

A Generalization of the Massey-Ding Algorithm

Joachim Althaler, Arne Dür

Institut für Mathematik, Universität Innsbruck, Technikerstrasse 25, A-6020 Innsbruck, Austria

Received: January 31, 1997; revised version: September 2, 1997

Abstract. The set of all linear recurrence relations satisfied by given sequences of finite length is described by the annihilator ideal of the sequences. The Massey-Ding algorithm to compute a linear recurrence relation of minimal order for several finite sequences of equal length is generalized to compute a minimal Gröbner basis of the annihilator ideal of several finite sequences of generally different lengths.

Keywords: Linear recurrence relation, Shift register synthesis problem, Annihilator ideal, Minimal Gröbner basis.

1 Introduction

Let $s = (s_0, s_1, \dots, s_{n-1})$ be a finite sequence of length n in an arbitrary field K . A *linear recurrence relation* for s

$$s_{L+j} = \sum_{i=0}^{L-1} a_i s_{i+j} \quad \text{for } j = 0, 1, \dots, n-1-L \quad (1)$$

can be described by its *characteristic polynomial*

$$f(X) = X^L - \sum_{i=0}^{L-1} a_i X^i \in K[X].$$

The degree L is called the *order* of the linear recurrence relation. Such recurrence relations can be realized by linear feedback shift registers, and the resulting sequences are employed in various branches of electrical engineering, especially in coding theory and in cryptography. In these applications, the ground field K is a finite field, usually the binary field or some finite extension thereof (see, e.g., [7] or [9]).

A central problem in the theory of linear recurring sequences is the *synthesis problem*:

Given several sequences in K of finite but generally different lengths, find the linear recurrence relation of least order that is satisfied by all the sequences.

In general, the solution of the synthesis problem is not unique. In the case of a single sequence, Massey has described the complete solution, i.e., the set of all solutions of the synthesis problem, in [8] by two polynomials obtained from the Berlekamp-Massey algorithm. A generalization of this algorithm to several sequences of equal length was conjectured by Massey, and Ding [4] proved that Massey's conjectured algorithm yields a particular solution of the synthesis problem. Other algorithms to compute particular solutions of the synthesis problem have been proposed by Feng and Tzeng [6] and by Sakata and Dai [11]. In [5] Feng and Tzeng used a generalized Euclidean algorithm to find the complete solution for multiple sequences of equal length. In [1] the authors described the complete solution by a polynomial ideal called the *annihilator ideal* of the sequences and proposed computing a Gröbner basis of this ideal by first applying the Berlekamp-Massey algorithm to each sequence separately and then using an ideal intersection algorithm.

In the present paper, we generalize the Massey-Ding algorithm (MDA) to obtain a Gröbner basis of the annihilator ideal for several finite sequences of generally different lengths. As the MDA, the Generalized Massey-Ding algorithm (GMDA) iterates along all sequences simultaneously. The GMDA has a more complicated control structure than the MDA but the computational work is not much higher. To explain the idea of the GMDA, we use the ideal-theoretic approach introduced in [1] and briefly recall the necessary notation. Let A be the K -vector space of all formal series

$$a = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} a_{i,j} X^{-i} Y^{-j}$$

where X, Y are indeterminates such that $X^i Y^j = 0$ whenever $i > 0$ or $j > 0$. Then the polynomial ring $K[X, Y]$ operates on the space A by multiplying a polynomial with a power series and omitting terms with positive powers of either indeterminate. Let

$$S := \sum_{j=0}^{n-1} s_j X^{-j} Y^{-(n-1-j)} \in A$$

be the *generating function* of the sequence $s = (s_0, s_1, \dots, s_{n-1})$, and let

$$F := X^L - \sum_{i=0}^{L-1} a_i X^i Y^{L-i}$$

be the homogenization of the characteristic polynomial. Then direct computation shows that the sequence s satisfies the linear recurrence relation (1) if and only if

$$F \cdot S = 0.$$

Thus linear recurrence relations can be studied in terms of their generating functions in the $K[X, Y]$ -module A . For a detailed discussion of the topological duality between polynomials and formal series, we refer to [1] and [10]. Given several sequences $s^{(1)}, s^{(2)}, \dots, s^{(m)}$ with generating functions $S^{(1)}, \dots, S^{(m)}$, the *annihilator ideal* of the sequences is

$$\text{Ann}(s^{(1)}, \dots, s^{(m)}) := \{G \in K[X, Y] \mid G \cdot S^{(1)} = \dots = G \cdot S^{(m)} = 0\}.$$

Then the solution of the synthesis problem is

$$\mathcal{R}(s^{(1)}, \dots, s^{(m)}) := \left\{ G(X, 1) \left| \begin{array}{l} G \text{ homogeneous polynomial in } \text{Ann}(s^{(1)}, \dots, s^{(m)}) \\ \text{of minimal degree that is not a multiple of } Y \end{array} \right. \right\}.$$

Example 1 Let $s^{(1)} := (110)$, $s^{(2)} = (001)$, and $s^{(3)} := (010)$ be three sequences in $K = GF(2)$. Then

$$\text{Ann}(s^{(1)}, s^{(2)}) = \langle X^3, XY + Y^2, Y^3 \rangle \neq \langle X^3, X^2Y, XY^2, Y^3 \rangle = \text{Ann}(s^{(1)}, s^{(2)}, s^{(3)}).$$

However, the linear recurrence relations satisfied by $s^{(1)}, s^{(2)}$ and by $s^{(1)}, s^{(2)}, s^{(3)}$ coincide and are all linear recurrence relations of order at least 3. Thus two sets of finite sequences may have different annihilator ideals but satisfy the same linear recurrence relations. In [1] it was shown that the annihilator ideal describes exactly the linear recurrence relations satisfied by both the sequences and by their initial parts, i.e., the sequences shortened by removal of trailing digits.

The GMDA presented here iterates along a descending chain of ideals

$$K[X, Y] = \mathcal{J}_{-1} \supseteq \mathcal{J}_0 \supseteq \mathcal{J}_1 \supseteq \dots \supseteq \mathcal{J}_{n-2} \supseteq \mathcal{J}_{n-1} = \text{Ann}(s^{(1)}, \dots, s^{(m)})$$

where n denotes the maximum length of the sequences and where all the factors

$$\mathcal{J}_N / Y \mathcal{J}_{N-1}$$

are *principal ideals*. The GMDA starts with the basis $\{1\}$ of the ideal $K[X, Y]$ and computes a generating polynomial of $\mathcal{J}_N \bmod Y \mathcal{J}_{N-1}$ at each step. We prove that the resulting basis is in fact a minimal Gröbner basis of the ideal $\text{Ann}(s^{(1)}, \dots, s^{(m)})$. Then an explicit representation of the complete solution of the synthesis problem can be obtained from the low degree polynomials of the Gröbner basis.

If all sequences have equal length, the GMDA reduces to the MDA and hence the ideal-theoretic interpretation of the GMDA given above sheds new light on the MDA.

2 The Generalized Massey-Ding Algorithm

Let $s^{(1)} = (s_0^{(1)}, s_1^{(1)}, \dots, s_{n_1-1}^{(1)})$, $\dots$, $s^{(m)} = (s_0^{(m)}, s_1^{(m)}, \dots, s_{n_m-1}^{(m)})$ be m finite sequences in the ground field K , and let

$$n := \max(n_1, \dots, n_m)$$

denote the maximum length of the sequences. For $N = -1, 0, 1, \dots, n-1$ and $i = 1, \dots, m$, we consider the initial parts $(s_0^{(i)}, s_1^{(i)}, \dots, s_N^{(i)})$ of the sequences $s^{(i)}$ and their generating functions

$$S_N^{(i)} := \begin{cases} \sum_{j=0}^N s_j^{(i)} X^{-j} Y^{-(N-j)} & \text{if } N \leq n_i - 1 \\ \sum_{j=0}^{n_i-1} s_j^{(i)} X^{-j} Y^{-(n_i-1-j)} & \text{otherwise.} \end{cases}$$

(For $N = -1$, the initial part $(s_0^{(i)}, s_1^{(i)}, \dots, s_N^{(i)})$ is empty and $S_N^{(i)} = 0$). Then, for $N = -1, 0, 1, \dots, n-1$,

$$\mathcal{J}_N := \{G \in K[X, Y] \mid G \cdot S_{N-n+n_i}^{(i)} = 0 \text{ for } i = 1, \dots, m\}$$

is a homogeneous ideal in $K[X, Y]$. In particular, $\mathcal{J}_{-1} = K[X, Y]$ and $\mathcal{J}_{n-1} = \text{Ann}(s^{(1)}, \dots, s^{(m)})$. In general, the ideals $\mathcal{J}_N$ enjoy the following properties.

Lemma 1 For $N = 0, 1, \dots, n-1$,

- (i) $(\mathcal{J}_N : Y) = \mathcal{J}_{N-1}$
(Here $(\mathcal{J}_N : Y) = \{f \in K[X, Y] \mid Yf \in \mathcal{J}_N\}$ is the ideal quotient [2], [3]).
- (ii) $Y\mathcal{J}_{N-1} \subseteq \mathcal{J}_N \subseteq \mathcal{J}_{N-1}$
- (iii) $\mathcal{J}_N/Y\mathcal{J}_{N-1}$ is a principal ideal.

Proof. (i) We have $(\mathcal{J}_N : Y) = \{f \in K[X, Y] \mid Yf \in \mathcal{J}_N\} = \{f \mid (Yf) \cdot S_{N-n+n_i}^{(i)} = 0 \text{ for all } i\} = \{f \mid f \cdot S_{N-1-n+n_i}^{(i)} = 0 \text{ for all } i\} = \mathcal{J}_{N-1}$ because $N \leq n-1$ implies $N-n+n_i \leq n_i-1$ and hence $Y \cdot S_{N-n+n_i}^{(i)} = S_{N-1-n+n_i}^{(i)}$.

(ii) The first inclusion $Y\mathcal{J}_{N-1} \subseteq \mathcal{J}_N$ is an immediate consequence of (i). The second inclusion $\mathcal{J}_N \subseteq \mathcal{J}_{N-1}$ follows from the observation that, for $G \in \mathcal{J}_N$, $G \cdot S_{N-1-n+n_i}^{(i)} = G \cdot (Y \cdot S_{N-n+n_i}^{(i)}) = Y \cdot (G \cdot S_{N-n+n_i}^{(i)}) = 0$ for all i and thus $G \in \mathcal{J}_{N-1}$.

(iii) is a consequence of Lemma 2. □

Looking at the definition of the ideals $\mathcal{J}_N$, one sees that the first time that the term $s_k^{(i)}$ affects the ideal $\mathcal{J}_N$ is for $N = k + n - n_i$. Thus the terms of *shorter* sequences are considered *later* when iterating $N = -1, 0, 1, \dots, n-1$. The reason for our choosing this delayed approach is that although the straightforward definition

$$\mathcal{J}_N := \{G \in K[X, Y] \mid G \cdot S_N^{(i)} = 0 \text{ for } i = 1, \dots, m\}$$

yields a chain of ideals

$$K[X, Y] = \mathcal{J}_{-1} \supseteq \mathcal{J}_0 \supseteq \mathcal{J}_1 \supseteq \dots \supseteq \mathcal{J}_{n-2} \supseteq \mathcal{J}_{n-1} = \text{Ann}(s^{(1)}, \dots, s^{(m)}),$$

some factor ideal $\mathcal{J}_N/Y\mathcal{J}_{N-1}$ may not be principal as the following example illustrates.

Example 2 Let $s^{(1)} := (1011)$ and $s^{(2)} := (111)$ be two sequences over $GF(2)$. Then the ideal

$$\mathcal{J}_3/Y\mathcal{J}_2 = \langle X^3 + Y^3, X^2Y + Y^3, XY^2, Y^4 \rangle / \langle X^2Y + Y^3, XY^3, Y^4 \rangle$$

is generated by the cosets of $X^3 + Y^3$ and XY^2 and thus is not principal.

Definition 1 Let $N \in \{-1, 0, 1, \dots, n-1\}$. Let

$$v_N := \min\{\deg(F) \mid F \in \mathcal{J}_N \text{ homogeneous and not a multiple of } Y\}$$

where $\deg(F)$ denotes the total degree of F . The homogeneous polynomials in $\mathcal{J}_N$ congruent to X^{v_N} mod Y are the minimal polynomials in $\mathcal{J}_N$.

Lemma 2 Let $N \in \{0, 1, \dots, n-1\}$ and let F_N be a minimal polynomial in $\mathcal{J}_N$. Then

$$\mathcal{J}_N = Y\mathcal{J}_{N-1} + K[X, Y]F_N.$$

Hence the factor ideal $\mathcal{J}_N/Y\mathcal{J}_{N-1}$ is generated by the residue class of F_N and thus is a principal ideal.

Proof. By Lemma 1, (ii), $Y\mathcal{J}_{N-1} + K[X, Y]F_N$ is contained in $\mathcal{J}_N$. To prove the opposite inclusion, let G be a homogeneous polynomial in $\mathcal{J}_N$. Then $G \equiv aX^\mu \pmod{Y}$ for some $a \in K$ and $\mu \in \{0, 1, 2, \dots\}$. As F_N is minimal, we can write $G - aX^{\mu - v_N} F_N = YG_1$ where $G_1 \in (\mathcal{J}_N : Y)$. Lemma 1, (i), now implies that $G_1 \in \mathcal{J}_{N-1}$ and hence $G \in Y\mathcal{J}_{N-1} + K[X, Y]F_N$. $\square$

The chain of ideals

$$K[X, Y] = \mathcal{J}_{-1} \supseteq \mathcal{J}_0 \supseteq \mathcal{J}_1 \supseteq \dots \supseteq \mathcal{J}_{n-2} \supseteq \mathcal{J}_{n-1} = \text{Ann}(s^{(1)}, \dots, s^{(m)}),$$

and the relation $\mathcal{J}_N = Y\mathcal{J}_{N-1} + K[X, Y]F_N$ suggest computing an ideal basis of $\text{Ann}(s^{(1)}, \dots, s^{(m)})$ by starting with

$$\mathcal{B}_{-1} := \{1\}$$

and iterating

$$\mathcal{B}_N := \{YF | F \in \mathcal{B}_{N-1}\} \cup \{F_N\}$$

for $N = 0, 1, \dots, n-1$ where F_N is an arbitrary minimal polynomial in $\mathcal{J}_N$. The next theorem shows that, by omitting some of these polynomials, a minimal Gröbner basis can be obtained. Here we use the following notation from Gröbner basis theory (see, e.g., [3] or [2]):

For $g \in K[X, Y]$, $g \neq 0$, let $lt(g)$ denote the leading term of g with respect to the *graded-lexicographic* order where $X > Y$, and let $lc(g)$ denote the leading coefficient of g . A subset $\mathcal{B}$ of an ideal $\mathcal{I}$ of $K[X, Y]$ is called a *Gröbner basis* of $\mathcal{I}$ if $\mathcal{B}$ is finite, $0 \notin \mathcal{B}$, and

$$\langle lt(g); g \in \mathcal{B} \rangle = \langle lt(f); f \in \mathcal{I}, f \neq 0 \rangle.$$

A Gröbner basis $\mathcal{B}$ is *minimal* if, for all $g \in \mathcal{B}$, $lc(g) = 1$ and

$$lt(g) \notin \langle lt(f); f \in \mathcal{B}, f \neq g \rangle.$$

A minimal Gröbner basis $\mathcal{B}$ is *reduced* if, for all $g \in \mathcal{B}$, no term of $g - lt(g)$ lies in $\langle lt(f); f \in \mathcal{B}, f \neq g \rangle$. It can be shown that every Gröbner basis for $\mathcal{I}$ is a basis of the ideal $\mathcal{I}$, and that every ideal $\mathcal{I}$ has a unique reduced Gröbner basis.

Theorem 1 Define $\Omega_{-1} := \emptyset$ and, for $N = 0, 1, \dots, n-1$,

$$\Omega_N := \begin{cases} \Omega_{N-1} & \text{if } v_N = v_{N-1} \\ \Omega_{N-1} \cup \{N-1\} & \text{if } v_N > v_{N-1}. \end{cases}$$

Then, for $N \in \{-1, 0, 1, \dots, n-1\}$, the set

$$\Omega'_N := \Omega_N \cup \{N\}$$

is a subset of $\{-1, 0, 1, \dots, N\}$, the numbers $v_j, j \in \Omega'_N$, are strictly increasing, and $\{Y^{N-j}F_j | j \in \Omega'_N\}$ is a minimal Gröbner basis of $\mathcal{J}_N$.

Proof. As $v_{-1} \leq v_0 \leq \dots \leq v_{n-1}$, the definition of Ω_N implies that $\Omega'_N \subseteq \{-1, 0, 1, \dots, N\}$ and that $v_j, j \in \Omega'_N$, are strictly increasing. For $j \in \Omega'_N$, $Y^{N-j}F_j \in Y^{N-j}\mathcal{J}_j \subseteq \mathcal{J}_N$ by Lemma 1, (ii). To prove that $\{Y^{N-j}F_j | j \in \Omega'_N\}$ is a minimal Gröbner basis of $\mathcal{J}_N$, we use induction on N . For $N = -1$, $\{1\}$ clearly is a minimal Gröbner basis of $K[X, Y]$. Now let $N \in \{0, 1, \dots, n-1\}$. To show that $\{Y^{N-j}F_j | j \in \Omega'_N\}$ is a Gröbner basis of $\mathcal{J}_N$, let G be an arbitrary nonzero homogeneous polynomial in $\mathcal{J}_N$. If $lt(G) = X^k$ for some $k \in \{0, 1, 2, \dots\}$, then the

definition of v_N implies that $k \geq v_N$, and hence $lt(G)$ is a multiple of $X^{v_N} = lt(F_N)$. Therefore we may assume that $G = YH$ for some $H \in K[X, Y]$. Then $H \in (\mathcal{J}_N : Y) = \mathcal{J}_{N-1}$ and, by the induction hypothesis, $lt(H)$ is a multiple of $Y^{N-1-j}lt(F_j)$ for some $j \in \Omega'_{N-1}$. Consequently, $lt(G) = Ylt(H)$ is a multiple of $Y^{N-l}lt(F_l)$ where $l \in \Omega'_N$ is defined by $l := j$ if $j \in \Omega_N$ and $l := N$ otherwise. Observe that $j \notin \Omega_N$ implies $j = N - 1$ and $v_N = v_{N-1}$, and hence $lt(F_{N-1}) = lt(F_N)$.

Finally, we prove that the Gröbner basis $\{Y^{N-j}F_j | j \in \Omega'_N\}$ is minimal. Clearly $lc(Y^{N-j}F_j) = 1$ for all j , and thus it remains to prove that

$$lt(Y^{N-j}F_j) \notin \langle lt(Y^{N-l}F_l); l \in \Omega'_N, l \neq j \rangle.$$

Suppose that $lt(Y^{N-j}F_j) = X^{v_j}Y^{N-j}$ is a multiple of $lt(Y^{N-l}F_l) = X^{v_l}Y^{N-l}$ for some $j, l \in \Omega'_N$ with $j \neq l$. Then both $v_j \geq v_l$ and $N - j \geq N - l$. But $j \leq l$ implies $v_j \leq v_l$ and hence $v_j = v_l$, which is a contradiction. $\square$

Corollary 1 *The complete solution of the synthesis problem is given by*

$$\left\{ F_{n-1}(X, 1) + \sum_{j \in \Omega_{n-1}} g_j(X) F_j(X, 1) \mid \deg(g_j(X)) \leq v_{n-1} - v_j - (n - 1 - j) \right\}.$$

To compute a minimal Gröbner basis of $\text{Ann}(s^{(1)}, \dots, s^{(m)})$ by Theorem 1, there remains the nontrivial task of computing a minimal polynomial in $\mathcal{J}_N$ for each $N \in \Omega'_{n-1}$. We will do this iteratively by generalizing the Massey-Ding algorithm [4] to the case of finite sequences of generally different lengths. To this end we recall the notion of “discrepancy”.

Lemma 3 *For $N \in \{-1, 0, 1, \dots, n - 2\}$ and $i \in \{1, \dots, m\}$, the operation of the polynomial*

$$F_N = \sum_{j=0}^{v_N} F_N^{(j)} X^{v_N-j} Y^j \in \mathcal{J}_N$$

on the generating function

$$S_{N+1-n+n_i}^{(i)} = \sum_{k=0}^{N+1-n+n_i} s_k^{(i)} X^{-k} Y^{-(N+1-n+n_i-k)}$$

is given by

$$F_N \cdot S_{N+1-n+n_i}^{(i)} = d_N^{(i)} X^{-(N+1-n+n_i-v_N)}$$

where

$$d_N^{(i)} := \begin{cases} \sum_{j=0}^{v_N} F_N^{(j)} s_{N+1-n+n_i-j}^{(i)} & \text{if } v_N \leq N+1-n+n_i \\ 0 & \text{otherwise.} \end{cases}$$

Remark: The vector $d_N := (d_N^{(1)}, d_N^{(2)}, \dots, d_N^{(m)})$ is the N -th discrepancy.

Proof: As $N \leq n - 2$, $Y \cdot (F_N \cdot S_{N+1-n+n_i}^{(i)}) = F_N \cdot (Y \cdot S_{N+1-n+n_i}^{(i)}) = F_N \cdot S_{N-n+n_i}^{(i)} = 0$. Hence $F_N \cdot S_{N+1-n+n_i}^{(i)}$ is a scalar multiple of $X^{-(N+1-n+n_i-v_N)}$ and $F_N \cdot S_{N+1-n+n_i}^{(i)} = \sum_{j=0}^{v_N} \sum_{k=v_N-j}^{N+1-n+n_i-j} F_N^{(j)} s_k^{(i)} X^{-(k-v_N+j)} Y^{-(N+1-n+n_i-j-k)} = (\sum_{j=0}^{v_N} F_N^{(j)} s_{N+1-n+n_i-j}^{(i)}) X^{-(N+1-n+n_i-v_N)}$. $\square$

Lemma 4 Let $N \in \{-1, 0, 1, \dots, n-1\}$. Then there exists a minimal polynomial in $\mathcal{J}_{N+1}$ of the form

$$X^E F_N - \sum_{j \in \Omega_N} a_j X^{E-(N-j+v_j-v_N)} Y^{N-j} F_j, \quad (2)$$

where $E \geq 0$ and $a_j \in K$, such that, for all j with $a_j \neq 0$, $E \geq N-j+v_j-v_N$. Conversely, if F_{N+1} is an arbitrary polynomial of this form, then F_{N+1} is contained in $\mathcal{J}_{N+1}$ if and only if

$$E \geq N+2-v_N-n+n_i \quad \text{or} \quad d_N^{(i)} = \sum_{j \in \Omega_N} a_j d_j^{(i)} \quad \text{for } i = 1, \dots, m.$$

Furthermore, F_{N+1} is minimal if and only if E is minimal.

Proof. Let F_{N+1} be any minimal polynomial in $\mathcal{J}_{N+1}$. As $F_{N+1} \in \mathcal{J}_N$ and $\{Y^{N-j} F_j | j \in \Omega_N\}$ is an ideal basis of $\mathcal{J}_N$, we can write

$$F_{N+1} = \sum_{j \in \Omega_N} Q_j Y^{N-j} F_j$$

where the homogeneous polynomials $Q_j \in K[X, Y]$ are either zero or have total degree $v_{N+1} - v_j - N + j$. Since $Y \mathcal{J}_N \subseteq \mathcal{J}_{N+1}$, we may reduce F_{N+1} modulo $Y \mathcal{J}_N$ to obtain $Q_j = b_j X^{E_j}$ with $b_j \in K$. Then the leading monomial of F_{N+1} is $X^{v_{N+1}} = b_N X^{E_N} X^{v_N}$ which implies $b_N = 1$ and $E_N = v_{N+1} - v_N \geq 0$. Hence

$$F_{N+1} = X^{E_N} F_N + \sum_{j \in \Omega_N} b_j X^{E_j} Y^{N-j} F_j$$

where, for all j with $b_j \neq 0$, $0 \leq E_j = E_N - (N-j+v_j-v_N)$. Thus F_{N+1} has the form (2). Conversely, let F_{N+1} be an arbitrary polynomial of this form. Then F_{N+1} is a monic homogeneous polynomial with leading term X^{E+v_N} . Hence F_{N+1} is minimal in $\mathcal{J}_{N+1}$ if and only if E is minimal with $F_{N+1} \in \mathcal{J}_{N+1}$. By definition, $F_{N+1} \in \mathcal{J}_{N+1}$ if and only if $F_{N+1} \cdot S_{N+1-n+n_i}^{(i)} = 0$ for $i = 1, \dots, m$. But

$$\begin{aligned} F_{N+1} \cdot S_{N+1-n+n_i}^{(i)} &= X^E \cdot (F_N \cdot S_{N+1-n+n_i}^{(i)}) - \sum_j a_j X^{E-(N-j+v_j-v_N)} \\ &\quad \cdot (F_j \cdot (Y^{N-j} \cdot S_{N+1-n+n_i}^{(i)})) \\ &= X^E \cdot (F_N \cdot S_{N+1-n+n_i}^{(i)}) - \sum_j a_j X^{E-(N-j+v_j-v_N)} \cdot (F_j \cdot S_{j+1-n+n_i}^{(i)}) \\ &= d_N^{(i)} X^{E-(N+1-n+n_i-v_N)} - \sum_j a_j d_j^{(i)} X^{E-(N+1-n+n_i-v_N)} \\ &= (d_N^{(i)} - \sum_j a_j d_j^{(i)}) X^{E-(N+1-n+n_i-v_N)} \end{aligned}$$

is 0 if and only if $E > N+1-v_N-n+n_i$ or $d_N^{(i)} = \sum_j a_j d_j^{(i)}$. $\square$

Lemma 4 suggests computing a minimal polynomial F_{N+1} in $\mathcal{J}_{N+1}$ by starting with (2) and searching for the smallest $E \geq 0$ such that

$$E \geq N+2-v_N-n+n_i \quad \text{or} \quad d_N^{(i)} = \sum_{j \in \Omega_N} a_j d_j^{(i)} \quad \text{for } i = 1, \dots, m.$$

To analyze these conditions we introduce some definitions. Hereafter we assume with no loss of generality that the sequences $s^{(1)}, s^{(2)}, \dots, s^{(m)}$ are ordered by length, i.e., $n_1 \geq n_2 \geq \dots \geq n_m$.

Definition 2 Let

$$\Delta := \{0\} \cup \{i \in \{1, \dots, m-1\} | n_i > n_{i+1}\} \cup \{m\}$$

be the set of length changes and, for $\delta \in \Delta \setminus \{m\}$, let δ^+ denote the successor of δ in Δ . For $\delta \in \Delta$ and $N \in \{-1, 0, 1, \dots, n-1\}$, let

$$d_N^{[\delta]} := (d_N^{(1)}, d_N^{(2)}, \dots, d_N^{(\delta)}) \in K^\delta$$

denote the initial parts of the discrepancies. For $J \subseteq \{-1, 0, 1, \dots, n-1\}$, let $K^J = \{(a_j)_{j \in J} \mid a_j \in K \text{ for all } j \in J\}$ and, for $a \in K^J$, define

$$\mu_N(a) := \begin{cases} \max\{N - j + v_j - v_N \mid j \in J \text{ with } a_j \neq 0\} & \text{if } a \neq 0 \\ -\infty & \text{if } a = 0. \end{cases}$$

We can now state our main result.

Theorem 2 (1) Let $N \in \{-1, 0, 1, \dots, n-1\}$. Then, for each $\delta \in \Delta$, there exists a subset $\Psi_N^{(\delta)}$ of Ω_N such that

- (i) $\{d_j^{[\delta]} \mid j \in \Psi_N^{(\delta)}\}$ is a K -basis of $\sum_{j \in \Omega_N} K d_j^{[\delta]}$ and,
- (ii) for all $a \in K^{\Omega_N}$, $\mu_N(a) \geq \mu_N(b)$ where $b \in K^{\Psi_N^{(\delta)}}$ is defined by

$$\sum_{j \in \Omega_N} a_j d_j^{[\delta]} = \sum_{j \in \Psi_N^{(\delta)}} b_j d_j^{[\delta]}.$$

In particular, $\Psi_N^{(0)} = \emptyset$. We call the K -basis $\{d_j^{[\delta]} \mid j \in \Psi_N^{(\delta)}\}$ a minimal basis. For $\varepsilon \in \Delta$, let

$$\eta_\varepsilon := \begin{cases} \max(0, N + 2 - v_N - n + n_{\varepsilon^+}) & \text{if } \varepsilon < m \\ 0 & \text{if } \varepsilon = m \end{cases}$$

and

$$\mu_\varepsilon := \begin{cases} \max(0, \mu_N(c)) & \text{if } d_N^{[\varepsilon]} = \sum_{j \in \Psi_N^{(0)}} c_j d_j^{[\varepsilon]} \\ N + 2 - v_N & \text{otherwise.} \end{cases}$$

Let τ be the smallest ε such that $\eta_\varepsilon \leq \mu_\varepsilon$, let σ denote the predecessor of τ in Δ , and let $D := \min\{\eta_\sigma, \mu_\tau\}$. Then

$$v_{N+1} = v_N + D$$

and

$$F_{N+1} := X^D F_N - \sum_{j \in \Psi_N^{(\rho)}} c_j X^{D - (N - j + v_j - v_N)} Y^{N-j} F_j \quad \text{if } v_{N+1} < N + 2,$$

where

$$\rho := \begin{cases} \sigma & \text{if } \eta_\sigma \leq \mu_\tau \\ \tau & \text{otherwise} \end{cases} \quad \text{and} \quad d_N^{[\rho]} = \sum_{j \in \Psi_N^{(\rho)}} c_j d_j^{[\rho]},$$

or

$$F_{N+1} := X^{N+2} \quad \text{if } v_{N+1} = N + 2,$$

is a minimal polynomial in $\mathcal{J}_{N+1}$.

(2) The subsets $\Psi_N^{(\delta)}$ can be computed inductively by $\Psi_{-1}^{(\delta)} := \emptyset$ and, for $N \in \{-1, 0, 1, \dots, n-2\}$, as follows:

- (a) if $D_N = 0$ or $d_N^{[\delta]} = \sum_{j \in \Psi_N^{(0)}} c_j d_j^{[\delta]}$ with $\mu_N(c) \leq 0$, then

$$\Psi_{N+1}^{(\delta)} := \Psi_N^{(\delta)}.$$

(b) if $D_N > 0$ and $d_N^{[\delta]} = \sum_{j \in \Psi_N^{(\delta)}} c_j d_j^{[\delta]}$ with $\mu_N(c) > 0$, then

$$\Psi_{N+1}^{(\delta)} := (\Psi_N^{(\delta)} \setminus \{M_\delta\}) \cup \{N\}.$$

where M_δ is the smallest j with $c_j \neq 0$ and $N - j + v_j - v_N = \mu_N(c)$.

(c) if $D_N > 0$ or $d_N^{[\delta]} \notin \sum_{j \in \Psi_N^{(\delta)}} K d_j^{[\delta]}$, then

$$\Psi_{N+1}^{(\delta)} := \Psi_N^{(\delta)} \cup \{N\}.$$

Proof. (1) The existence of the sets $\Psi_N^{(\delta)}$ with properties (i) and (ii) will be proved in (2) below by induction on N . Here we prove the other results. As $n_1 \geq n_2 \geq \dots \geq n_m$, the sequence $(\eta_\varepsilon)_{\varepsilon \in \Delta}$ is monotone decreasing. We claim that the sequence $(\mu_\varepsilon)_{\varepsilon \in \Delta}$ is monotone increasing. To see this, observe that $v_j \leq j + 1$ for all j , hence $\mu_N(c) \leq N + 1 - v_N$ for all c , and $\mu_\varepsilon \leq N + 1 - v_N$ if $d_N^{[\varepsilon]} \in \sum_{j \in \Psi_N^{(\varepsilon)}} K d_j^{[\varepsilon]}$. Moreover, for $\gamma, \varepsilon \in \Delta$ with $\gamma < \varepsilon$ and $d_N^{[\varepsilon]} \in \sum_{j \in \Psi_N^{(\varepsilon)}} K d_j^{[\varepsilon]}$, the basis representation $d_N^{[\varepsilon]} = \sum_{j \in \Psi_N^{(\varepsilon)}} c_j d_j^{[\varepsilon]}$ yields the representation $d_N^{[\gamma]} \in \sum_{j \in \Psi_N^{(\varepsilon)}} c_j d_j^{[\gamma]}$ and, by property (ii), $\mu_\gamma \leq \mu_\varepsilon$ which settles the claim. Since $\eta_0 = N + 2 - v_N > 0 = \mu_0$ and $\eta_m = 0 \leq \mu_m$, the number τ promised in the theorem exists and

$$0 \leq D = \min \{ \max(\eta_\varepsilon, \mu_\varepsilon) \mid \varepsilon \in \Delta \} \leq N + 2 - v_N$$

because $(\eta_\varepsilon)_{\varepsilon \in \Delta}$ is monotone decreasing and $(\mu_\varepsilon)_{\varepsilon \in \Delta}$ is monotone increasing. We next prove that $v_{N+1} = v_N + D$. By Lemma 4, there exists a minimal polynomial in $\mathcal{J}_{N+1}$ of the form

$$X^E F_N - \sum_{j \in \Omega_N} a_j X^{E - (N - j + v_j - v_N)} Y^{N-j} F_j,$$

where $E \geq 0$ and $a_j \in K$, such that, for all j with $a_j \neq 0$, $E \geq N - j + v_j - v_N$. As $n_1 \geq n_2 \geq \dots \geq n_m$, there is a unique $\gamma \in \{0, 1, \dots, m\}$ such that

$$\{i \in \{1, 2, \dots, m\} \mid E < N + 2 - v_N - n + n_i\} = \{1, 2, \dots, \gamma\}.$$

Clearly $\gamma \in \Delta$ and $E \geq \eta_\gamma$. By Lemma 4, $d_N^{[\gamma]} = \sum_{j \in \Omega_N} a_j d_j^{[\gamma]}$. Hence there exists a basis representation $d_N^{[\gamma]} = \sum_{j \in \Psi_N^{(\gamma)}} c_j d_j^{[\gamma]}$ with $\mu_N(a) \leq \mu_N(c)$. Consequently, $E \geq \mu_N(c)$ and $E \geq \mu_\gamma$. Since $D = \min \{ \max(\eta_\varepsilon, \mu_\varepsilon) \mid \varepsilon \in \Delta \}$, we conclude that $E \geq D$ and $v_{N+1} = v_N + E \geq v_N + D$. To show that $v_{N+1} = v_N + D$, observe first that

$$D = \max \{ \eta_\rho, \mu_\rho \}.$$

If $D = N + 2 - v_N$, then X^{N+2} is a polynomial in $\mathcal{J}_{N+1}$ of degree $v_N + D$ and hence minimal. Otherwise $\mu_\rho < N + 2 - v_N$, and hence there exists a representation $d_N^{[\rho]} = \sum_{j \in \Psi_N^{(\rho)}} c_j d_j^{[\rho]}$. Then Lemma 4 implies that the polynomial

$$X^D F_N - \sum_{j \in \Psi_N^{(\rho)}} c_j X^{D - (N - j + v_j - v_N)} Y^{N-j} F_j$$

is contained in $\mathcal{J}_{N+1}$, has degree $v_N + D$, and thus is minimal.

(2) For $N = -1$, we have $\Psi_N^{(\delta)} = \emptyset = \Omega_N$ and all assertions are evident. Thus let $N \in \{-1, 0, 1, \dots, n-2\}$. We first prove that $\Psi_{N+1}^{(\delta)} \subseteq \Omega_{N+1}$. By the induction hypothesis, $\Psi_N^{(\delta)} \subseteq \Omega_N$. As $v_{N+1} = v_N + D_N$,

$$\Omega_{N+1} = \begin{cases} \Omega_N & \text{if } D_N = 0 \\ \Omega_N \cup \{N\} & \text{if } D_N > 0. \end{cases}$$

Hence, in case (a), $\Psi_{N+1}^{(\delta)} = \Psi_N^{(\delta)} \subseteq \Omega_N \subseteq \Omega_{N+1}$, whereas in case (b) and (c), $\Psi_{N+1}^{(\delta)} \subseteq \Psi_N^{(\delta)} \cup \{N\} \subseteq \Omega_N \cup \{N\} = \Omega_{N+1}$. Property (i) follows from the construction of $\Psi_{N+1}^{(\delta)}$. To prove property (ii), we show that

$$\sum_{j \in \Omega_{N+1}} a_j d_j^{[\delta]} = \sum_{j \in \Psi_{N+1}^{(\delta)}} b_j d_j^{[\delta]}$$

implies $\mu_{N+1}(a) \geq \mu_{N+1}(b)$. If $D_N = 0$, then $\Omega_{N+1} = \Omega_N$ and $\Psi_{N+1}^{(\delta)} = \Psi_N^{(\delta)}$, hence $\mu_N(a) \geq \mu_N(b)$ by the induction hypothesis, and $\mu_{N+1}(a) \geq \mu_{N+1}(b)$ by the definition of μ_N . Therefore, we may assume that $D_N > 0$. Then $\Omega_{N+1} = \Omega_N \cup \{N\}$. Now define $a' \in K^{\Omega_N}$ by $a'_j := a_j$ for $j \in \Omega_N$.

In case (a), $\mu_{N+1}(c) = \mu_N(c) + 1 + v_N - v_{N+1} \leq 1 + v_N - v_{N+1}$ and

$$\sum_{j \in \Omega_N} a'_j d_j^{[\delta]} = \sum_{j \in \Psi_{N+1}^{(\delta)}} b_j d_j^{[\delta]} - a_N d_N^{[\delta]} = \sum_{j \in \Psi_N^{(\delta)}} b_j d_j^{[\delta]} - a_N \sum_{j \in \Psi_N^{(\delta)}} c_j d_j^{[\delta]} = \sum_{j \in \Psi_N^{(\delta)}} b'_j d_j^{[\delta]}$$

where $b'_j := b_j - a_N c_j$ for $j \in \Psi_N^{(\delta)}$. By the induction hypothesis, $\mu_N(a') \geq \mu_N(b')$, hence $\mu_{N+1}(a') \geq \mu_{N+1}(b')$. If $a_N = 0$, then $\mu_{N+1}(a) = \mu_{N+1}(a') \geq \mu_{N+1}(b) = \mu_{N+1}(b)$. If $a_N \neq 0$, then

$$\mu_{N+1}(a) = \max(\mu_{N+1}(a'), 1 + v_N - v_{N+1}) \geq \max(\mu_{N+1}(b'), \mu_{N+1}(c)) \geq \mu_{N+1}(b)$$

where in the last inequality we have used the fact that, for each $j \in \Psi_N^{(\delta)}$ with $b_j \neq 0$, $b'_j \neq 0$ or $c_j \neq 0$. In case (b), $\mu_{N+1}(c) = \mu_N(c) + 1 + v_N - v_{N+1} > 1 + v_N - v_{N+1}$ and

$$\sum_{j \in \Omega_N} a'_j d_j^{[\delta]} = \sum_{j \in \Psi_{N+1}^{(\delta)}} b_j d_j^{[\delta]} - a_N d_N^{[\delta]} = \sum_{j \in \Psi_N^{(\delta)} \setminus \{M_\delta\}} b_j d_j^{[\delta]} + (b_N - a_N) \sum_{j \in \Psi_N^{(\delta)}} c_j d_j^{[\delta]} = \sum_{j \in \Psi_N^{(\delta)}} b'_j d_j^{[\delta]}$$

where $b'_{M_\delta} := (b_N - a_N) c_{M_\delta}$ and, for $j \in \Psi_N^{(\delta)} \setminus \{M_\delta\}$, $b'_j := b_j + (b_N - a_N) c_j$. By the induction hypothesis, $\mu_N(a') \geq \mu_N(b')$, hence $\mu_{N+1}(a') \geq \mu_{N+1}(b')$. If $a_N = b_N = 0$, then $\mu_{N+1}(a) = \mu_{N+1}(a') \geq \mu_{N+1}(b') = \mu_{N+1}(b)$. If $a_N = b_N \neq 0$, then

$$\mu_{N+1}(a) = \max(\mu_{N+1}(a'), 1 + v_N - v_{N+1}) \geq \max(\mu_{N+1}(b'), 1 + v_N - v_{N+1}) = \mu_{N+1}(b).$$

If $a_N \neq b_N$, then $b'_{M_\delta} \neq 0$, hence $\mu_{N+1}(b') \geq \mu_{N+1}(c)$ and

$$\mu_{N+1}(a) \geq \mu_{N+1}(a') \geq \mu_{N+1}(b') \geq \max(\mu_{N+1}(b'), \mu_{N+1}(c)) \geq \mu_{N+1}(b)$$

because $\mu_{N+1}(c) > 1 + v_N - v_{N+1}$ and, for $j \in \Psi_{N+1}^{(\delta)} \setminus \{N\}$, $b_j \neq 0$ implies $b'_j \neq 0$ or $c_j \neq 0$. Finally, in case (c),

$$\sum_{j \in \Omega_N} a'_j d_j^{[\delta]} = \sum_{j \in \Psi_N^{(\delta)}} b_j d_j^{[\delta]} + (b_N - a_N) d_N^{[\delta]} = \sum_{j \in \Psi_N^{(\delta)}} b'_j d_j^{[\delta]}$$

where $b'_j := b_j$ for $j \in \Psi_N^{(\delta)}$. By the induction hypothesis, $\mu_N(a') \geq \mu_N(b')$, hence $\mu_{N+1}(a') \geq \mu_{N+1}(b')$. As $a_N = b_N$, we conclude that $\mu_{N+1}(a) \geq \mu_{N+1}(b)$. $\square$

Combining Theorem 1 and 2, we obtain the following iterative algorithm formulated in the notation of Definition 2. In the algorithm, variables with * are used for temporary storage.

Algorithm 1 (*Generalized Massey-Ding Algorithm, GMDA*)

1) Initialize $N := -1$, $v_N := 0$, $F_N := 1$, $\Omega := \emptyset$, and $\Psi^{(\delta)} := \emptyset$ for all $\delta \in \Delta \setminus \{0\}$.

2) If $N = n - 1$, stop. Otherwise compute $d_N := (d_N^{(1)}, \dots, d_N^{(m)})$ where

$$d_N^{(i)} := \begin{cases} \sum_{j=0}^{v_N} F_N^{(j)} s_{N+1-n+n_i-j}^{(i)} & \text{if } v_N \leq N + 1 - n + n_i \\ 0 & \text{otherwise} \end{cases}$$

and

$$F_N := \sum_{j=0}^{v_N} F_N^{(j)} X^{v_N-j} Y^j.$$

3) Initialize $\tau := 0^+$, $\text{Search} := \text{true}$, $\eta^* := N + 2 - v_N$, and $(c_j) := (0)$.

4) a) Solve the linear system $d_N^{[\tau]} = \sum_{j \in \Psi^{(\tau)}} a_j d_j^{[\tau]}$ for (a_j) .

If no solution exists put

$D := \eta^*$ if Search is true, $\Psi_*^{(\delta)} := \Psi^{(\delta)} \cup \{N\}$ for all $\delta \geq \tau$, and go to 5).

b) Compute $\mu := \max(\{0\} \cup \{N - j + v_j - v_N | a_j \neq 0\})$ and put

$$\Psi_*^{(\tau)} := \begin{cases} \Psi^{(\tau)} & \text{if } \mu = 0 \\ (\Psi^{(\tau)} \setminus \{M_\tau\}) \cup \{N\} & \text{otherwise} \end{cases}$$

where M_τ is the smallest index for which the maximum is reached.

c) If Search is false, go to g).

d) Compute $\eta := \begin{cases} \max(0, N + 2 - v_N - n + n_\tau) & \text{if } \tau < m \\ 0 & \text{otherwise.} \end{cases}$

If $\eta > \mu$, go to g).

e) Set $\text{Search} := \text{false}$ and $D := \begin{cases} \eta^* & \text{if } \eta^* \leq \mu \\ \mu & \text{otherwise.} \end{cases}$

f) If $\eta^* > \mu$, put $(c_j) := (a_j)$.

g) If $\tau \neq m$, set $\tau := \tau^+$, $\eta^* := \eta$ and return to 4).

5) Set $v_{N+1} := v_N + D$ and

$$F_{N+1} := \begin{cases} X^D F_N - \sum_j c_j X^{D-(N-j+v_j-v_N)} Y^{N-j} F_j & \text{if } D < N + 2 - v_N \\ X^{N+2} & \text{otherwise.} \end{cases}$$

6) If $D > 0$, put $\Omega := \Omega \cup \{N\}$ and $\Psi^{(\delta)} := \Psi_*^{(\delta)}$ for all $\delta \in \Delta \setminus \{0\}$.

7) Set $N := N + 1$ and return to 2).

When the GMDA stops, the set $\{Y^{n-1-N} F_N | N \in \Omega \cup \{n-1\}\}$ is a minimal Gröbner basis of $\text{Ann}(s^{(1)}, \dots, s^{(m)})$. We next analyze the complexity of this algorithm. The GMDA consists of two loops, an outer loop 2)–7) for $N = -1, 0, \dots, n-2$ and an inner loop 4) for $\tau \in \Delta \setminus \{0\}$. Note that only the polynomials F_N and the discrepancies d_N with $N \in \Omega$ have to be stored during the execution of the algorithm. The boolean variable Search indicates whether τ of Theorem 2, the smallest ε such that $\eta_\varepsilon \leq \mu_\varepsilon$, has already been found.

If all sequences $s^{(1)}, \dots, s^{(m)}$ have equal length, then the GMDA reduces to the original Massey-Ding Algorithm (MDA) [4]: As $\Delta \setminus \{0\} = \{m\}$, there is only one minimal basis $\{d_j | j \in \Psi^{(m)}\}$ for the discrepancies, and the formula in 2) for the discrepancies simplifies to $d_N^{(i)} = \sum_{j=0}^{v_N} F_N^{(j)} s_{N+1-j}^{(i)}$. Furthermore, the inner loop 4) is traversed only once, with $\tau = m$. If the linear system in 4)a) has no solution, then $D = N + 2 - v_N$ and $F_{N+1} = X^{N+2}$. Otherwise, $D = \mu < N + 2 - v_N$ and F_{N+1} is computed from the solution of the linear system.

In the case of sequences of different lengths, however, Algorithm 1 yields several minimal bases $\{d_j^{(\delta)} \mid j \in \Psi_N^{(\delta)}\}$. The following example shows that $\Psi_N^{(\gamma)}$ is not always a subset of $\Psi_N^{(\varepsilon)}$ for $\gamma < \varepsilon$ (We could not find a smaller example). Therefore, the GMDA has slightly higher storage requirements than the MDA. In 4)a), a linear system with linearly independent columns of length τ has to be solved, e.g., by Gaussian elimination. In the following example, $\tau = 1$ or $\tau = 3$. In general, τ is upper bounded by m , the number of sequences, independently of the lengths of the sequences. Moreover, if no solution of the linear system for some τ exists, no linear system for higher values of τ has to be solved. Consequently, for m small compared to n , the computational work of the GMDA is dominated by the computation of the discrepancy in 2) and by the computation of the new minimal polynomial in 5).

Example 3 Let $s^{(1)} := (3, 4, 3, 4, -4, 1, 2, -2, 0, 0, -3, 5, 4, -3)$, $s^{(2)} := (-5, 5, 4, 1, -5, 1, 1, 3, -1, 4, -1, 1)$, $s^{(3)} := (3, 4, -4, 0, 1, -3, -1, -1, 0, -4, 0, -1)$ be three sequences over the ground field $GF(11)$. Then $n = n_1 = 14$, $n_2 = n_3 = 12$, $\Delta = \{0, 1, 3\}$, and Algorithm 1 proceeds as follows.

N	v_N	Ω_N	$\Psi_N^{(1)}$	$\Psi_N^{(3)}$	d_N
-1	0	$\emptyset$	$\emptyset$	$\emptyset$	$(3, 0, 0)$
0	1	$\{-1\}$	$\{-1\}$	$\{-1\}$	$(4, 0, 0)$
1	1	$\{-1\}$	$\{-1\}$	$\{-1\}$	$(5, 0, 0)$
2	2	$\{-1, 1\}$	$\{1\}$	$\{1\}$	$(-3, 0, 0)$
3	2	$\{-1, 1\}$	$\{1\}$	$\{1\}$	$(4, -2, 4)$
4	3	$\{-1, 1, 3\}$	$\{3\}$	$\{1, 3\}$	$(-3, 5, -4)$
5	4	$\{-1, 1, 3, 4\}$	$\{3\}$	$\{1, 3, 4\}$	$(-4, -4, -3)$
6	5	$\{-1, 1, 3, 4, 5\}$	$\{3\}$	$\{3, 4, 5\}$	$(-4, 5, 0)$
7	5	$\{-1, 1, 3, 4, 5\}$	$\{3\}$	$\{3, 4, 5\}$	$(5, 5, -4)$
8	6	$\{-1, 1, 3, 4, 5, 7\}$	$\{7\}$	$\{4, 5, 7\}$	$(0, 4, 3)$
9	7	$\{-1, 1, 3, 4, 5, 7, 8\}$	$\{7\}$	$\{5, 7, 8\}$	$(3, -5, -5)$
10	8	$\{-1, 1, 3, 4, 5, 7, 8, 9\}$	$\{7\}$	$\{7, 8, 9\}$	$(2, -5, 0)$
11	8	$\{-1, 1, 3, 4, 5, 7, 8, 9\}$	$\{7\}$	$\{7, 8, 9\}$	$(0, 4, 0)$
12	9	$\{-1, 1, 3, 4, 5, 7, 8, 9, 11\}$	$\{7\}$	$\{8, 9, 11\}$	$(2, 5, 4)$
13	10	$\{-1, 1, 3, 4, 5, 7, 8, 9, 11, 12\}$	$\{12\}$	$\{8, 11, 12\}$	-

The minimal polynomials in $\mathcal{J}_N$ are $F_{-1} = 1$, $F_0 = X$, $F_1 = X - 5Y$, $F_2 = X^2 - 5XY + 2Y^2$, $F_3 = X^2 - Y^2$, $F_4 = X^3 - 4XY^2 + 4Y^3$, $F_5 = X^4 - 2X^3Y - 4X^2Y^2 - 5XY^3$, $F_6 = X^5 - 2X^4Y - 3X^3Y^2 - 5X^2Y^3 - XY^4$, $F_7 = X^5 - 4X^4Y + 3X^3Y^2 - 2X^2Y^3 + XY^4 + 2Y^5$, $F_8 = X^6 - 4X^5Y + 3X^3Y^3 - 3X^2Y^4 - XY^5 + Y^6$, $F_9 = X^7 + 2X^6Y - 2X^5Y^2 - X^3Y^4 + X^2Y^5 - XY^6 - 2Y^7$, $F_{10} = X^8 + 4X^7Y - 2X^6Y^2 + X^5Y^3 + 4X^4Y^4 - 4X^3Y^5 - 5X^2Y^6 - 2XY^7$, $F_{11} = X^8 - 4X^7Y - 2X^6Y^2 - 3X^5Y^3 + 4X^4Y^4 - 3X^3Y^5 + 5X^2Y^6 + XY^7 - Y^8$, $F_{12} = X^9 - 4X^8Y - 5X^7Y^2 - 5X^6Y^3 - 2X^5Y^4 + 3X^4Y^5 - X^3Y^6 + 2XY^8 - 4Y^9$, and $F_{13} = X^{10} + 4X^9Y - 4X^8Y^2 + 4X^7Y^3 + 2X^6Y^4 - 4X^5Y^5 - 3X^4Y^6 + 4X^3Y^7 + 2X^2Y^8 - 4XY^9 + 5Y^{10}$.

The resulting minimal Gröbner basis of $\text{Ann}(s^{(1)}, s^{(2)}, s^{(3)})$

$$\{Y^{13-j}F_j | j = -1, 1, 3, 4, 5, 7, 8, 9, 11, 12, 13\}$$

is not reduced.

Finally, we discuss whether the case of sequences of different lengths can be reduced to the case of sequences of equal length by extending the shorter sequences. The following example shows some difficulties that arise.

Example 4 Let $s^{(1)} := (1000)$ and $s^{(2)} := (001)$ be two sequences in $K = GF(2)$. By Algorithm 1, their annihilator ideal is found to be

$$\text{Ann}(s^{(1)}, s^{(2)}) = \langle X^3, XY, Y^4 \rangle.$$

The annihilator ideals of the extended sequences are

$$\text{Ann}(s^{(1)}, s^{(2)}0) = \langle X^3, XY^2, Y^4 \rangle \quad \text{and} \quad \text{Ann}(s^{(1)}, s^{(2)}1) = \langle X^3 + X^2Y, XY^2, Y^4 \rangle.$$

Thus all three ideals are different and, moreover,

$$\text{Ann}(s^{(1)}, s^{(2)}) \neq \text{Ann}(s^{(1)}, s^{(2)}0) + \text{Ann}(s^{(1)}, s^{(2)}1) = \langle X^3, X^2Y, XY^2, Y^4 \rangle.$$

The complete solutions of the synthesis problem are

$$\mathcal{R}(s^{(1)}, s^{(2)}) = X^3 + KX^2 + KX,$$

$$\mathcal{R}(s^{(1)}, s^{(2)}0) = X^3 + KX \quad \text{and} \quad \mathcal{R}(s^{(1)}, s^{(2)}1) = X^3 + X^2 + KX.$$

In general, any solution of the synthesis problem for the given sequences is a solution of the synthesis problem for a suitable extension of the sequences to equal length. The problem, however, is how to extend the sequences without knowing a minimal linear recursion in advance. Checking all possibilities is clearly inferior to applying the GMDA, even for the binary field. In [6] the authors proposed filling up the shorter sequences with “don’t cares” and, during the execution of the algorithm, choosing the don’t cares so as to make the corresponding discrepancies zero. It remains unclear, however, how this strategy can be used for an efficient computation of all solutions or of the annihilator ideal. One obstacle is illustrated in Example 2 where the factor ideal $\mathcal{I}_3/Y\mathcal{I}_2$ is not principal.

References

1. Althaler, J., Dür, A.: Finite Linear Recurring Sequences and Homogeneous Ideals. AAECC **7**, 377–390 (1996)
2. Becker, T., Weispfenning, V.: Gröbner Bases – A Computational Approach to Commutative Algebra. Berlin, Heidelberg, New York: Springer 1993
3. Cox, D., Little, J., O’Shea, D.: Ideals, Varieties, and Algorithms. Berlin, Heidelberg, New York: Springer 1992
4. Ding, C.: Proof of Massey’s conjectured algorithm. In: Guenther, C. G. (ed.) Advances in Cryptology – EUROCRYPT ’88, 345–349. Lecture Notes in Computer Science, Vol. 330. Berlin, Heidelberg, New York: Springer 1988
5. Feng, G. L., Tzeng, K. K.: A generalized Euclidean algorithm for multisequence shift-register synthesis. IEEE Trans. Inform. Theory **35**, 584–594 (1989)
6. Feng, G. L., Tzeng, K. K.: A Generalization of the Berlekamp-Massey Algorithm for Multisequence Shift-Register Synthesis with Applications to Decoding Cyclic Codes. IEEE Trans. Inform. Theory **37**, 1274–1287 (1991)
7. Lidl, R., Niederreiter, H.: Finite Fields. Reading, MA: Addison-Wesley 1983

8. Massey, J. L.: Shift-Register Synthesis and BCH Decoding. *IEEE Trans. Inform. Theory* **15**, 122–127 (1969)
9. McEliece, R. J.: *Finite Fields for Computer Scientists and Engineers*. Boston, MA: Kluwer 1987
10. Oberst, U.: Multidimensional Constant Linear Systems. *Acta Applicandae Mathematicae*, 1–175 (1990)
11. Sakata, S.: N-Dimensional Berlekamp-Massey Algorithm for Multiple Arrays and Construction of Multivariate Polynomials with Preassigned Zeros. In: Mora, T. (ed.) *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes '88*, 356–376. *Lecture Notes in Computer Science*, Vol. 357. Berlin, Heidelberg, New York: Springer 1989