Proof: The case $L=3$ was proved in Lemma 3. For the case $L \geq 4$, we have $L^2 > 4L-3$. Then by Lemma 4 we have

$$C_{\max} \geq \sqrt{\frac{1}{4L-3}} > \frac{1}{L}.$$

Since s_1 and s_2 are generalized Barker sequences, by definition we have

$$C_2 = \max_{x \in \{s_1, s_2\}} \max_{1 \leq |\tau| \leq L-1} \frac{1}{L}|C_{x,x}(\tau)| \leq \frac{1}{L}.$$

Hence we have

$$C_1 = \max_{0 \leq |\tau| \leq L-1} \frac{1}{L}|C_{s_1,s_2}(\tau)| > \frac{1}{L}.$$

This implies

$$\max_{0 \leq |\tau| \leq L-1} |C_{s_1,s_2}(\tau)| > 1. \qquad \square$$

Corollary: If s_1 and s_2 are any two normalized generalized Barker sequences of length L, (i.e., $C_{s_1,s_1}(0) = C_{s_2,s_2}(0) = 1$), then

$$\max_{0 \leq |\tau| \leq L-1} |C_{s_1,s_2}(\tau)| \geq \sqrt{\frac{1}{4L-3}}, \qquad \text{for all } L \geq 4.$$

Note: For $L=3$, a stronger result, with strict inequality, follows from Lemma 3. For $L=2$, the best result possible must allow $C_{s_1,s_2}(0)=0$, $|C_{s_1,s_2}(1)| = 1/2$, since this occurs when $s_1 = \{1/\sqrt{2}, 1/\sqrt{2}\}$ and $s_2 = \{1/\sqrt{2}, -1/\sqrt{2}\}$.

References

[1] S. W. Golomb and R. A. Scholtz, "Generalized Barker sequences," *IEEE Trans. Inform. Theory*, vol. IT-11, no. 4, pp. 533–537, Oct. 1965.

[2] S. W. Golomb, "Correlation properties of periodic and aperiodic sequences, and applications to multi-user systems," in *New Concepts in Multi-User Communication*, J. K. Skwirzynski, Ed. Sijthoff and Noordhoff, NASI: series E, no. 43, pp. 161–197, 1981.

[3] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, 1980, pp. 593–619.

[4] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inform. Theory*, vol. IT-20, no. 3, pp. 397–399, May 1974.

Finding a Basis for the Characteristic Ideal of an n-Dimensional Linear Recurring Sequence

PATRICK FITZPATRICK AND GRAHAM H. NORTON

***Abstract*—We consider an n-dimensional linear recurring sequence (σ) of elements from a field $\mathbb{F}$, for $n \geq 1$. We present an algorithm χ-BASE, which determines a basis for the ideal $\mathscr{I}(\sigma)$ of characteristic polynomials of (σ) under certain reasonable conditions. Our analysis applies to doubly periodic arrays in particular.**

***Index Terms*—*n-D* linear recurring sequences, characteristic ideal basis algorithm.**

Manuscript received July 11, 1989; revised May 9, 1990. This work was supported in part by EOLAS (Dublin), the CNRS (Paris), and the Royal Society. This work was presented at the IEEE International Symposium on Information Theory, San Diego, CA, January 14–19, 1990.

P. Fitzpatrick is with the Department of Mathematics, University College, Cork, Ireland.

G. Norton was on leave at the Laboratoire d'Analyse Numérique, Université Paul Sabatier, Toulouse, France. He is with the Centre for Communications Research, Faculty of Engineering, University of Bristol, University Walk, Bristol BS8 1TR, England.

IEEE Log Number 9038004.

I. Introduction

Let $\mathbb{N}$ denote the set $\{0, 1, \cdots\}$, let $n \geq 1$ and let Z_n be the set $\{1, 2, \cdots, n\}$. We consider the cartesian product $\mathbb{N}^n$ as embedded in $\mathbb{Z}^n$ for addition, and partially ordered by the relation $\leq$ on each component. Thus, $\boldsymbol{i} := (i_1, i_2, \cdots, i_n) \leq \boldsymbol{j} := (j_1, j_2, \cdots, j_n)$ if and only if $i_k \leq j_k$ for each index $k \in Z_n$. We use $\boldsymbol{j} \geq \boldsymbol{i}$ synonymously with $\boldsymbol{i} \leq \boldsymbol{j}$, and $\boldsymbol{i} \not\leq \boldsymbol{j}$ will mean that, for at least one index $k, i_k > j_k$.

Let $(\sigma) := (\sigma_{\boldsymbol{i}})$ be a sequence of elements from a field $\mathbb{F}$, where $\boldsymbol{i} \in \mathbb{N}^n$ and $\boldsymbol{i} \geq \boldsymbol{0} := (0, 0, \cdots, 0)$. If (σ) satisfies a *linear recurrence relation* of the form

$$\sum_{s \in S} f_s \sigma_{s+i} = 0, \qquad \text{for all } \boldsymbol{i} \geq \boldsymbol{0}$$

where S is some finite nonempty subset of $\mathbb{N}^n$ and $f_s \in \mathbb{F}$ for all s, then (σ) is called an *n-dimensional linear recurring sequence* (or *n-D lrs*) in $\mathbb{F}$. We denote the power series ring $\mathbb{F}[[X_1, X_2, \cdots, X_n]]$ by $\mathbb{F}[[\boldsymbol{X}]]$ and abbreviate the monomial $X_1^{i_1} \cdots X_n^{i_n}$ to $\boldsymbol{X}^{\boldsymbol{i}}$. The corresponding polynomial

$$f(\boldsymbol{X}) := \sum_{s \in S} f_s \boldsymbol{X}^s$$

in $\mathbb{F}[\boldsymbol{X}]$ is the *characteristic polynomial* of (σ) associated with the previous relation. For convenience we define the zero polynomial to be a characteristic polynomial of every *n-D* lrs.

The set $\mathscr{I}(\sigma)$ of characteristic polynomials of (σ) clearly forms an ideal in $\mathbb{F}[\boldsymbol{X}]$, the *characteristic ideal* of (σ). By Hilbert's Basis theorem, $\mathscr{I}(\sigma)$ has a finite set of generators. Our aim in this paper is to describe a constructive method (Algorithm χ-BASE in Section III) by which such a basis may be determined when (σ) is *rectilinear*, that is, when $\mathscr{I}(\sigma)$ contains a polynomial in X_k with nonzero constant term for each $k \in Z_n$ (cf. Definition 3.2). From this we can derive a reduced Gröbner basis (RGB) for $\mathscr{I}(\sigma)$ for appropriate (σ). The construction of a basis for $\mathscr{I}(\sigma)$ is equivalent to the synthesis of an *n-D* linear feedback shift register (LFSR).

In [6], [7] we considered the problem of finding the minimal polynomial f of the (principal) ideal $\mathscr{I}(\sigma)$ where (σ) is a 1-D lrs in a factorial domain. The theory for such lrs developed in those papers will be used extensively in the present work. In particular, we shall have occasion to refer to the algorithm MINPOL developed there. For the convenience of the reader, Theorem 4.1 of [7] is repeated here as Theorem 3.1.

Sakata [22], [23] also gives a solution to the problem of synthesizing an *n-D* LFSR, based on an extension of the Berlekamp–Massey (BM) algorithm to n dimensions. On the other hand, *all* the steps in the χ-BASE algorithm may be carried out using techniques that are by now well-established. We illustrate our methods by applying them to [22, Example 2, p. 234], to a 3-D example over GF(2) and to a 2-D example over $\mathbb{Q}$.

Apart from rectilinearity, we shall also assume in Section IV that either a) certain degree bounds and beginning terms of (σ) are known, or b) certain 1-variable characteristic polynomials are known. These hypotheses are reasonable, since our methods apply in particular to doubly periodic arrays [20]–[22], 2-D linear recurring arrays [14], 2-D cyclic (or TDC) codes [8]–[12], [21], and also to more general polynomial codes in several variables [3]–[5], [15]–[17]. Moreover, our results may be applied to related areas such as the theory of the rational transfer functions associated with the synthesis of digital filters (cf. for example, [18]).

Notation

$\mathbb{F}$	Field.
$\mathbb{Q}$	Rational numbers.
U	Factorial domain.
$\mathbb{N}$	$\{0,1,2,\cdots\}$.
$\mathbb{N}^r$	Cartesian product of r copies of $\mathbb{N}$.
$\boldsymbol{i},\boldsymbol{j},\cdots$	Elements of $\mathbb{N}^r$ (r will be clear from the context).
$\leq$	Partial order on $\mathbb{N}^r$: the usual $\leq$ on each component.
Z_n	$\{1,\cdots,n\}$.
$\boldsymbol{X}$	$X_1, X_2,\cdots,X_n$.
$\hat{\boldsymbol{X}}_k$	$X_1,\cdots,X_{k-1},X_{k+1},\cdots,X_n$ ("X_k omitted").
$\mathbb{F}[\boldsymbol{X}]$	Polynomial domain.
$\mathbb{F}[[\boldsymbol{X}]]$, $\mathbb{F}[[\hat{\boldsymbol{X}}_k]]$	Power series domains.
U_k	Factorial domain $\mathbb{F}[[\hat{\boldsymbol{X}}_k]]$.
$\boldsymbol{X}^{\boldsymbol{i}}$	$X_1^{i_1}\cdots X_n^{i_n}$.
$\hat{\boldsymbol{X}}_k^{\boldsymbol{j}}$	$X_1^{j_1}\cdots X_{k-1}^{j_{k-1}}X_{k+1}^{j_{k+1}}\cdots X_n^{j_n}$ (here $\boldsymbol{j}\in\mathbb{N}^{n-1}$ and the context makes clear which element from Z_n is *not* used as subscript).
(σ)	n-dimensional linear recurring sequence (n-D lrs) in $\mathbb{F}$.
$G[(\sigma)]$	Generating function of (σ), as element of $\mathbb{F}[[\boldsymbol{X}]]$.
$(\sigma)^{(k)}$	(σ) regarded as a 1-D lrs in U_k.
$G[(\sigma)^{(k)}]$	Generating function of $(\sigma)^{(k)}$ in $U_k[[X_k]]$.
$\mathscr{I}(\sigma)$	Characteristic ideal of (σ).
$((\sigma)(k,\boldsymbol{j}))$	1-D lrs obtained from (σ) by fixing $\boldsymbol{j}\in\mathbb{N}^{n-1}$ and allowing the kth index to vary.
$f,g,\cdots$	Polynomials in $\boldsymbol{X}$.
(u,v)	Greatest common divisor of the polynomials u,v.
$p_k(X_k)$	Minimal X_k-polynomial of (σ).
$p[(\sigma)]$	Minimal product polynomial $p_1p_2\cdots p_n$ of (σ).
f^*	Reciprocal of f.
$\boldsymbol{\delta}f$	Degree of f.
$\mathscr{S}(f)$	Support of f.
$\boldsymbol{\epsilon}_kf$	$\min\{s_k\colon s\in\mathscr{S}(f)\}$.
$u\sim v$	$u(\boldsymbol{X})=av(\boldsymbol{X})$, where $a\in\mathbb{F}$, $a\neq 0$.

II. Preliminaries

Let $f\in\mathbb{F}[[\boldsymbol{X}]]$. The set $\mathscr{S}(f):=\{s\in\mathbb{N}^n\colon f_s\neq 0\}$ is called the *support* of f, where $\mathscr{S}(0)=\varnothing$. Thus the polynomials in $\boldsymbol{X}$ are precisely the elements of finite support in $\mathbb{F}[[\boldsymbol{X}]]$ and are expressed in the form

$$f=f(\boldsymbol{X})=\sum_{s\in\mathscr{S}(f)}f_s\boldsymbol{X}^s.$$

If f is a polynomial, the kth *partial degree* δ_kf of f is the degree of f regarded as a polynomial in X_k. If X_k does not appear in f then $\delta_kf=0$ except that $\delta_k(\mathbf{0})=-1$, for all k. The *degree* of f is the vector $\boldsymbol{\delta}f$ whose kth component is δ_kf. The *reciprocal* f^* of the polynomial f is $f^*(\boldsymbol{X}):=\boldsymbol{X}^{\boldsymbol{\delta}f}f(1/X_1,\cdots,1/X_n)$. Note that when $n=1$ this reduces to the usual definition (cf. [6], [7]).

It is clear that $\delta_kf=\max\{s_k\colon s\in\mathscr{S}(f)\}$. To clarify the relationship between f and f^*, we define the corresponding vector $\boldsymbol{\epsilon}f$, by $\epsilon_kf:=\min\{s_k\colon s\in\mathscr{S}(f)\}$ for f nonzero. If $u,v\in\mathbb{F}[\boldsymbol{X}]$ we denote their greatest common divisor by (u,v).

Lemma 2.1: Let $f\in\mathbb{F}[\boldsymbol{X}]$ be nonzero. Then

a) there is a polynomial $g(\boldsymbol{X})$ satisfying $\boldsymbol{\epsilon}g=\mathbf{0}$ such that $f(\boldsymbol{X})=\boldsymbol{X}^{\boldsymbol{\epsilon}f}g(\boldsymbol{X})$,
b) $\mathscr{S}(f^*)=\boldsymbol{\delta}f-\mathscr{S}(f):=\{\boldsymbol{\delta}f-s\colon s\in\mathscr{S}(f)\}$,
c) $\boldsymbol{\delta}f^*=\boldsymbol{\delta}f-\boldsymbol{\epsilon}f$,
d) $f^*=\sum_{t\in\mathscr{S}(f)}f_{\boldsymbol{\delta}f-t}\boldsymbol{X}^t$,
e) $\mathscr{S}(f^{**})=\mathscr{S}(f)-\boldsymbol{\epsilon}f:=\{s-\boldsymbol{\epsilon}f\colon s\in\mathscr{S}(f)\}$,
f) if $f(\boldsymbol{X})=u(\boldsymbol{X})v(\boldsymbol{X})$ then $f^*=u^*v^*$,
g) $f=\boldsymbol{X}^{\boldsymbol{\epsilon}f}f^{**}$,
h) if $g\in\mathbb{F}[\boldsymbol{X}]$, then $(f,g)^*=(f^*,g^*)$.

Proof: Properties a)–d) are straightforward consequences of the definitions. From b) $\mathscr{S}(f^{**})=\boldsymbol{\delta}f^*-\mathscr{S}(f^*)=\boldsymbol{\delta}f^*-(\boldsymbol{\delta}f-\mathscr{S}(f))=\mathscr{S}(f)-\boldsymbol{\epsilon}f$ by c). This proves e).

Next, note that $\boldsymbol{\delta}f=\boldsymbol{\delta}u+\boldsymbol{\delta}v$ so $f^*(\boldsymbol{X})=\boldsymbol{X}^{\boldsymbol{\delta}u+\boldsymbol{\delta}v}u(1/\boldsymbol{X})v(1/\boldsymbol{X})=u^*v^*$, as required for f). Finally, applying f) to $f=\boldsymbol{X}^{\boldsymbol{\epsilon}f}g(\boldsymbol{X})$ where $\boldsymbol{\epsilon}g=\mathbf{0}$, we have $f^*=(\boldsymbol{X}^{\boldsymbol{\epsilon}f})^*g^*=g^*$, so $f^{**}=g^{**}$. But $\boldsymbol{\epsilon}g=\mathbf{0}$ implies $\mathscr{S}(g^{**})=\mathscr{S}(g)$ by e), and d) applied twice gives $g^{**}=g$. Thus $f=\boldsymbol{X}^{\boldsymbol{\epsilon}f}f^{**}$ and g) is proved. Part h) is a straightforward extension of the proof of [7, Lemma 4.7] using a), f) and g). $\square$

We also need a lemma similar to the following result in the theory of Gröbner bases. Let u be a polynomial in the ideal $\mathscr{V}\subseteq\mathbb{F}[\boldsymbol{X}]$, and let $\{v_1,\cdots,v_l\}$ be a Grobner basis of $\mathscr{V}$. Then u can be expressed in the form $\sum_{i=1}^{l}h_iv_i$ where the leading power product in each summand h_iv_i is less than or equal to the leading power product of u in the total order under consideration (cf., for example, [19, Theorem 5.2A]). The following result, which we refer to throughout as the *reduction lemma*, differs in that we are not using a total order—it depends crucially on the assumption we shall make that each v_i is a 1-variable polynomial.

Lemma 2.2 (reduction lemma): Let $v_k\in\mathbb{F}[X_k]$ for $k\in Z_n$ be nonzero and let $u=\sum_{k=1}^{n}a_k(\boldsymbol{X})v_k$ where $a_k\in\mathbb{F}[\boldsymbol{X}]$. Then there exist polynomials $b_k(\boldsymbol{X})$, $k\in Z_n$ such that $u=\sum_{k=1}^{n}b_k(\boldsymbol{X})v_k$, where $\boldsymbol{\delta}u\geq\max_k\{\boldsymbol{\delta}(b_kv_k)\}$.

Proof: We consider degrees in X_1: there are three possibilities.

Case 1) $\delta_1a_1+\delta_1v_1>\delta_1a_k$ for all $k>1$. Here

$$\delta_1u=\delta_1a_1+\delta_1v_1=\max_k\{\delta_1(a_kv_k)\}$$

and the required condition on the degree of X_1 holds with $b_k=a_k$ for all k.

Case 2) $\delta_1a_1+\delta_1v_1=\delta_1a_{i_2}=\cdots=\delta_1a_{i_r}>\delta_1a_{i_j}$, for all $i_j\notin\{1,i_2,\cdots,i_r\}$. Now, either $\delta_1u=\delta_1a_1+\delta_1v_1=\max\{\delta_1(a_kv_k)\}$, in which case the condition already holds for the degree of X_1, or else the coefficient of $X_1^{\delta_1a_1+\delta_1v_1}$ on the right-hand side is zero. In the latter event, we may write

$$u_1X_1^{\delta_1a_1}cX_1^{\delta_1v_1}+u_{i_2}X_1^{\delta_1a_{i_2}}v_{i_2}+\cdots+u_{i_r}X_1^{\delta_1a_{i_r}}v_{i_r}=0$$

where $u_j\in\mathbb{F}[\hat{X}_1]$ is the coefficient of $X_1^{\delta_1a_j}$ in a_j and $c\in\mathbb{F}$ is the coefficient of $X_1^{\delta_1v_1}$ in v_1. Thus,

$$cu_1+u_{i_2}v_{i_2}+\cdots+u_{i_r}v_{i_r}=0$$

and we observe that this is an equation not involving X_1. By induction on the number of variables (the result is clearly true for $n=1$) we may replace, if necessary, the u_{i_j} by polynomials u'_{i_j} such that $u_1=\sum_{j=2}^{r}u'_{i_j}v_{i_j}$ where $u_1\in\mathbb{F}[\hat{X}_1]$ and $\delta_su_1\geq\max_j\{\delta_s(u'_{i_j}v_{i_j})\}$, for $s=2,3,\cdots,n$ and we have divided through by the coefficient c. Then,

$$u=\left(u_1X_1^{\delta_1a_1}+a'_1\right)v_1+a_{i_2}v_{i_2}+\cdots+a_{i_r}v_{i_r}+\sum_l a_lv_l$$

for some polynomial a'_1 where $\delta_1a'_1<\delta_1a_1$ and where l runs through those indexes not appearing in the set $\{1, i_2, \cdots, i_r\}$. Thus

$$\begin{aligned} u &= \left[\left[\sum_{j=2}^{r} u'_{i_j} v_{i_j}\right] X_1^{\delta_1 a_1} + a'_1\right] v_1 + a_{i_2} v_{i_2} + \cdots + a_{i_r} v_{i_r} + \sum_l a_l v_l \\ &= a'_1 v_1 + \sum_{j=2}^{r} \left[u'_{i_j} v_1 X_1^{\delta_1 a_1}\right] v_{i_j} + a_{i_2} v_{i_2} + \cdots + a_{i_r} v_{i_r} + \sum_l a_l v_l \\ &= a'_1 v_1 + \sum_{j=2}^{r} \left[u'_{i_j} v_1 X_1^{\delta_1 a_1} + a_{i_j}\right] v_{i_j} + \sum_l a_l v_l. \end{aligned}$$

Now the degree in X_1 of the first summand has been reduced, while that of the other summands has not been increased. Also, for $2 \le s \le n$, the degree in X_s of the first summand has clearly not been increased and the inequalities

$$\max_{1 \le k \le n} \delta_s(a_k v_k) \ge \delta_s u_1 \ge \max_{2 \le j \le r} \delta_s(u'_{i_j} v_{i_j})$$

show that the maximum degree in X_s of the other summands has not been increased. A similar statement holds for the other variables.

Case 3) $\delta_1 a_1 + \delta_1 v_1 < \delta_1 a_j$ for some $j > 1$. Here,

$$\delta_1 a_{i_1} = \cdots = \delta_1 a_{i_r} > \delta_1 a_{i_{r+1}} \ge \cdots \ge \delta_1 a_1 + \delta_1 v_1 \ge \cdots.$$

Now either $\delta_1 u = \delta_1 a_{i_1}$, in which case the condition already holds for X_1, or else the coefficient of $X_1^{\delta_1 a_{i_1}}$ on the right-hand side is zero. Thus,

$$u_{i_1} X_1^{\delta_1 a_{i_1}} v_{i_1} + \cdots + u_{i_r} X_1^{\delta_1 a_{i_r}} v_{i_r} = 0$$

where u_{i_j} is the coefficient of $X_1^{\delta_1 a_{i_j}}$ in a_{i_j}. These terms may simply be omitted from the summation thus reducing $\max\{\delta_1(a_k v_k)\}$ and without increasing the maximum degrees in the other variables.

The process outlined above may be repeated until eventually, either $\delta_1 u = \delta_1 a_1 + \delta_1 v_1 = \max\{\delta_1(a_k v_k)\}$, or $\delta_1 u = \delta_1 a_{i_1} = \max\{\delta_1(a_k v_k)\}$. The process clearly ends since $\max\{\delta_1(a_k v_k)\}$ is reduced at each stage, and it produces an expression for u in which the degree condition holds for X_1 *without increasing* $\max_k\{\delta_j(a_k v_k)\}$, for $j > 1$. It can now be repeated for each of the other variables in turn to give an expression of the required form. □

Remark 2.3: Although the proof of the Reduction Lemma is constructive, it is important to notice that only the *existence* of such an expression for u is used in the ideal basis theorem (Theorem 5.2) and the χ-BASE algorithm (Algorithm 3.8).

We continue with an example to illustrate the proof of the reduction lemma.

Example 2.4: Take $\mathbb{F} = \mathrm{GF}(2)$, $v_1(X) = X^2 + X + 1$, $v_2(Y) = Y^3 + 1$, $v_3(Z) = Z + 1$ and

$$\begin{aligned} u &= XYZ + X^2 Z + XZ + Z + XY^3 + XY + X \\ &= (XZ + X + 1)v_1 + (X^3 Z + X^3 + X)v_2 \\ &\quad + (X^3 Y^3 + XY + 1)v_3. \end{aligned}$$

Note that $\delta_1 u = 2$, and the conditions for Case 2) hold. The equation for the term that is a multiple of X^3 on the right-hand side is

$$[(Z+1)X]X^2 + (Z+1)X^3 v_2 + Y^3 X^3 v_3 = 0.$$

Thus,

$$(Z+1) + (Z+1)v_2 + Y^3 v_3 = 0 \text{ (the coefficient } c = 1).$$

This is an equation in one fewer variables that can be rewritten to satisfy the conclusion of the lemma as

$$Z + 1 = 0.v_2 + 1.v_3.$$

On substitution into the original equation, this inductive step gives

$$\begin{aligned} u &= [(0.v_2 + 1.v_3)X + 1]v_1 + a_2 v_2 + a_3 v_3 \\ &= 1.v_1 + a_2 v_2 + (a_3 + X v_1)v_3. \end{aligned}$$

Transferring the labels a_i to the coefficients in this new equation we have $\delta_1(a_1 v_1) = 2$, $\delta_1(a_j v_j) = 3$, for $j = 2, 3$ and so the conditions for Case 3) hold. The equation for the term in X^3 on the right-hand side is

$$(Z+1)X^3 v_2 + (Y^3+1)X^3 v_3 = 0$$

and hence these terms may be omitted to give

$$u = 1.v_1 + X.v_2 + (XY + X^2 + X + 1)v_3,$$

which satisfies the degree condition in X and also in Y, Z.

III. The Algorithm χ-Base

For the convenience of the reader we collect the main concepts and results in this section. This enables us to state the algorithm χ-BASE. We illustrate our approach by computing the reduced Gröbner basis (RGB) for [22, Example 2, p. 324].

We begin with a statement of one of the main results of [6], [7]. Here U is a factorial domain and we recall that if f is a polynomial in $U[Z]$ of degree $m \ge 0$ then $f^*(Z)$ is defined as $Z^m f(1/Z)$.

Theorem 3.1: Let (σ) be a 1-dimensional lrs in U with generating function $G(Z)$ and let f be a characteristic polynomial of (σ) of degree $m \ge 1$. Then there exists a polynomial g of degree at most $m - 1$ such that $f^* G = g$. Conversely, let u, v be polynomials with $v \ne 0$ and let (σ) be the sequence of coefficients of the power series $G = u/v$, which lies in $U[[Z]]$. Then (σ) is a linear recurring sequence with generating function G having $Z^e v^*$ as a characteristic polynomial where $e = \max\{0, \delta u - \delta v + 1\}$.

Definition 3.2: The *n-D* lrs (σ) is *rectilinear* if for each $k \in Z_n$, $\mathscr{I}(\sigma)$ contains a polynomial in X_k with nonzero constant term. In particular (σ) is *periodic* if, for each k, $\mathscr{I}(\sigma)$ contains $X_k^{i_k} - 1$ for some positive integer i_k.

Remark 3.3:

a) Clearly every 1-D lrs is rectilinear.
b) The definition of periodic for $n = 2$ is equivalent to that of *doubly periodic* as given in [22, p. 324]).
c) If $\mathbb{F}$ is finite, every rectilinear *n-D* lrs is periodic.
d) The requirement in the definition that the polynomial in X_k have nonzero constant term is used in the proofs of Theorems 4.1 and 4.2.

Definition 3.4: Let (σ) be rectilinear. Then a) the monic polynomial in X_k of least possible degree in $\mathscr{I}(\sigma)$ will be called the *minimal X_k-polynomial* of (σ) and denoted by $p_k(X_k)$ (p_X, p_Y, p_Z when only two or three variables are involved), b) the *minimal product polynomial* of (σ) is $p[(\sigma)] = p_1(X_1) p_2(X_2) \cdots p_n(X_n)$.

The requirement that $p_k(X_k)$ be monic is clearly no restriction. Moreover it will be clear from our analysis that $p_k(X_k)$ has nonzero constant term (cf. Corollary 4.6).

We associate with the *n-D* lrs (σ) its *generating function*

$$G[(\sigma)] := \sum_{i \in \mathbb{N}^n} \sigma_i X^i,$$

which lies in $\mathbb{F}[[X]]$. To illustrate the concepts of this section and the algorithm χ-BASE we shall work with the following example.

Example 3.5 ([22, Example 2, p. 324]): $n = 2$, $\mathbb{F} = \mathrm{GF}(2)$ and (σ) is the *doubly periodic sequence* whose generating function $G[(\sigma)]$ satisfies

$$\begin{aligned}(X^6+1)(Y^6+1)G[(\sigma)] &= (X^5+X^4+X^3+X^2)Y^5+(X^4+X^2)Y^4 \\ &\quad +(X^5+X^4+X+1)Y^3+(X^4+1)Y^2 \\ &\quad +(X^3+X^2+X+1)Y+X^2+1 \\ &= h(X,Y).\end{aligned}$$

(Note that this is the transpose of Sakata's array.)

To calculate the minimal X_k-polynomials for Example 3.5 we invoke the following theorem which is proved in Section IV.

Theorem 3.6 (cf. Theorem 4.3, Corollary 4.4): Let (σ) be periodic, with $X_k^{n_k} - 1 \in \mathscr{I}(\sigma)$, for $k \in Z_n$. Then a) $G[(\sigma)] = h(X)/\prod_{k \in Z_n}(X_k^{n_k} - 1)$ for some polynomial h, where $\delta_k h \leq n_k - 1$, and b) $p_k(X_k) = (X_k^{n_k} - 1)/(h^*, X_k^{n_k} - 1)$.

In Example 3.5, a simple calculation gives $(h^*, X^6 + 1) = X^2 + 1$, so that by Theorem 3.6, $p_X = X^4 + X^2 + 1$. Similarly $p_Y = Y^4 + Y^2 + 1$.

In Section IV we shall show how the results of [6], [7] may be used to calculate the minimal X_k-polynomials under two hypotheses that generalize [7, Theorem 4.8] and [7, Theorem 5.1], respectively. The first hypothesis is used when 1-variable characteristic polynomials are known, so it applies in particular to Example 3.5.

Effective Rectilinearity (ER-) Hypothesis) The following are known:

a) for each $k \in Z_n$, some (nonconstant) $g_k(X_k) \in \mathscr{I}(\sigma)$ satisfying $g_k(0) \neq 0$, and
b) the beginning terms σ_i of (σ) for all $\mathbf{0} \leq i \leq (d_1 - 1, \cdots, d_n - 1)$ where $d_k = \delta_k g_k$.

Berlekamp–Massey (BM-) Hypothesis) The following are known:

a) an upper bound $m_k \geq 1$ on the degree of $p_k(X_k)$ each $k \in Z_n$, and
b) the beginning terms σ_i of (σ), for all $\mathbf{0} \leq i \leq (2m_1 - 1, \cdots, 2m_n - 1)$.

The main theorem on which our methods depend is the following. It will be proved in Section V.

Theorem 3.7 (χ-Base Theorem cf. Theorem 4.2, Corollary 4.3): Let (σ) be a rectilinear *n-D* lrs in $\mathbb{F}$. Then $f \in \mathscr{I}(\sigma)$ if and only if there exist polynomials $u_k(X)$ such that

$$fq^* = \sum_{k=1}^{n} u_k p_k$$

where $q = p[(\sigma)]^* G[(\sigma)]$.

We are now able to state our algorithm.

Algorithm 3.8: χ-BASE.

Input: an *n-D* lrs (σ) satisfying either the ER- or the BM-hypothesis.

Output: a basis for $\mathscr{I}(\sigma)$, converted to an RGB if required.

1) Calculate the minimal X_k-polynomials $p_k(X_k)$ for $k \in Z_n$.
2) Determine $q := p[(\sigma)]^* G[(\sigma)]$ and hence determine q^*.
3) Find a set of generators for the polynomial solutions of the homogeneous equation

$$fq^* + a_1 p_1 + \cdots + a_n p_n = 0.$$

The set of polynomials f thus determined forms a basis for $\mathscr{I}(\sigma)$.

4) Convert the basis found in Step 3) to an RGB by standard methods (if required).

Remarks 3.9: a) In the following section we use the theory of lrs over a factorial domain to show how to carry out Step 1) in case (σ) satisfies the BM-hypothesis. (We have already seen in the example how this is carried out for the ER-case.) However, it should be noted that (even in the BM-case) Step 1) requires only calculations (MINPOL or Berlekamp-Massey) with lrs over $\mathbb{F}$. b) Step 3) is the calculation of a basis of syzygies of the ideal J generated by $\{q^*, p_1, \cdots, p_n\}$, which can be carried out using [2, Method 6.17, p. 219], for example. It is known (cf. [1]) that the complexity of calculating syzygies is—in the worst case—doubly exponential in n. However, because of the special form of the generators and their interrelationships there is reason to believe that the *regularity* of J (as defined in [1]) is "small" and hence that χ-BASE is inherently tractable. It should also be noted that in most of the applications mentioned in the Introduction it is the case $n = 2$ that is of current interest.

To apply the algorithm to our running example, we first find $q = X^3Y^3 + X^2Y^3 + X^2Y^2 + XY + Y + 1$ and $q^* = X^3Y^3 + X^3Y^2 + X^2Y^2 + XY + X + 1$. The three polynomials f that arise from the calculation following [1, p. 219] and using lexicographic ordering are $X^3Y^3 + X^3Y^2 + X^3Y + X^3 + 1$, $(Y^3 + Y^2 + Y + 1)(Y + X^3 + X + 1)$ and $X^4 + X^2 + 1$. The RGB for the ideal generated by these three polynomials is $\{X^4 + X^2 + 1, Y + X^3 + X + 1\}$ which (after account is taken of the change of ordering —Sakata uses graduated total degree ordering) is the same as that obtained in [22].

IV. Minimal X_k-Polynomials

In this section we show how the minimal X_k-polynomials may be calculated, beginning with easier case of lrs which satisfy the ER-hypothesis.

The first result establishes a fundamental property of characteristic polynomials which reduces in the case $n = 1$ to the first part of Theorem 3.1. Note that for this lemma (σ) need not necessarily be rectilinear.

Lemma 4.1: Let $f \in \mathscr{I}(\sigma)$. Then for all $\mathbf{r} \geq \boldsymbol{\delta} f$ the coefficient of $X^{\mathbf{r}}$ in $f^* G[(\sigma)]$ is zero.

Proof: For each $s \in \mathscr{S}(f)$ there is a term $f_s X^{\boldsymbol{\delta} f - s}$ in f^* which multiplies the term $\sigma_{\mathbf{r} - \boldsymbol{\delta} f + s} X^{\mathbf{r} - \boldsymbol{\delta} f + s}$ in $G = G[(\sigma)]$ (note that $\mathbf{r} - \boldsymbol{\delta} f + s \geq \mathbf{0}$ by virtue of the hypothesis on $\mathbf{r}$) to give $\sigma_{\mathbf{r} - \boldsymbol{\delta} f + s} f_s X^{\mathbf{r}}$ in $f^* G$. Thus the coefficient of $X^{\mathbf{r}}$ in $f^* G$ is $\sum_{s \in \mathscr{S}(f)} f_s \sigma_{\mathbf{r} - \boldsymbol{\delta} f + s}$, which is zero since f is a characteristic polynomial and $\mathbf{r} - \boldsymbol{\delta} f \geq \mathbf{0}$. □

When (σ) is rectilinear with minimal X_k-polynomial $p_k(X_k)$ for $k \in Z_n$, $p = p[(\sigma)]$ is clearly in $\mathscr{I}(\sigma)$. Note that $\delta_k p = \delta_k p_k$ for each k. Applying the previous lemma we have the following.

Corollary 4.2: Define $q := p^*G[(\sigma)]$. Then q is a polynomial satisfying $\boldsymbol{\delta} q \leq (\delta_1 p_1 - 1, \cdots, \delta_n p_n - 1)$.

Similarly, under the ER-hypothesis, we can write $g^*(X)G[(\sigma)] = h(X)$ where g is the product of the known characteristic polynomials $g_k(X_k)$ and $h \in \mathbb{F}[X]$ satisfies the corresponding degree restriction.

Theorem 4.3: Let (σ) be rectilinear and suppose that $G[(\sigma)] = h(X)/g^*(X)$ where $g(X) = \prod_{k \in Z_n} g_k(X_k)$ is a monic polynomial with $g_k(0) \neq 0$ for each k. Then $g_k/(h^*, g_k)$ is the minimal X_k-polynomial of (σ).

Proof: In the following the pi sign denotes the product taken over $k \in Z_n$ and the tilde means is equal to, up to multiplication by a nonzero element of $\mathbb{F}$.

Let $p = \prod p_k$ be the minimal product polynomial of (σ) and $q = p^*G[(\sigma)]$, so that $hp^* = g^*q$. If $d_k = (h, g_k^*)$, then

$$(h/\textstyle\prod d_k)p^* = (g^*/\prod d_k)q = (\prod g_k^*/d_k)q$$

by Lemma 2.5 f). Further $(q, p_k^*) = 1$, because otherwise we could replace p_k by a polynomial of smaller degree. Since g_k^* is a polynomial in X_k, any divisor of h and $\prod g_k^*$ is a divisor of h and of g_k^* for all $k \in Z_n$ (and conversely). In other words $(h, g^*) = \prod (h, g_k^*) = \prod d_k$ and $h/\prod d_k$ is relatively prime to $g^*/\prod d_k$. Using unique factorization in $\mathbb{F}[X]$, we conclude that $p^* \sim g^*/\prod d_k$, that is, $\prod p_k^* \sim \prod (g_k^*/d_k)$. This implies that $p_k^* \sim g_k^*/d_k$ (because $p_k, g_k \in \mathbb{F}[X_k]$) and so $p_k = p_k^{**} \sim (g_k^*/d_k)^* = g_k/d_k^*$. Now p_k and g_k are both monic so the conclusion follows from Lemma 2.5 h). □

In the periodic case $g_k(X_k)$ has the form $X_k^{n_k} - 1$ and clearly the product g satisfies $g^* = \pm g$. Thus $G[(\sigma)] = h(X)/\prod_{k \in Z_n}(X_k^{n_k} - 1)$ for some h. Applying the theorem to this case, we have the following corollary.

Corollary 4.4: Let (σ) be periodic and express $G[(\sigma)]$ in the form previously given. Then $(X_k^{n_k} - 1)/(h^*, X_k^{n_k} - 1)$ is the minimal X_k-polynomial of (σ).

We note that Theorem 4.3 also yields $q = p^*G[(\sigma)]$ as $h/\prod(h^*, g_k)^*$. In general, the gcd calculations of the theorem would be carried out using, for example, a polynomial remainder sequence algorithm in $\mathbb{F}[X]$. However, in the periodic case described by the corollary, we may take advantage of the special form of $g_k = X_k^{n_k} - 1$, when its factors are known, to reduce the calculation to a systematic sequence of trials, as illustrated in Example 3.5.

Turning now to the general case we observe that the sequence (σ) may also be regarded for each $k \in Z_n$ as a 1-parameter sequence each term of which is itself an $(n-1)$-parameter sequence of elements from $\mathbb{F}$. When (σ) is so regarded we shall denote it by $(\sigma)^{(k)}$. We write $\hat{X}_k$ (read "X_k omitted") for the list $X_1, \cdots, X_{k-1}, X_{k+1}, \cdots, X_n$ (and make the corresponding extension to monomials such as $\hat{X}_k^{j}$ where $j \in \mathbb{N}^{n-1}$). By [24, Theorem 6, p. 148] $U_k = \mathbb{F}[[\hat{X}_k]]$ is a factorial domain: this fact will be used without further mention. The generating function $G[(\sigma)^{(k)}]$ is a power series in X_k each coefficient of which may be represented as a power series in $\hat{X}_k$. Thus $G[(\sigma)^{(k)}]$ is simply $G[(\sigma)]$ regarded as an element of $U_k[[X_k]]$. Our first aim is to show that $(\sigma)^{(k)}$ is a 1-D lrs in U_k, whose minimal polynomial is in fact the minimal X_k-polynomial of (σ).

Theorem 4.5: Let $f = f(X_k)$ where $f(0) \neq 0$. Then $f \in \mathscr{I}(\sigma)$ if and only if $(\sigma)^{(k)}$ is a 1-D lrs in U_k with f as a characteristic polynomial.

Proof: For simplicity we consider the case $k = 1$. The analogous proof for $k \geq 2$ is similar. If $(\sigma)^{(1)}$ is a 1-D lrs in U_1 with $f = f(X_1)$ as a characteristic polynomial, let d be the degree of f. Then, by Theorem 2.1, $f^*G[(\sigma)^{(1)}] = g$ is a polynomial in X_1 of degree at most $d-1$ with coefficients in U_1. Thus $f^*G[(\sigma)] = g \in \mathbb{F}[[X]]$. Also, if f is regarded as an element of $\mathbb{F}[X]$, then $\mathscr{S}(f) = \mathscr{S}(f^*) = \{\boldsymbol{s} = (s, 0, \cdots, 0): 0 \leq s \leq d\}$. Since g is a polynomial in X_1 of degree less than d, the coefficient of $X_1^{i_1}$ in $f^*G[(\sigma)]$ is zero for $i_1 \geq d$. In order to write out this coefficient, we denote vectors in $\mathbb{N}^n$ by $(r, \boldsymbol{t})$, where $r \in \mathbb{N}$ and $\boldsymbol{t} \in \mathbb{N}^{n-1}$. The required coefficient is

$$\sum_{j \in \mathbb{N}^{n-1}} \left[f_0 \sigma_{(i_1 - d, j)} + \cdots + f_d \sigma_{(i_1, j)} \right] \hat{X}_1^{j},$$

where we have used the fact that $f^* = f_d + f_{d-1}X_1 + \cdots + f_0 X_1^d$. Putting this equal to zero we find that for all $i_1 \geq d$ and all $j \in \mathbb{N}^{n-1}$,

$$\sum_{s=0}^{d} f_s \sigma_{(i_1 - d + s, j)} = 0.$$

Since $(i_1 - d, j)$ is an arbitrary element, $\boldsymbol{i}$ say, of $\mathbb{N}^n$, we have

$$\sum_{\boldsymbol{s} \in \mathscr{S}(f)} f_{\boldsymbol{s}} \sigma_{\boldsymbol{s}+\boldsymbol{i}} = 0, \qquad \text{for all } \boldsymbol{i} \geq \boldsymbol{0}$$

and this means that $f \in \mathscr{I}(\sigma)$.

Conversely, it is clear that this argument may be reversed to show that if $f = f(X_1) \in \mathscr{I}(\sigma)$, then $f^*G[(\sigma)]$ is a polynomial in X_1 of degree l less than d. Since this is just $f^*G[(\sigma)^{(1)}]$, we conclude, by Theorem 3.1, that $(\sigma)^{(1)}$ is a 1-D lrs in U_1 and $X_1^e f^{**}$ is a characteristic polynomial of $(\sigma)^{(1)}$ where $e = \max\{0, l - d + 1\}$. Thus $e = 0$ and since $f^{**} = f$ the theorem is proved. □

Corollary 4.6: The minimal X_k-polynomial $p_k(X_k)$ of the rectilinear $n - D$ lrs (σ) is the minimal polynomial of $(\sigma)^{(k)}$. Furthermore, $p_k(0) \neq 0$.

Proof: The theorem implies that $p_k(X_k)$ is a characteristic polynomial of $(\sigma)^{(k)}$. If $p_k(X_k)$ is not the minimal polynomial of $(\sigma)^{(k)}$ then some polynomial $g_k(X_k) \in U_k[X_k]$ of smaller degree is a characteristic polynomial of $(\sigma)^{(k)}$, divides p_k and hence by the theorem is in $\mathscr{I}(\sigma)$. Since any polynomial that is irreducible in $\mathbb{F}[X_k]$ is also irreducible in $U_k[X_k]$, g divides p_k in $\mathbb{F}[X_k]$, which contradicts the definition of p_k. Now, by definition $\mathscr{I}(\sigma)$ contains some polynomial $f(X_k)$ with $f(0) \neq 0$, and by the theorem f is a characteristic polynomial of $(\sigma)^{(k)}$. Thus $p_k | f$ and consequently $p_k(0) \neq 0$. □

We can therefore regard a rectilinear *n-D* lrs in $\mathbb{F}$ as a 1-D lrs in U_k for each k.

Corollary 4.7: Let (σ) be rectilinear and assume the BM-hypothesis. Then the minimal X_k-polynomial of (σ) can be calculated using MINPOL in U_k.

In theory this calculation involves applying the XPRS algorithm of [6], [7] to $X_k^{2m_k}$ and a polynomial in X_k of degree (at most) $2m_k - 1$ with coefficients in U_k. If those coefficients were arbitrary elements of U_k, the calculation could not be carried out effectively: it is the presence of the minimal X_l-polynomials for $l \neq k$ that will make this possible. Our next aim is to reduce the determination of $p_k(X_k)$ to finding a *finite* number of minimal polynomials of 1-D lrs in $\mathbb{F}$.

Let (σ) be rectilinear with minimal X_1-polynomial $p_1(X_1) = p_{1,0} + p_{1,1}X_1 + \cdots + p_{1,\delta_1 p_1} X^{\delta_1 p_1}$, and let $j \in \mathbb{N}^{n-1}$ be fixed.

Then, as in the proof of Theorem 4.5,

$$\sum_{s=0}^{\delta_1 p_1} p_{1,s}\sigma_{(s+i_1,j)} = 0, \qquad \text{for all } i_1 \geq 0.$$

Definition 4.8: Let $j \in \mathbb{N}^{n-1}$ be fixed. We denote by $(\sigma(1,j))$ the sequence whose i_1th term is $\sigma_{(i_1,j)}$ and call it the *X_1-subsequence of (σ) associated with j*. For $k \geq 1$ the X_k-subsequences $(\sigma(k,l))$ of (σ) are defined similarly (where l is an exponent of $\hat{X}_k$).

The following lemma is a consequence of the definition.

Lemma 4.9: The minimal X_k-polynomial $p_k(X_k)$ is a characteristic polynomial of each X_k-subsequence.

We shall now prove that to determine $p_k(X_k)$, it is sufficient to consider only a finite number of the X_k-subsequences of (σ). The precise sense in which this is true is given by Theorem 4.10.

Theorem 4.10: The minimal X_k-polynomial of (σ) is the least common multiple of the minimal polynomials of the X_k-subsequences $(\sigma(k,l))$ for

$$l \leq (\delta_1 p_1 - 1, \cdots, \delta_{k-1}p_{k-1} - 1,\, \delta_{k+1}p_{k+1} - 1, \cdots, \delta_n p_n - 1).$$

Proof: In the following discussion we take $k = 1$ for notational convenience and clarity of expression. The argument for $k \geq 2$ follows the same pattern.

We have seen that p_1 is a characteristic polynomial of each X_1-subsequence. Let $u_1(X_1)$ be the least common multiple of the (monic) minimal polynomials of the X_1-subsequences $(\sigma(1,j))$ for $j \leq (\delta_2 p_2 - 1, \cdots, \delta_n p_n - 1)$. Thus $u_1 | p_1$. We shall prove that, in fact, $p_1 = u_1$. For this we show that $X_1^e u_1$ is a characteristic polynomial of $(\sigma)^{(1)}$ for some exponent $e \geq 0$. Then $p_1 | X_1^e u_1$ by Corollary 4.6 and since p_1 is not divisible by X_1 we have $p_1 | u_1$. Since p_1 and u_1 are both monic this means they are the same.

To prove that $X_1^e u_1$ is a characteristic polynomial of $(\sigma)^{(1)}$, it suffices to show that $u_1^* G[(\sigma)] = u_1^* G[(\sigma)^{(1)}]$ is a polynomial in X_1. By Theorem 3.1 this will imply that $X_1^e u_1^{**}$ is a characteristic polynomial of $(\sigma)^{(1)}$ for some $e \geq 0$, and the desired conclusion will follow since $u_1 | p_1$ implies $u_1^{**} = u_1$.

Write $G = G[(\sigma)^{(1)}]$ in the form

$$\sum_{j \in \mathbb{N}^{n-1}} \left\{ \sum_{i_1 \in \mathbb{N}} \sigma_{(i_1,j)} X_1^{i_1} \right\} \hat{X}_1^j.$$

Since $u_1 \in \mathscr{I}(\sigma(1,j))$ for $j \leq (\delta_2 p_2 - 1, \cdots, \delta_n p_n - 1)$, it is clear that for such j the coefficient of $\hat{X}_1^j$ in the product $u_1^* G$ is a polynomial in X_1. We prove that this is also the case for the coefficient of $\hat{X}_1^j$ for $j \nleq (\delta_2 p_2 - 1, \cdots, \delta_n p_n - 1)$. To achieve this we use induction on each component of j separately. Consider, then, the coefficient of $\hat{X}_1^j$ with $j = (\delta_2 p_2, \delta_3 p_3 - 1, \cdots, \delta_n p_n - 1)$ and write this coefficient as $\sum_{i_1 \in \mathbb{N}} \sigma_{(i_1,j)} X_1^{i_1}$. We also define $j' \in \mathbb{N}^{n-2}$ by $j = (\delta_2 p_2, j')$. By hypothesis $p_2 \in \mathscr{I}(\sigma)$ so

$$\sum_{s=0}^{\delta_2 p_2} p_{2,s}\sigma_{(0,s,0,\cdots,0)+(i_1,\cdots,i_n)} = 0, \qquad \text{for all } \boldsymbol{i} \geq \boldsymbol{0},$$

where we have written $p_2(X_2) = \sum_{s=0}^{\delta_2 p_2} p_{2,s} X_2^s$. In particular, taking $\boldsymbol{i} = (i_1, 0, j')$, we have

$$\sum_{s=0}^{\delta_2 p_2} p_{2,s}\sigma_{(i_1,s,j')} = 0,$$

and, since p_2 is monic, we can write

$$\sigma_{(i_1,\delta_2 p_2,j')} + \sum_{s=0}^{\delta_2 p_2 - 1} p_{2,s}\sigma_{(i_1,s,j')} = 0.$$

Thus the coefficient of $\hat{X}_1^j$ is

$$-\sum_{i_1 \in \mathbb{N}} \sum_{s=0}^{\delta_2 p_2 - 1} p_{2,s}\sigma_{(i_1,s,j')} X_1^{i_1} = -\sum_{s=0}^{\delta_2 p_2 - 1} p_{2,s} \sum_{i_1 \in \mathbb{N}} \sigma_{(i_1,s,j')} X_1^{i_1}.$$

Note that each of the sums $\sum_{i_1 \in \mathbb{N}} \sigma_{(i_1,s,j')} X_1^{i_1}$ for $0 \leq s \leq \delta_2 p_2 - 1$ is the coefficient of $\hat{X}_1^l$ for some $l \leq (\delta_2 p_2 - 1, \cdots, \delta_n p_n - 1)$ and thus the coefficient of $\hat{X}_1^j$ for $j = (\delta_2 p_2, \delta_3 p_3 - 1, \cdots, \delta_n p_n - 1)$ is an $\mathbb{F}$-linear combination of coefficients of $\hat{X}_1^l$ for such l. Consequently, when this coefficient is multiplied by u_1^*, the resulting product is a polynomial in X_1. The induction step is now clear and we have proved the claim for $j = (j_2, \delta_3 p_3 - 1, \cdots, \delta_n p_n - 1)$ for arbitrary j_2.

When $n \geq 3$ we need to consider the coefficient of $\hat{X}_1^j$ for $j = (j_2, \delta_3 p_3, j'')$ where j_2 is arbitrary and $j'' \in \mathbb{N}^{n-3}$ satisfies $j'' \leq (\delta_4 p_4 - 1, \cdots, \delta_n p_n - 1)$. An argument similar to the foregoing reduces this coefficient to a sum of coefficients of $\hat{X}_1^l$ for $l \leq (j_2, \delta_3 p_3 - 1, \cdots, \delta_n p_n - 1)$ each of which gives, by the previous step, a polynomial in X_1 when multiplied by u_1^*. The induction necessary to complete the argument for $j = (j_2, j_3, j'')$ for arbitrary j_2, j_3 and for $j'' \leq (\delta_4 p_4 - 1, \cdots, \delta_n p_n - 1)$ is now clear, as is the induction on the number of variables necessary to complete the analysis for the first variable. As remarked earlier, the other minimal X_k-polynomials for $k \geq 2$ may be treated similarly, and this completes the proof of the theorem. □

Remark 4.11: Assuming the BM-Hypothesis we have an upper bound on the degree $\delta_k p_k$ so the theorem provides a (finite) procedure for determining the minimal X_k-polynomial from at most $\prod_{j \neq k} m_j$ X_k-subsequences. In practice this reduces to $\prod_{\substack{j<k \\ l>k}} (\delta_j p_j) m_l$ since the actual degree may be used instead of the upper bound once the corresponding polynomial has been found. When the ER-Hypothesis is assumed at most $\prod_{j \neq k} \delta_j p_j$ X_k-subsequences must be analyzed.

We illustrate the ideas developed thus far with several examples.

Example 4.12 (Example 3.5 revisited): We have

$$G[(\sigma)] = (1 + X^2 + \cdots) + (1 + X + X^2 + X^3 + \cdots)Y + (1 + X^4 + \cdots)Y^2 + \cdots.$$

The upper bounds for the BM-Hypothesis can both be taken as 6, and so the minimal X-polynomial p_X is the lcm of the minimal polynomials of the X-subsequences corresponding to Y^l for $l \leq \delta p_Y - 1 = 5$. Using MINPOL or BM over GF(2), or simply factorizing $X^6 + 1$ and trying each factor in turn, we find that $X^4 + X^2 + 1$ is the minimal polynomial of each of these sequences, and hence $p_X = X^4 + X^2 + 1$. This means $\delta p_X = 4$ so p_Y is the lcm of the Y-subsequences corresponding to X^l for $l \leq \delta p_X - 1 = 3$. Again, a simple calculation gives $p_Y = Y^4 + Y^2 + 1$.

Example 4.13: $\mathbb{F} = \mathrm{GF}(2)$, and (σ) is the *triply periodic* sequence such that $(X^2+1)(Y^3+1)(Z^4+1)G[(\sigma)] = (Y^2+1)(XZ^2+1)$. It is easy to see that the minimal X_k-polynomials are $p_X = X^2 + 1$, $p_Y = Y^2 + Y + 1$, $p_Z = Z^4 + 1$.

Example 4.14: $n = 2$, $\mathbb{F} = \mathbb{Q}$ and (σ) is the *doubly periodic* sequence such that $(X^4 - 1)(Y^2 - 1)G[(\sigma)] = (X^2+1)(-XY+1)$. Here $p_X = X^2 - 1$ and $p_Y = Y^2 - 1$.

V. Characteristic Polynomials in More Than One Variable

For the characteristic polynomials f of (σ) that contain more than one variable, we generalize Theorem 3.1.

Theorem 5.1: Let (σ) be rectilinear with minimal product polynomial p and let $p^*G = q$. Suppose that $f \in \mathscr{I}(\sigma)$. Then there exist polynomials $g_k(X)$ such that

$$f^*q = \sum_{k=1}^{n} g_k p_k^*.$$

Conversely, if v is a nonzero polynomial and there exist polynomials $u_k(X)$ such that

$$vq = \sum_{k=1}^{n} u_k p_k^*$$

then $v^* \in \mathscr{I}(\sigma)$.

Proof: Suppose first that $f \in \mathscr{I}(\sigma)$. By Lemma 4.1 the coefficient of X^r in f^*G is zero for all $r \geq \boldsymbol{\delta} f$. Thus, for each monomial X^j in f^*G with a nonzero coefficient, at least one of the components j_k is less than $\delta_k f$. We group the terms of f^*G together according to the following partition of the set $\mathscr{T} := \mathbb{N}^n - \{r \in \mathbb{N}^n : r \geq \boldsymbol{\delta} f\}$. Define $\mathscr{T}_1 := \{j \in \mathscr{T}: j_1 < \delta_1 f\}$ and, when $\mathscr{T}_1, \cdots, \mathscr{T}_{k-1}$ have been defined, define $\mathscr{T}_k := \{j \in \mathscr{T} - \cup_{i=1}^{k-1} \mathscr{T}_i : j_k < \delta_k f\}$. (It is clear that $\cup_{i=1}^{n} \mathscr{T}_i = \mathscr{T}$ and that $\mathscr{T}_i \cap \mathscr{T}_j = \varnothing$, for $i \neq j$.) Thus $f^*G = G_1 + G_2 + \cdots + G_n$ where $G_k \in U_k[X_k]$ and has support $\mathscr{T}_k$. As such, we can denote its degree by $\delta_k G_k$ and observe that $\delta_k G_k < \delta_k f$. We now prove that, for all k, $g_k = (p^*/p^*_k) G_k$ is a polynomial in X.

For a contradiction, suppose that k is the smallest index for which g_k is not a polynomial in X. It is certainly a polynomial in X_k, by definition of G_k, so let r be the smallest exponent such that the coefficient of X_k^r in g_k is not a polynomial in $\hat{X}_k$. Since $p_k^*(0) \neq 0$ this means that the coefficient of X_k^r in $p^*G_k = p_k^* g_k$ is not a polynomial in $\hat{X}_k$. But p^*G is a polynomial in X so the term in X_k^r in the expansion of p^*G_k as a polynomial in X_k must cancel with other multiples of X_k^r in the expansion of p^*G. Now $r \leq \delta_k G_k < \delta_k f$ and for $l > k$, $X_k^{\delta_k f}$ divides G_l by construction, so these cancelling terms cannot come from the summands p^*G_l for $l > k$. Also, by definition of k, either $k = 1$ or all the previous terms $p^*G_1, \cdots, p^*G_{k-1}$ are polynomials in X and so the required cancellation cannot take place. From this contradiction we conclude that g_k is a polynomial for each k, and

$$\begin{aligned} f^*q &= p^*f^*G = p^*G_1 + \cdots + p^*G_n \\ &= p_1^* g_1 + \cdots + p_n^* g_n. \end{aligned}$$

Conversely, let $v \neq 0$ be a polynomial in X and suppose there exist polynomials $u_k(X)$ such that $vq = \sum_k u_k p_k^*$. Define $\boldsymbol{e}$ by $e_k = \max\{0, \delta_k u_k - \delta_k v + 1\}$ so that $\boldsymbol{e} \geq \boldsymbol{0}$ and

$$\delta_k v + e_k = \begin{cases} \delta_k v, & \text{if } \delta_k v \geq \delta_k u_k + 1 \\ \delta_k u_k + 1, & \text{if } \delta_k v \leq \delta_k u_k \end{cases}.$$

The assumption on vq implies that

$$vG = \sum_{k=1}^{n} \frac{u_k(X)}{\prod_{j \neq k} p_j^*} = \sum_{k=1}^{n} H_k$$

where $H_k \in U_k[X_k]$ and has degree $\delta_k u_k$. The coefficient of X^r in vG is 0 for $r \geq \boldsymbol{\delta} v + \boldsymbol{e}$, by hypothesis, and thus

$$\sum_{s \in \mathscr{S}(v)} v_s \sigma_{\boldsymbol{\delta} v + \boldsymbol{e} - s + i} = 0, \qquad \text{for all } i \geq \boldsymbol{0}.$$

Define $t = \boldsymbol{\delta} v + \boldsymbol{e} - s$, so that t runs through $\boldsymbol{e} + \mathscr{S}(v^*)$ as s runs through $\mathscr{S}(v)$. Then,

$$\sum_{t \in \boldsymbol{e} + \mathscr{S}(v^*)} v_{\boldsymbol{\delta} v + \boldsymbol{e} - t} \sigma_{t+i} = 0, \qquad \text{for all } i \geq \boldsymbol{0},$$

that is,

$$\sum_{t \in \boldsymbol{e} + \mathscr{S}(v^*)} w_t \sigma_{t+i} = 0, \qquad \text{for all } i \geq \boldsymbol{0}$$

where the corresponding polynomial $w(X)$ satisfies $\mathscr{S}(w) = \boldsymbol{e} + \mathscr{S}(v^*)$, $w \in \mathscr{I}(\sigma)$ and $w = X^{\boldsymbol{e}} v^*$.

However, by the reduction lemma we can assume that $\boldsymbol{\delta}(vq) \geq \max_k \{\boldsymbol{\delta}(u_k p_k^*)\}$. Corollary 4.2 now implies $\delta_k u_k < \delta_k v_k$, so that $e_k = 0$ and this completes the proof. □

We now consider the relationship between $\mathscr{I}(\sigma)$ and the syzygy module (cf. [24, Section VII.13, pp. 237ff.]) of the ideal in $\mathbb{F}[X]$ generated by $\{q^*, p_1, \cdots, p_n\}$.

Theorem 5.2 (χ-BASE theorem): Let (σ) be a rectilinear lrs. Then $f \in \mathscr{I}(\sigma)$ if and only if there exist polynomials $u_k(X)$ such that

$$fq^* = \sum_{k=1}^{n} u_k p_k(X_k).$$

Proof: Suppose $f \in \mathscr{I}(\sigma)$. Then by Theorem 5.1 $f^*q = \sum a_k p_k^*$, where by the reduction lemma we may assume $\boldsymbol{\delta}(f^*q) \geq \boldsymbol{\delta} a_k + \boldsymbol{\delta} p_k^*$, for $k \in Z_n$. Now,

$$(f^*q)^* = X^{\boldsymbol{\delta}(f^*q)} \sum a_k(1/X_1, \cdots, 1/X_n) p_k^*(1/X_1, \cdots, 1/X_n)$$

so that

$$f^{**}q^* = \sum X^{\boldsymbol{\delta}(f^*q) - \boldsymbol{\delta} a_k - \boldsymbol{\delta} p_k^*} a_k^* p_k^{**}$$

since the exponent of X in each summand is nonnegative. Therefore, multiplying both sides by $X^{\epsilon f}$, we obtain

$$X^{\epsilon f} f^{**} q^* = \sum X^{\boldsymbol{\delta}(f^*q) - \boldsymbol{\delta} a_k - \boldsymbol{\delta} p_k + \epsilon f} a_k^* p_k$$

where we have used the fact that $p_k^{**} = p_k$ and $\boldsymbol{\delta} p_k^* = \boldsymbol{\delta} p_k$. But the left-hand side of this expression is fq^* by Lemma 5.5g), and the right-hand side is in the required form.

Conversely, if $fq^* = \sum u_k p_k$ then, again using the reduction lemma, we may assume $\boldsymbol{\delta}(fq^*) \geq \boldsymbol{\delta} u_k + \boldsymbol{\delta} p_k$ so that

$$f^*q^{**} = (fq^*)^* = \sum X^{\boldsymbol{\delta}(fq^*) - \boldsymbol{\delta} u_k - \boldsymbol{\delta} p_k} u_k^* p_k^*.$$

Hence, multiplying both sides by $X^{\epsilon q}$, we obtain

$$f^*q = \sum X^{\boldsymbol{\delta}(fq^*) - \boldsymbol{\delta} u_k - \boldsymbol{\delta} p_k + \epsilon q} u_k^* p_k^* = \sum b_k p_k^*.$$

By Theorem 5.1, $f^{**} \in \mathscr{I}(\sigma)$ and since $f = X^{\epsilon f} f^{**}$, f itself lies in $\mathscr{I}(\sigma)$. □

As a consequence of the previous two theorems we have the next corollary.

Corollary 5.3: Let (σ) be a rectilinear lrs. The following are equivalent

a) $f \in \mathscr{I}(\sigma)$,
b) there exist polynomials $g_k(X)$ such that $f^*q = \sum_{k=1}^{n} g_k p_k^*$,
c) there exist $u_k(X)$ such that $fq^* = \sum_{k=1}^{n} u_k p_k$.

Proof: It only remains to see that b) implies $f^{**} \in \mathscr{I}(\sigma)$ by Theorem 5.1 and hence by Lemma 2.1g), $f \in \mathscr{I}(\sigma)$. □

We end by reconsidering Examples 4.13 and 4.14. (Recall that lexicographic ordering is used.)

Example 5.4 (from 4.13): Here $q = XYZ^2 + XZ^2 + Y + 1 = (XZ^2 + 1)(Y + 1) = q^*$. The polynomials f that arise in the calculation are $X^2Y^2 + X^2Y + 1$, $XYZ^2 + X^2Y$, $X^2 + 1$ and $Y^2 + Y + 1$. The RGB for the ideal generated by these four polynomials is $\{Z^2 + X, Y^2 + Y + 1, X^2 + 1\}$.

Example 5.5 (from 4.14): Here $q = -XY + 1$ and $q^* = XY - 1$. The polynomials that arise in the calculation are $-X^2 + 1$, $-XY - X^2$ and $-X^3 + X$. The RGB for the ideal generated by these three polynomials is $\{X^2 - 1, Y + X\}$.

Notes Added in Proof

When carrying out the computation required by Step 3 of the χ-BASE algorithm and discussing its complexity we used Method 6.17 of [2]. We realized later that Method 6.7 of the same paper is more appropriate to our purposes and gives a significant improvement in the algorithm. The complexity is now $O(D)^3$ where D is the product of the degrees of the minimal X_k-polynomials.

Acknowledgment

The authors wish to thank the referees for their helpful comments.

References

[1] D. Bayer and M. Stillman, "On the complexity of computing syzygies," *J. Symb. Computation*, vol. 6, pp. 135–147, 1988.
[2] B. Buchberger, "Gröbner bases: An algorithmic method in polynomial ideal theory," in *Multidimensional Systems Theory*, N. K. Bose, Ed. Dordrecht: Reidel, 1985, 184–232.
[3] P. Charpin, "Les codes de Reed–Solomon en tant qu'idéaux d'une algèbre modulaire," *C. R. Acad. Sc. Paris (I)*, vol. 294, pp. 597–600, 1982.
[4] ____, "Codes cycliques étendus et idéaux principaux d'une algèbre modulaire," *C. R. Acad. Sc. Paris (I)*, vol. 295, pp. 313–315, 1982.
[5] ____, "Codes cycliques étendus invariants sous le groupe affine," Thèse de Doctorat d'Etat, Univ. Paris VII, 1987.
[6] P. Fitzpatrick and G. H. Norton, "Linear recurrence relations and an extended subresultant algorithm," in *Coding Theory and Applications*, G. Cohen and J. Wolfmann, Eds. Toulon: Springer Lecture Notes in Computer Science 388, 1988, pp. 232–243.
[7] ____, "The Berlekamp–Massey algorithm and linear recurring sequences over a factorial domain," submitted to *J. Algorithms*.
[8] T. Ikai, H. Kosako, and Y. Kojima, "Two-dimensional cyclic codes," *Electron. and Commun. in Japan*, vol. 57A, pp. 27–35, 1975.
[9] ____, "Basic theory of two-dimensional cyclic codes—Periods of ideals and fundamental theorems," *Electron. and Commun. in Japan*, vol. 59A, pp. 31–38, 1976.
[10] ____, "Basic theory of two-dimensional cyclic codes—Structure of cyclic codes and their dual codes," *Electron. and Commun. in Japan*, vol. 59A, pp. 39–47, 1976.
[11] H. Imai, "Two-dimensional Fire codes," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 796–806, 1973.
[12] ____, "A theory of two-dimensional codes," *Inform. Contr.*, vol. 34, pp. 1–21, 1977.
[13] R. Lidl and H. Neiderreiter, "Finite fields," in *Encyclopedia of Mathematics and its Applications*, vol. 20, Reading, MA: Addison-Wesley, 1983.
[14] T. Nomura, H. Miyakawa, H. Imai, and A. Fukuda, "A theory of two-dimensional linear recurring arrays," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 775–785, 1972.
[15] A. Poli, "Idéaux principaux nilpotents de dimension maximale dans l'algèbre $\mathbb{F}_q[G]$ d'un groupe abelien fini G," *Comm. Alg.*, vol. 12, pp. 391–401, 1984.
[16] ____, "Important algebraic calculations for n-variable polynomial codes," *Disc. Math.*, vol. 56, pp. 255–263, 1985.
[17] A. Poli and M. Ventou, "Codes autoduaux principaux et groupe d'automorphismes de l'algèbre $\mathbb{F}_q[X_1, \cdots, X_n]/(X_1^2 - 1, \cdots, X_n^2 - 1)$, $q = p^r$," *Eur. J. Combin.*, vol. 2, pp. 179–183, 1981.
[18] K. A. Prahbu and N. K. Bose, "Impulse response arrays of discrete-space systems over a finite field," *IEEE Trans. Acoust. Speech and Signal Processing*, vol. ASSP-30, pp. 10–18, 1982.
[19] L. Robbiano, "Introduction to the theory of Gröbner bases," *Queen's Papers*, Kingston, Ontario, 1988.
[20] S. Sakata, General theory of doubly periodic arrays over an arbitrary finite field and its applications, *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 719–730, 1978.
[21] ____, "On determining the independent point set for doubly periodic arrays and encoding two-dimensional cyclic codes and their duals," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 556–565, 1981.
[22] ____, "Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array," *J. Symb. Comput.*, vol. 5, pp. 321–337, 1988.
[23] ____, "Extension of the Berlekamp–Massey algorithm to n dimensions, *Inform. Computat.*, vol. 84, pp. 207–239, 1990.
[24] O. Zariski and P. Samuel, *Commutative Algebra Vol. 2.* Princeton, NJ: Van Nostrand, 1960.

Periodic Complementary Binary Sequences

LEOPOLD BÖMER AND MARKUS ANTWEILER

Abstract —**Two or more sequences are called a set of periodic complementary sequences if the sum of their respective periodic autocorrelation functions is a delta function. In this correspondence properties, existence conditions and recursive construction procedures for sets of periodic complementary binary sequences are given. Relationships to sets of aperiodic complementary binary sequences and to perfect binary arrays, whose two-dimensional periodic autocorrelation function is a delta function, are pointed out. The connections of periodic complementary binary sequences and difference families are given. Sets of periodic complementary binary sequences, which result from computer search, are presented. A diagram showing what is currently known about the existence of periodic complementary binary sequences with $P \leq 12$ sequences of $N \leq 50$ elements is given.**

I. Introduction

A set of binary sequences is called a set of periodic complementary sequences (PCS), if the sum of the *periodic* autocorrelation functions of all sequences is a delta function. If the sum of their *aperiodic* autocorrelation functions is a delta function, the sequences are called a set of aperiodic complementary sequences (ACS). These ACS form a subclass of the PCS and have been well examined. First, in 1960, Golay [1] published properties of ACS. However, Golay's results are limited to ACS with two sequences. ACS with an even number of sequences were examined in 1972 by Tseng and Liu [2]. Whereas ACS are limited to an even number of sequences, PCS may exist for any number of sequences.

A PCS may alternatively be defined by the two-dimensional periodic autocorrelation function (PACF) of a binary array. If the nonzero horizontal shift of the two-dimensional PACF contributes zero, the rows of the array are the sequences of a PCS. Such two-dimensional periodic correlation problems are fundamental in coded aperture imaging [3] and higher-dimensional signal processing applications such as time-frequency-coding [4] or spatial correlation [5].

PCS's can be formed from perfect binary arrays, which are arrays whose two-dimensional PACF is a delta function. Perfect binary arrays were examined in [6], [7]. A number of new perfect binary arrays were constructed for a specified number of ele-

Manuscript received July 5, 1988; revised April 3, 1990.
The authors are with the Institute for Communication Engineers, Technical University of Aachen, D-5100 Aachen, FRG.
IEEE Log Number 9036981.