factorial domain,* $s \in S^1(R)^-$, $f \in \mathrm{Ann}(s)$ *with* $\delta f \geq 1$. *Put* $d = \gcd(f, \beta_0(f,s)/X)$ *and* $g = f/d$. *Then*

(a) $g \in \mathrm{Ann}(s)$

(b) $\beta_0(g,s) = \beta_0(f,s)/d$

(c) $\gcd(g, \beta_0(g,s)/X) = 1$

(d) if $d = 1$ *and* $h \in \mathrm{Ann}(s)$ *, then* $\beta_0(f,s) | \beta_0(h,s)$ *and* $h = (\beta_0(h,s)/\beta_0(f,s)) \cdot f$.

PROOF. (a) Since $f \in \mathrm{Ann}(s), f\Gamma(s) = \beta_0(f,s)$ and so $g\Gamma(s) = X\ (\beta_0(f,s)/X)/d \in XR[X]$. By Corollary 2.8, $g \in \mathrm{Ann}(s)$.

(b) $\beta_0(f,s)/d = f\Gamma(s)/d = g\Gamma(s) = \beta_0(g,s)$ by part (a) since $g \in \mathrm{Ann}(s)$.

(c) By part (b), $\gcd(g, \beta_0(g,s)/X) = \gcd(g, (\beta_0(f,s)/X)/d) = 1$.

(d) From Proposition 4.1, $h\beta_0(f,s)/X = f\beta_0(h,s)/X$ and since $d = 1$, $\beta_0(f,s)/X$ divides $\beta_0(h,s)/X$. □

REMARK 4.3 *On the other hand, if* $g \in \mathrm{Ann}(s) \setminus \{0\}$ *has minimal degree, then* $\gcd(g, \beta_0(g,s)/X) \in R$ *— otherwise we can replace* g *by a characteristic polynomial of smaller degree by part (a) of the previous result. If* g *is also primitive, then since* $d = \gcd(g, \beta_0(g,s)/X) \in R$, $d | g_0$, *and inductively,* d *divides all the coefficients of* g. *Thus* $d = 1$.

THEOREM 4.4 *Let* R *be a factorial domain and* $\mathrm{Ann}(s) \neq (0)$. *Then*

(a) $\mathrm{Ann}(s)$ *is generated by a* primitive *polynomial* g, *say.*

(b) g is unique up to a unit of R, and $\gcd(g, \beta_0(g,s)/X) = 1$.

(c) $\delta g = \min\{\delta f : f \in \mathrm{Ann}(s) \setminus \{0\}\}$.

PROOF. We need only prove (a). For any $f \in \mathrm{Ann}(s)$ with $\delta f \geq 1$, $g = f/\gcd(f, \beta_0(f,s)/X)$ generates $\mathrm{Ann}(s)$ by Lemma 4.2, and we may take g to be primitive. □

DEFINITION 4.5 *If R is a factorial domain and* $\mathrm{Ann}(s) \neq (0)$*, we denote the* primitive *generator of* $\mathrm{Ann}(s)$ *(which is unique up to a unit of R) by* $\gamma(s)$.

We remark that $\gamma(s)$ may be computed using the minimal realization algorithm of Norton (1994); see *loc. cit.* Corollary 3.28. For an alternative approach to $\gamma(s)$ using polynomial remainder sequences, see Fitzpatrick & Norton (1995), Section 4.5.

4.2 Associated sequences

DEFINITION 4.6 *For $n \geq 2$ and $\mathbf{i} \ll \mathbf{n}$, let $s^{(\mathbf{i},*)} \in S^{|\mathbf{i}|}(R[[X_{\mathbf{i}'}]])$ be given by*

$$s_a^{(\mathbf{i},*)} = \sum_{a' \in -\mathbb{N}^{\mathbf{i}'}} s_{(a,a')} X_{\mathbf{i}'}{}^{a'}$$

for $a \in -\mathbb{N}^{\mathbf{i}}$.

Thus for $\mathbf{i} \ll \mathbf{n}$, the superscript $^{(\mathbf{i},*)}$ is used to suggest *summation over* $\mathbf{i}'$ (whereas for $a \in -\mathbb{N}^{\mathbf{i}}$, the superscript $^{(a)}$ is used to denote a *section*). Special cases of these associated sequences were used in Fitzpatrick & Norton (1990).

For $\mathbf{i} \ll \mathbf{n}$, we let $R[X_{\mathbf{i}}]$ act on n-D sequences via:

$$\left(\sum_{a \in \mathrm{Supp}(f)} f_a X_{\mathbf{i}}^a \circ s \right)_b = \sum_{a \in \mathrm{Supp}(f)} f_a \; s_{b-(a,\mathbf{0}')}$$

where $b \leq \mathbf{0}$ and $\mathbf{0}' \in \mathbb{N}^{\mathbf{i}'}$.

LEMMA 4.7 *Let $n \geq 2$, $\mathbf{i} \ll \mathbf{n}$, $f \in R[X_{\mathbf{i}}], f' \in R[X_{\mathbf{i}'}]$ and $a \in -\mathbb{N}^{\mathbf{i}}, a' \in -\mathbb{N}^{\mathbf{i}'}$. Then*

(a) $(f' \circ s^{(a)})_{a'} = (f' \circ s)_{(a,a')}$

(b) $s_a^{(\mathbf{i},*)} = \Gamma(s^{(a)})(X_{\mathbf{i}'}^{-\mathbf{1}})$

(c) $\Gamma(f \circ s^{(\mathbf{i},*)})(X_{\mathbf{i}}^{-\mathbf{1}}) = \Gamma(f \circ s)(X^{-\mathbf{1}})$.

PROOF. (a)

$$(f' \circ s^{(a)})_{a'}$$

$$= \sum_{d' \in \mathrm{Supp}(f')} f'_{d'} s^{(a)}_{a'-d'} = \sum_{d' \in \mathrm{Supp}(f')} f'_{d'} s_{(a'-d',a)}$$
$$= \sum_{d' \in \mathrm{Supp}(f')} f'_{d'} s_{(a',a)-(d',\mathbf{0})} = (f' \circ s)_{(a',a)}.$$

(b), (c) These are also easy consequences of the definitions. □

The characteristic ideals of associated sequences are related as follows:

PROPOSITION 4.8 *Let $n \geq 2$ and $\mathbf{i} \ll \mathbf{n}$. Then*

$$\bigcap_{a' \in -\mathbb{N}^{\mathbf{i}'}} \mathrm{Ann}(s^{(a')}) = \mathrm{Ann}(s) \cap R[X_{\mathbf{i}}] = \mathrm{Ann}(s^{(\mathbf{i},*)}).$$

PROOF. Let $f \in R[X_{\mathbf{i}}]$. By Lemma 4.7(a),

$$\forall (a' \in -\mathbb{N}^{\mathbf{i}'})(f \circ s^{(a')} = 0) \Longleftrightarrow \forall (b \in -\mathbb{N}^n)((f \circ s)_b = 0) \Longleftrightarrow f \in \mathrm{Ann}(s).$$

To prove the second equality, note that $f \circ s = 0 \Longleftrightarrow f \circ s^{(\mathbf{i},*)} = 0$ by Lemma 4.7(c). □

4.3 Some properties of EVR sequences

It follows from the previous subsection that for $n \geq 2$ and $i \in \mathbf{n}$, there are n associated sequences $s^{(i,*)} = s^{(\{i\},*)} \in S^1(R[[\widehat{\mathbf{X}}_i^{-\mathbf{1}}]])^-$ given by

$$s^{(i,*)}_j = \sum_{j' \in -\mathbb{N}^{\mathbf{n}\setminus\{i\}}} s_{(j,j')} \widehat{\mathbf{X}}_i^{\,j'}$$

for $j \leq 0$, $\mathrm{Ann}(s^{(i,*)}) = \mathrm{Ann}(s) \cap R[X_i]$ and $\Gamma(f_i \circ s^{(i,*)})(X_i^{-1}) = \Gamma(f_i \circ s)(X^{-\mathbf{1}})$.

The next result is a considerable generalization of Prabhu & Bose (1982), Theorem 1 and Fitzpatrick & Norton (1990), Corollary 4.2:

THEOREM 4.9 *Let $f_i \in R[X_i]$ with $\delta f_i \geq 1$ for all $i \in \mathbf{n}$ and let $f = \prod_{i=1}^n f_i$. The following are equivalent:*

(a) for all $i \in \mathbf{n}$, $f_i \in \mathrm{Ann}(s)$

(b) $f\Gamma(s) \in XP_n$

(c) $f\Gamma(s) = \beta_0(f, s)$.

PROOF. (a) $\Longrightarrow$ (b): For all $i \in \mathbf{n}$ and $a_i \leq 0$, the coefficient of $X_i^{a_i}$ in $f\Gamma(s)$ is

$$(f\Gamma(s))_{(a_i,\mathbf{0}')} = (f \circ s)_{(a_i,\mathbf{0}')}$$

which is zero since f is a multiple of $f_i \in \mathrm{Ann}(s)$. Hence $\mathrm{Supp}(f\Gamma(s)) \subseteq [\mathbf{1}, \delta f]$.

(b) $\Longrightarrow$ (a): Fix $i \in \mathbf{n}$. Put $t = s^{(i,*)}$ and let $f\Gamma(s) = Xg$, where $g \in P_n$. By Lemma 4.7, $\Gamma(t)(X_i^{-1}) = \Gamma(s)(X^{-\mathbf{1}})$. Thus

$$\delta_i(f_i\Gamma(t)) = \delta_i(f\Gamma(t)) = \delta_i(f\Gamma(s)) = \delta_i Xg \geq 1,$$

whereas for $j \neq i$,

$$\delta_j(f_i\Gamma(t)) \leq \delta_j f_i + \delta_j\Gamma(t) \leq \delta_j\Gamma(t) \leq 0$$

i.e. $f_i\Gamma(t) \in X_i(R[[\widehat{\mathbf{X}}_i^{-\mathbf{1}}]])[X_i]$. Thus by Corollary 2.8, $f_i \in \mathrm{Ann}(t)$ and by Lemma 4.7 again, $\Gamma(f_i \circ s) = \Gamma(f_i \circ t) = 0$ i.e. $f_i \in \mathrm{Ann}(s)$.

(b) $\Longrightarrow$ (c): Let $f\Gamma(s) = Xg \in P_n$ where $\delta g \leq \delta f - \mathbf{1}$. Since (b) $\Longleftrightarrow$ (a), $\Gamma(f \circ s) = 0$ and so

$$Xg - \beta_0(f,s) = f\Gamma(s) - \beta_0(f,s) = \sum_{k=1}^{2^n-2} \beta_k(f,s).$$

The support of the left-hand side is contained in $[\mathbf{1}, \delta f]$, whereas the support of the right-hand side is contained in $(-\infty, \delta f] \setminus [\mathbf{1}, \delta f]$ by construction. Therefore both sides vanish and $f\Gamma(s) = \beta_0(f,s)$. □

We now discuss $\mathrm{Ann}(s) \cap R[X_i]$, which is an ideal of $R[X_i]$. So when R is a field, $\mathrm{Ann}(s) \cap R[X_i]$ is principal and has a *monic* generator. We will see that this is also true more generally.

For $n = 1$, the following notion was introduced in Fitzpatrick & Norton (1995):

DEFINITION 4.10 *A factorial domain R will be called* potential *if for all $n \geq 1$, S_n is factorial.*

In fact, for the known examples R for which $R[[X]]$ is factorial, S_n is also factorial. Principal ideal domains, $R[X]$ (where R is a field or a discrete valuation ring) are potential domains, but not every factorial domain is potential: see Bourbaki (1972), Exercise 8(c), p.566. We refer the reader to Bourbaki (1972), Proposition 8, p.511 and Exercise 9(c), p.566 and to Fossum (1973) for more details.

LEMMA 4.11 *Let R be factorial and $s \in S^1(R)^-$. If $R[[X]]$ is factorial, we can assume that $\gamma(s)$ is monic.*

PROOF. $\mathrm{Ann}(s) \cong \mathrm{Ann}(s^-)$, and so the result follows from Fitzpatrick & Norton (1995), Corollary 4.8. □

THEOREM 4.12 *If R potential and s is EVR, then for all $i \in \mathbf{n}$, $\mathrm{Ann}(s) \cap R[X_i]$ is principal and has a unique* monic *generator.*

PROOF. We can assume that $n \geq 2$. Fix i and let $U = R[[\widehat{\mathbf{X}}_i^{-\mathbf{1}}]]$ and $t = s^{(i,*)} \in S^1(U)^-$. By Proposition 4.8, $\mathrm{Ann}(s) \cap R[X_i] = \mathrm{Ann}(t)$. Also, U and $U[[X_i^{-1}]] = S_n$ are factorial since R is potential. Thus the result follows from Lemma 4.11. □

The next result simplifies and extends Fitzpatrick & Norton (1990), Theorem 4.3:

THEOREM 4.13 *Let R be a potential domain and for all $i \in \mathbf{n}$, let $f_i \in \mathrm{Ann}(s) \cap R[X_i]$ with $\delta f_i \geq 1$. Put $f = \prod_{i=1}^{n} f_i$ and $d_i = \gcd(f_i, \beta_0(f,s)/X_i)$. Then for all $i \in \mathbf{n}$, there is a unit u_i of R such that $u_i f_i/d_i$ is the monic generator of* $\mathrm{Ann}(s) \cap R[X_i]$.

PROOF. For $i \in \mathbf{n}$, let γ_i be the monic generator of $\mathrm{Ann}(s) \cap R[X_i]$ and $\gamma = \prod_{i=1}^{n} \gamma_i$. By Theorem 4.9,

$$\gamma \beta_0(f,s) = \gamma f \Gamma(s) = f \beta_0(\gamma, s).$$

Now $\gcd(\gamma, \beta_0(\gamma,s)/X) \in R$, otherwise we could replace some γ_j by a polynomial of smaller degree. Since P_n is factorial, γ is primitive by Gauss' Lemma and so $\gcd(\gamma, \beta_0(\gamma,s)/X) = 1$. Hence there is a unit u of R with $\gamma = uf/\gcd(f, \beta_0(f,s)/X)$. Also,

$$\gcd(f, \beta_0(f,s)/X) = \gcd(\prod f_i, \beta_0(f,s)/X) = \prod \gcd(f_i, \beta_0(f,s)/X_i) = \prod d_i$$

since $f_i \in R[X_i]$. Thus $\prod \gamma_i = u \prod (f_i/d_i)$ and since P_n is factorial, $\gamma_i = u_i f_i/d_i$ for some unit u_i of R. □

We now combine Theorems 4.9 and 4.13 to characterize generating functions of EVR lrs:

COROLLARY 4.14 *Let $f_i \in R[X_i]$ with $\delta f_i \geq 1$ for $i \in \mathbf{n}$, and put $f = \prod_{i=1}^{n} f_i$.*

(a) If R is potential and $f_i \in \mathrm{Ann}(s)$ for all $i \in \mathbf{n}$, then $\Gamma(s) = \beta_0(f,s)/f$ and we can assume that for all $i \in \mathbf{n}$, f_i is monic, $\gcd(f_i, \beta_0(f,s)/X_i) = 1$ *and* $\mathrm{Ann}(s) \cap R[X_i] = (f_i)$.

(b) If for all $i \in \mathbf{n}$, f_i is monic, $g \in R[X], \delta g \leq \delta f - \mathbf{1}$ and $\gcd(f_i, g) = 1$, *then s defined by $\Gamma(s) = Xg/f$ is an (EVR) lrs with $Xg = \beta_0(f,s)$ and* $\mathrm{Ann}(s) \cap R[X_i] = (f_i)$.

PROOF. For each $i \in \mathbf{n}$, f_i can be chosen as the monic generator of $\mathrm{Ann}(s) \cap R[X_i] = \mathrm{Ann}(s^{(i,*)})$ by Theorem 4.12. Since

$$f_i \Gamma(s^{(i,*)}) = f_i \Gamma(s) = \beta_0(f,s) / \prod_{j \neq i} f_j$$

we must have $d_i = \gcd(f_i, \beta_0(f,s)/X_i) \in R$ — for otherwise by Lemma 4.2, we can replace f_i by a characteristic polynomial of smaller degree. Since d_i divides each coefficient of f_i, which is monic, $d_i = 1$.

For the converse, we have $Xg = \beta_0(f,s)$ from Theorem 4.9. Thus $\gcd(f_i, \beta_0(f,s)/X_i) = 1$ and by Theorem 4.13, $\mathrm{Ann}(s) \cap R[X_i] = (f_i)$. □

For completeness, we give an alternative way of finding the generator of $\mathrm{Ann}(s) \cap R[X_i]$ (Corollary 4.16 below), generalizing Fitzpatrick & Norton (1990), Theorem 4.10.

LEMMA 4.15 *Let $n \geq 2$, R be a domain, let $f_i \in \mathrm{Ann}(s) \cap R[X_i]$ with $\delta f_i \geq 1$ for all $i \in \mathbf{n}$, and put $\Delta_i' = \delta(\prod_{j=1, j\neq i}^{n} f_j) - \mathbf{1}' \in \mathbb{N}^{\mathbf{n}\setminus\{i\}}$. Then*

$$\bigcap_{a' \in -mathbbN^{\mathbf{n}\setminus\{i\}}} \mathrm{Ann}(s^{(a')}) = \bigcap_{-\Delta_i' \leq a' \leq \mathbf{0}'} \mathrm{Ann}(s^{(a')}).$$

PROOF. By definition, $s^{(a')} \in S^1(R)^-$ if $a' \in -\mathbb{N}^{\mathbf{n}\setminus\{i\}}$. We show that if $g \in R[X_i]$ satisfies $g \circ s^{(a')} = 0$ for $-\Delta_i' \leq a' \leq \mathbf{0}'$, then $g \circ s^{(a')} = 0$ for all a'. Let $i = 1$ and let λ_2 be the leading coefficient of f_2. Suppose first that $a' = (-\delta_2 f_2, -\delta_3 f_3 + 1, \ldots, -\delta_n f_n + 1)$. Since $f_2 \in \mathrm{Ann}(s)$, we can write

$$\lambda_2 s_{(a,a')} = -\sum_{b'=0}^{\delta_2 f_2 - 1} (f_2)_{b'} s_{(a,-b',c')}$$

for all $a \leq 0$, where $c' = (-\delta_3 f_3 + 1, \ldots, -\delta_n f_n + 1)$. Then for $a \leq 0$,

$$(\lambda_2 g \circ s^{(a')})_a = \sum_{c=0}^{\delta g} g_c \lambda_2 s_{(a-c,a')} = -\sum_{b'=0}^{\delta_2 f_2 - 1} (f_2)_{b'} \sum_{c=0}^{\delta g} g_c s_{(a-c,-b',c')}$$

and $\sum_{c=0}^{\delta g} g_c s_{(a-c,-b',c')} = (g \circ s^{(-b',c')})_a = 0$ since $\Delta_1' \leq (-b', c') \leq \mathbf{0}'$. Thus for $a' = (-\delta_2 f_2, -\delta_3 f_3 + 1, \ldots, -\delta_n f_n + 1)$, $\lambda_2 g \circ s^{(a')} = 0$. The argument is similar for $a' = (a_2, -\delta_3 f_3 + 1, \ldots, -\delta_n f_n + 1)$, $a_2 < -\delta_2 f_2$; in this case, $\lambda_2^{-a_2 - \delta_2 f_2} g \circ s^{(a')} = 0$. Since $\lambda_2 \in R$ and R is a domain, $g \circ s^{(a')} = 0$ for all $a_2 \leq 0$.

Suppose inductively that the result is true for $a' = (a_2, a_3, \ldots, a_{k-1}, -\delta_k f_k + 1, \ldots, -\delta_n f_n + 1)$ and $a' = (a_2, a_3, \ldots, a_k, -\delta_{k+1} f_{k+1} + 1, \ldots, -\delta_n f_n + 1), a_k \leq -\delta f_k$. An analogous argument using $f_k \in \mathrm{Ann}(s) \cap R[X_k]$ shows that $g \circ s^{(a')} = 0$. By induction $g \circ s^{(a')} = 0$ for all $a' \in -\mathbb{N}^{\mathbf{n}\setminus\{1\}}$. It is clear that the same argument applies to any $i \in \mathbf{n}$ and this completes the proof. □

THEOREM 4.16 *Let $n \geq 2$ and R be potential. Suppose that for all $i \in \mathbf{n}$, $f_i \in \mathrm{Ann}(s) \cap R[X_i]$, $\delta f_i \geq 1$ and let $\Delta_i' = \delta(\prod_{j=1, j\neq i}^{n} f_j) - \mathbf{1}' \in \mathbb{N}^{\mathbf{n}\setminus\{i\}}$. Then for all $i \in \mathbf{n}$,*

$$\mathrm{Ann}(s) \cap R[X_i] = \left(\mathrm{lcm}\{\gamma(s^{(a')}) : -\Delta_i' \leq a' \leq \mathbf{0}'\}\right)$$

PROOF. Fix $i \in \mathbf{n}$. For $a' \in -\mathbb{N}^{\mathbf{n}\setminus\{i\}}, \gamma(s^{(a')}) \in R[X_i]$ is well-defined (and indeed monic) by Lemma 4.11. By Proposition 4.8 and Lemma 4.15, $\mathrm{Ann}(s) \cap R[X_i] = \bigcap_{-\Delta_i' \leq a' \leq \mathbf{0}'} \mathrm{Ann}(s^{(a')})$. Since $R[X_i]$ is factorial, the intersection is non-empty and is generated by $\mathrm{lcm}\{\gamma(s^{(a')}) : -\Delta_i' \leq a' \leq \mathbf{0}'\}$. □

The least common multiple of Theorem 4.16 may be computed using Algorithm 3.30 of Norton (1994). If R is a field, it may also be computed using the "Fundamental Iterative Algorithm" of Feng & Tzeng (1989).

We conclude this subsection by generalizing a result of Cerlienco & Piras (1991) to sequences over domains.

DEFINITION 4.17 *We say that an ideal I of P_n is* cofinite *if P_n/I is a finitely generated R-module and that an n-D lrs over R is* cofinite *if its characteristic ideal contains a cofinite ideal.*

It is well known that if R is a field, then a cofinite ideal in $R[X_1,\ldots,X_n]$ has a finite zero set. Conversely, if R is an algebraically closed field, then an ideal in $R[X_1,\ldots,X_n]$ with a finite zero set is cofinite.

THEOREM 4.18 *If s is a cofinite lrs over R, then s is EVR. Conversely, if R is potential and s is EVR, then s is cofinite.*

PROOF. Suppose that $\mathrm{Ann}(s)\cap R[X_i]=\{0\}$ for some i. Then

$$R[X_i]=R[X_i]/(\mathrm{Ann}(s)\cap R[X_i])\cong (R[X_i]+\mathrm{Ann}(s))\,/\mathrm{Ann}(s)\subseteq P_n/\mathrm{Ann}(s)$$

and so $P_n/\mathrm{Ann}(s)$ is not finitely generated. Thus $\mathrm{Ann}(s)$ contains no cofinite ideals I (otherwise there would be a map of P_n/I *onto* $P_n/\mathrm{Ann}(s)$, implying that $P_n/\mathrm{Ann}(s)$ is finitely generated) i.e. s is not cofinite.

If R is potential and s is EVR, then by Theorem 4.12 we may assume that the $f_i\in\mathrm{Ann}(s)$ are monic, and set $F=(f_1,f_2,\ldots,f_n)$. Then the monomials $X^a \bmod F$ for $a\le(\delta f_1-1,\delta f_2-1,\ldots,\delta f_n-1)$ generate P_n/F. Thus $F\subseteq\mathrm{Ann}(s)$ is cofinite i.e. s is cofinite. □

In particular, if R is a field, the two notions coincide (cf. Cerlienco & Piras (1991), Section 4).

4.4 $\mathrm{Ann}(s)$ as Ideal Quotient

We generalize Proposition 4.1(c) and Fitzpatrick & Norton (1990), Theorem 5.1 to n-D sequences over R. (The first part of the proof generalizes the proof for the case $n=1$ and the second part generalizes the minimal counterexample idea of Fitzpatrick & Norton (1990), *loc. cit.*)

THEOREM 4.19 *If $f_i\in\mathrm{Ann}(s)\cap R[X_i]$, with $\delta f_i\ge 1$ for all $i\in\mathbf{n}$ and $f=\prod_{i=1}^n f_i$, then*

$$\mathrm{Ann}(s)=\left(\sum_{i=1}^n (f_i):\beta_0(f,s)/X\right).$$

PROOF. By Proposition 4.1(c), we can assume that $n\ge 2$.

$\supseteq$: Suppose that $g\in P_n\setminus\{0\}$ satisfies $g\beta_0(f,s)=X\sum_{i=1}^n f_iu_i$ for some $u_i\in P_n$. By Theorem 4.9,

$$g\Gamma(s)=g\beta_0(f,s)/f=\left(X\sum_{i=1}^n f_iu_i\right)/f=X\sum_{i=1}^n\left(u_i\,/\prod_{j=1,j\ne i}^n f_j\right)$$

and so for $a\le\mathbf{0}$,

$$(g\circ s)_a=\sum_{i=1}^n\left(u_i\,/\prod_{j=1,j\ne i}^n f_j\right)_{a-\mathbf{1}}=0$$

since each $u_i \in P_n$ i.e. $g \in \mathrm{Ann}(s)$.

$\subseteq$: Let $g \in \mathrm{Ann}(s)$ and $h = g\Gamma(s) \in L_n$. By Proposition 2.7(c), $\mathrm{Supp}(h) \subseteq (\mathbf{0}, \delta g]$. Let $\wp = \{\wp_i : 1 \leq i \leq n\}$ be the following partition of $(\mathbf{0}, \delta g]$:

$$\wp_1 = \{a \in (\mathbf{0}, \delta g] : a_1 > 0\} \text{ and } \wp_i = \{a \in (\mathbf{0}, \delta g] \setminus \bigcup_{j=1}^{i-1} \wp_j : a_i > 0\}$$

if $2 \leq i \leq n$. It is clear that $\wp$ is a partition of $(\mathbf{0}, \delta g]$ and that for $1 \leq i \leq n, \wp_i = \{a \in (\mathbf{0}, \delta g] : a_j \leq 0$ for $1 \leq j \leq i-1$ and $a_i > 0\}$. Let $h_i = h|\wp_i$ and $p_i = h_i f / f_i$ for $i \in \mathbf{n}$. Then $h_i \in X_i R((\widehat{\mathbf{X}}_i^{-\mathbf{1}}))[X_i]$ for all $i \in \mathbf{n}$ and

$$g\beta_0(f, s) = gf\Gamma(s) = hf = \sum_{i=1}^{n} h_i f = \sum_{i=1}^{n} p_i f_i.$$

So it suffices to show that $p_i \in XP_n$ for all $i \in \mathbf{n}$.

Suppose that for some $i \in \mathbf{n}, p_i \notin XP_n$, and let k be the smallest such integer. Now p_k / X_k is a polynomial in X_k, and so for some $r \geq 1$, the coefficient of X_k^r in p_k is not in $R[\widehat{\mathbf{X}}_k]$. Letting $d = \delta f_k$, the coefficient of X_k^{d+r} in $h_k f = p_k f_k$ cannot therefore be in $R[\widehat{\mathbf{X}}_k]$. But

$$\sum_{i=1}^{n} h_i f = g\beta_0(f, s) \in XP_n$$

and so the coefficient of X_k^{d+r} in $h_k f$ must cancel with other coefficients of X_k^{d+r} in the $h_i f$, for one or more $i \neq k$. If $1 \leq i < k$, the cancellation cannot take place by choice of k. If $k < i \leq n$, the exponent of X_k in $f h_i$ is at most d by construction of h_i. Thus cancellation of the coefficient of X_k^{d+r} in $h_k f$ cannot take place and we conclude that $p_i \in XP_n$ for all $i \in \mathbf{n}$, as required. $\square$

EXAMPLE 4.20 *Let s be as in Example 2.4(a). We know that $f_1 = X_1$ and $f_2 = X_2 - 1$ belong to* $\mathrm{Ann}(s)$ *and* $\Gamma(s) = 1/(X_2 - 1)$, $\beta_0(f_1 f_2, s) = X_1 X_2$. *From Theorem 4.19,* $\mathrm{Ann}(s) = ((f_1, f_2) : 1) = (f_1, f_2) = (X_1, X_2 - 1)$. *We remark that Fitzpatrick & Norton (1990), Theorem 5.2 gives* $\mathrm{Ann}(s) = (X_2 - 1)$ *if R is a field.*

EXAMPLE 4.21 *Let s satisfy $s_{(i,0)} = 1$ for $i \leq 0$, $s_{(0,j)} = 1$ for $j \leq 0$ and $s_{(i,j)} = 0$ otherwise. Then* $\Gamma(s) = (X_1 X_2 - 1)/(X_1 - 1)(X_2 - 1)$, *so that by Theorem 4.19,* $\mathrm{Ann}(s) = (X_1(X_1 - 1), X_2(X_2 - 1) : X_1 X_2 - 1)$.

Combining Theorems 4.13, 4.16 and 4.19 now yields an algorithm for computing a basis for $\mathrm{Ann}(s)$:

ALGORITHM 4.22 *(cf. Fitzpatrick & Norton (1990), Algorithm 3.8).*

Input: An EVR $s \in S^n(R)^-$, R a potential domain.

Output: A basis for $\mathrm{Ann}(s)$.

1. For each $i \in \mathbf{n}$, find the monic generator γ_i of $\mathrm{Ann}(s) \cap R[X_i]$ using Theorem 4.13 or Theorem 4.16.

2. Compute $\gamma = \prod_{i=1}^{n} \gamma_i$ and $\beta_0(\gamma, s)/X$.

3. Find a basis for the ideal quotient $(\sum_{i=1}^{n}(\gamma_i) : \beta_0(\gamma, s)/X)$.

REMARK 4.23 *Over a field $\mathbb{F}$, Step 3 may be done in several ways:*

(i) using the basis $\{X^m : m \leq \delta\gamma - \mathbf{1}\}$ for $\mathbb{F}[X]/(\gamma_1, \gamma_2, \ldots, \gamma_n)$, find an $\mathbb{F}$-basis for solutions f of the homogeneous equation

$$f\beta_0(\gamma, s)/X + \sum_{i=1}^{n} \gamma_i u_i = 0$$

where $u_i \in \mathbb{F}[X]$. Augmenting these solutions by $\{\gamma_1, \gamma_2, \ldots, \gamma_n\}$ yields an $\mathbb{F}$-basis for $\mathrm{Ann}(s)$.

This approach is an application of Buchberger (1985), Method 6.7, which applies since $\{\gamma_1, \gamma_2, \ldots, \gamma_n\}$ is trivially a (reduced) groebner basis for any term order. In this case, Algorithm 4.22 has complexity $O(\prod_{i=1}^{n} \delta\gamma_i^3)$. The $\mathbb{F}$-basis found can of course be converted to a reduced groebner basis with respect to any given term order, if desired.

(ii) Cox et al. (1991), Sections 3.3, 3.4 reduce the computation of a basis for an ideal quotient to computing a groebner basis (with respect to the lexicographic term order) of an intersection of ideals. In this way, we obtain a groebner basis for $\mathrm{Ann}(s)$. This approach was applied to computing an ideal basis of a 2-D cyclic code and its dual in Norton (1995a).

Acknowledgements

The author would like to thank Aidan Schofield for a useful conversation, the U.K. Science and Engineering Research Council for financial support and the referees for helpful comments and suggestions. Thanks also to Guy Chassé for a copy of Ferrand (1988).

Note added in proof: This paper combines two papers "On n-dimensional sequences I,II" that were submitted to this journal. The first paper described a border partition for left-shifting, gave an inductive proof of Corollary 3.10 and some applications of it. Lemma 3.4 (and right-shifting) appeared in the second paper. The author also suggested a new proof of Corollary 3.10 (via Lemma 3.4 and a direct, rather than inductive proof of Theorem 3.8) in the second paper. This revised version adopts the new approach.

References

Bourbaki, N. (1972). *Commutative Algebra*. Hermann.

Boztaş, S., Hammons, A.R., Kumar, P.V. (1992). 4-Phase sequences with near-optimum correlation properties. *IEEE Trans. Information Theory* **38**, 1101–1113.

Buchberger, B. (1985). Groebner bases: an algorithmic method in polynomial ideal theory. *Multidimensional Systems Theory, N.K. Bose (ed.)*, 184–232. Reidel, Dordrecht.

Cerlienco, L., Mignotte, M., Piras, F. (1987). Suites Récurrentes Linéaires. *L'Enseignement Mathématiques* **33**, 67–108.

Cerlienco, L., Piras, F. (1991). On the continuous dual of a polynomial bialgebra. *Communications in Algebra* **19**, 2707–2727.

Chabanne, H., Norton, G.H. (1994). The n-dimensional key equation and a decoding application. *IEEE Trans. Information Theory* **40**, 200 – 203.

Cox, D., Little, J. and O'Shea, D. (1991). *Ideals, Varieties and Algorithms*. Springer.

Fan, P.Z., Darnell,M. (1994). Maximal length sequences over Gaussian integers. *Electronic Letters* **30**, 1286–1287.

Feng, G.L., Tzeng, K.K. (1989). A generalization of the Berlekamp–Massey algorithm for multisequence shift register synthesis with applications to the decoding of cyclic codes. *IEEE Trans. Information Theory* **37**, 1274–1287.

Ferrand, D. (1988). *Suites Récurrentes*. IRMAR, Université de Rennes.

Fitzpatrick, P., Norton, G.H. (1990). Finding a basis for the characteristic ideal of an n-dimensional linear recurring sequence. *IEEE Transactions on Information Theory* **36**, 1480–1487.

Fitzpatrick, P., Norton, G.H. (1991). Linear recurring sequences and the path weight enumerator of a convolutional code. *Electronic Letters* **27**, 98–99.

Fitzpatrick, P., Norton, G.H. (1995). The Berlekamp-Massey algorithm and linear recurring sequences over a factorial domain. *J. Applicable Algebra in Engineering, Communications and Computing.* **6**, 309–323.

Fossum, R. (1973). *The divisor class group of a Krull domain.* Springer Ergebnisse **74**.

Greene, D.H. & Knuth, D.E. (1982). *Mathematics for the Analysis of Algorithms, 2nd Edition.* Birkhäuser, Boston.

Homer, S. and Goldman, J. (1985). Doubly periodic sequences and two-dimensional recurrences. *SIAM J. Alg. Disc. Math.* **6**, 360–370.

Ikai, T., Kosako, H., Kojima, Y. (1975). Two dimensional cyclic codes. *Electronics and Communications in Japan* **57–A**, 27–35.

Ikai, T., Kosako, H. and Kojima, Y. (1976). Basic theory of two-dimensional cyclic codes. *Electronics and Communications in Japan* **59–A**, 31–47.

Imai, H., Arakaki, M. (1974). A theory of two-dimensional cyclic codes. *National Convention Record of Institute of Electronics and Communication Engineers, Japan*, 1564. In Japanese.

Imai, H. (1977) A theory of two-dimensional codes. *Inform. Control* **34**, 1–21.

Lidl, R., Niederreiter, H. (1983). *Finite Fields, Encyclopedia of Mathematics and its Applications* **20**. Addison-Wesley.

Lin, D. & Liu, M. (1988). Linear Recurring m-Arrays. *Proceedings of Eurocrypt 88*. LNCS **330**, 351–357. Springer.

Massey, J.L. (1969). Shift register synthesis and BCH decoding. *IEEE Trans. Information Theory* **15**, 122–127.

McEliece, R. (1987). *Finite Fields for Computer Scientists and Engineers*. Kluwer Academic Press.

Nerode, A. (1958). Linear automaton transformations. *Proc. Amer. Math. Soc.* **9**, 541–544.

Niederreiter, H. (1988). Sequences with almost perfect linear complexity profile. In *Advances in Cryptology- Eurocrypt '87*. LNCS **304**, 37–51. Springer.

Norton, G.H. (1994). On the minimal realizations of a finite sequence. *J. Symbolic Computation*. To appear.

Norton, G.H. (1995a). The solution module (of n-dimensional sequences) of an ideal containing $(X_1^{M_1}-1,\ldots,X_n^{M_n}-1)$. *Proc. IV^{th} I.M.A. Conference on Coding and Cryptography (P.G. Farrell, ed.)*, Formara Ltd., 315–326.

Norton, G.H. (1995b). Encoding an n-dimensional cyclic code over a finite field. Presented at Third International Conference on Finite Fields, Glasgow, July 1995.

Norton, G.H. (1995c). Some decoding applications of minimal realization. *Proc. V^{th} I.M.A. Conference on Coding and Cryptography*. LNCS. Springer. To appear.

Norton, G.H. (1995d). On the minimal realizations of a finite n-D sequence. In preparation.

Peterson W. W., & Weldon, E.J. (1972). *Error Correcting Codes, 2nd Edition*. MIT Press. Cambridge, Massachusetts.

Prabhu, K.A. & Bose, N.K. (1982). Impulse Response Arrays of Discrete-Space Systems over a Finite Field. *IEEE Trans. Acoustics, Speech and Signal Processing* **30**, 10–18.

Rueppel, R.A. (1986). *Analysis and Design of Stream Ciphers*. Springer.

Sakata, S. (1978). General theory of doubly periodic arrays over an arbitrary finite field and its applications. *IEEE Trans. Information Theory* **24**, 719–730.

Sakata, S. (1981). On determining the independent point set for doubly periodic arrays and encoding two-dimensional cyclic codes and their duals. *IEEE Trans. Information Theory* **27**, 556–565.

Sakata, S. (1988). Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array. *J. Symbolic Computation* **5**, 321–337.

Sakata, S. (1990). Extension of the Berlekamp-Massey algorithm to n dimensions. *Information and Computation* **84**, 207–239.

Welch, L.R., Scholtz, R.A. (1979). Continued fractions and Berlekamp's algorithm. *IEEE Trans. Information Theory* **25**, 19–27.

Zierler, N. (1959). Linear recurring sequences. *J. S.I.A.M.* **7**, 31–48.