# Algebraic-Geometric Codes and Multidimensional Cyclic Codes: A Unified Theory and Algorithms for Decoding Using Gröbner Bases

Keith Saints and Chris Heegard, *Fellow, IEEE*

*Abstract*— **In this paper, it is proved that any algebraic-geometric code can be expressed as a cross section of an extended multidimensional cyclic code. Both algebraic-geometric codes and multidimensional cyclic codes are described by a unified theory of linear block codes defined over point sets: algebraic-geometric codes are defined over the points of an algebraic curve, and an $m$-dimensional cyclic code is defined over the points in $m$-dimensional space. The power of the unified theory is in its description of decoding techniques using Gröbner bases. In order to fit an algebraic-geometric code into this theory, a change of coordinates must be applied to the curve over which the code is defined so that the curve is in special position. For curves in special position, all computations can be performed with polynomials, rather than rational functions, and this also makes it possible to take advantage of the theory of Gröbner bases. Next, a transform is defined for algebraic-geometric codes which generalizes the discrete Fourier transform. The transform is also related to a Gröbner basis, and is useful in setting up the decoding problem. In the decoding problem, a key step is finding a Gröbner basis for an error locator ideal. For algebraic-geometric codes, multidimensional cyclic codes, and indeed, any cross section of an extended multidimensional cyclic code, Sakata's algorithm can be used to find linear recursion relations which hold on the syndrome array. In this general context, we give a self-contained and simplified presentation of Sakata's algorithm, and present a general framework for decoding algorithms for this family of codes, in which the use of Sakata's algorithm is supplemented by a procedure for extending the syndrome array.**

*Index Terms*— **Algebraic-geometric codes, multidimensional cyclic codes, Gröbner bases, transform methods, Sakata's algorithm.**

## I. Introduction

MULTIDIMENSIONAL cyclic codes and algebraic-geometric codes have played a more prominent role in the theory of error-correcting codes in recent years, and there is hope that these codes will be used in applications in the near future. These two families of codes have followed divergent approaches in their generalization of Reed–Solomon codes, and this has led to the development of two distinct bodies of research. In this paper, we present a unified theory for a new class of codes which includes both multidimensional cyclic codes and algebraic-geometric codes. Under the unified theory, the relationship between multidimensional cyclic codes and algebraic-geometric codes can be made explicit, and the decoding algorithms for the two families of codes can be described under a common framework.

The unified theory provides an interesting new perspective on algebraic-geometric codes, and therefore we find it worthwhile to review some previously known results. In particular, we give a new presentation of Sakata's algorithm and its use in implementing decoding algorithms. Although this paper contains large amounts of survey material, it also presents two new techniques which may prove to be quite useful in the implementation of algebraic-geometric codes.

The first technique is the use of a change of coordinates to give an alternative presentation of an algebraic-geometric code in which the representation and calculation of algebraic-geometric quantities is simpler, and the code is in a form suitable for decoding. In the new coordinate system, we need only consider polynomial functions in affine coordinates, rather than dealing with rational functions in projective coordinates.

The second technique is the definition of a transform, generalizing the Fourier transform, which may be used with an algebraic-geometric code (or any of the codes in the broader class of codes described by the unified theory). The transform may be described as an infinite $m$-dimensional array with redundancy, which is completely determined by a finite irredundant subarray, called the *proper transform*. This situation is well-known in the decoding algorithm introduced by Feng and Rao, where certain elements of the syndrome array are constrained to satisfy a consistency relation. Now, with the theory of the generalized transform, it is possible to precisely delineate an independent set of syndromes, and state consistency relations which will determine the dependent syndromes. The basic idea behind the transform is that the consistency relations should be represented by polynomials which form a Gröbner basis for a certain ideal.

## II. Gröbner Bases

In this section, we give a brief exposition of Gröbner bases, which have proved to be a useful tool both in the theory of multivariate polynomials, and in computations involving them. For more details, see [1]–[3].

Manuscript received February 17, 1994. This work was supported in part by the U.S. Army Research Office through the Army Center of Excellence for Symbolic Methods in Algorithmic Mathematics (ACSyAM), Mathematical Sciences Institute of Cornell University, under Contract DAAL03-92-G-0126, and in part by the National Science Foundation under Grant NCR-9207331.

K. Saints is with QUALCOMM Inc., San Diego, CA 92121 USA.

C. Heegard is with the School of Electrical Engineering, Cornell University, Ithaca, NY 14853 USA.

IEEE Log Number 9414219.

Let $\mathbb{F}$ be any field, and consider the ring $\mathbb{F}[\boldsymbol{x}] = \mathbb{F}[x_1, \cdots, x_m]$ of polynomials in $m$ variables over the field $\mathbb{F}$. A *monomial* $\boldsymbol{x}^{\boldsymbol{r}}$ is a product of powers of variables, $\boldsymbol{x}^{\boldsymbol{r}} = x_1^{r_1} x_2^{r_2} \cdots x_m^{r_m}$; a *polynomial* is a finite linear combination of monomials

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{r}} f_{\boldsymbol{r}} \boldsymbol{x}^{\boldsymbol{r}}.$$

Here, $\boldsymbol{r} = (r_1, r_2, \cdots, r_m)$ is an $m$-tuple of nonnegative integers, and we denote by $\mathbb{Z}_+^m$ the set of all $m$-tuples of nonnegative integers.

Write $\boldsymbol{r} \leq \boldsymbol{s}$ if $r_i \leq s_i$ for each $i = 1, 2, \cdots, m$. This indicates that the monomial $\boldsymbol{x}^{\boldsymbol{r}}$ divides $\boldsymbol{x}^{\boldsymbol{s}}$, and so we refer to $\leq$ as the *divisibility order*. Monomials are considered to be ordered according to their exponent vectors: thus we say $\boldsymbol{x}^{\boldsymbol{r}} \leq \boldsymbol{x}^{\boldsymbol{s}}$ if and only if $\boldsymbol{r} \leq \boldsymbol{s}$. For $m \geq 2$, the divisibility order is only a partial order on $\mathbb{Z}_+^m$: for example, $x_1$ and $x_2$ are not comparable under the divisibility order.

Define a *monomial order* on $\mathbb{Z}_+^m$ to be a *total* order $\leq_T$ with the property that $\boldsymbol{r} \leq_T \boldsymbol{s}$ whenever $\boldsymbol{r} \leq \boldsymbol{s}$. Thus a monomial order is a total ordering which preserves the divisibility order. Well-known examples of monomial orders are the *pure lexicographic* order, the *graded lexicographic* order, and *weighted-degree* orders.

The *leading monomial* of a polynomial

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{s}} f_{\boldsymbol{s}} \boldsymbol{x}^{\boldsymbol{s}}$$

(with respect to the monomial order $\leq_T$) is the monomial $\boldsymbol{x}^{\boldsymbol{s}}$ with nonzero coefficient ($f_{\boldsymbol{s}} \neq 0$) that is maximal in the order $\leq_T$. For a polynomial $f(\boldsymbol{x})$ we define $\text{lead}_{\leq_T}(f) = \boldsymbol{s}$, where $\boldsymbol{x}^{\boldsymbol{s}}$ is the leading monomial of $f(\boldsymbol{x})$ with respect to the monomial order $\leq_T$. The *leading coefficient* of a polynomial is the coefficient of its leading term, and is denoted by $\text{lc}\,(f)$. In other words, if $\text{lead}(f) = \boldsymbol{s}$, then $\text{lc}\,(f) = f_{\boldsymbol{s}}$.

*Definition 1:* Let $\mathcal{F}$ be any subset of the ring $\mathbb{F}[\boldsymbol{x}]$ and let $\leq_T$ be a monomial order. Define

$$\Delta_{\leq_T}(\mathcal{F}) = \{\boldsymbol{s} \in \mathbb{Z}_+^m\colon \text{lead}_{\leq_T}(f) \not\leq \boldsymbol{s} \quad \text{for each} \quad f \in \mathcal{F}\}.$$

(We will write simply $\Delta(\mathcal{F})$ if it is understood which monomial order $\leq_T$ is used.) Thus $\Delta_{\leq_T}(\mathcal{F})$ consists of all exponent vectors $\boldsymbol{s}$ for which $\boldsymbol{x}^{\boldsymbol{s}}$ is not divisible by the leading monomial of any member of $\mathcal{F}$.

*Definition 2:* A set $\Delta \subset \mathbb{Z}_+^m$ is called a *delta set* if it has the following property: whenever $\boldsymbol{s} \in \Delta$ and $\boldsymbol{r} \leq \boldsymbol{s}$, it follows that $\boldsymbol{r} \in \Delta$.

*Definition 3:* An *interior corner* $\boldsymbol{r}$ of $\Delta$ is a integer vector $\boldsymbol{r} \in \Delta$ which is maximal in the divisibility order. That is, there does not exist $\boldsymbol{s} \in \Delta$ with $\boldsymbol{r} \leq \boldsymbol{s}$. An *exterior corner* $\boldsymbol{s}$ of $\Delta$ is an integer vector $\boldsymbol{s} \notin \Delta$ which is minimal in the divisibility order. That is, there does not exist $\boldsymbol{r} \notin \Delta$ with $\boldsymbol{r} \leq \boldsymbol{s}$. The set of interior corners of a delta set $\Delta$ is denoted by $\text{Int}\,\Delta$, and the set of exterior corners of a delta set $\Delta$ is denoted by $\text{Ext}\,\Delta$. Thus a delta set is completely determined by its exterior corners, since we can write

$$\Delta = \{\boldsymbol{r}\colon \boldsymbol{u} \not\leq \boldsymbol{r} \quad \text{for each} \quad \boldsymbol{u} \in \text{Ext}\,\Delta\}.$$

Note that for any set $\mathcal{F}$, $\Delta_{\leq_T}(\mathcal{F})$ is a delta set.

Let $\boldsymbol{I}$ be an ideal in the ring $\mathbb{F}[\boldsymbol{x}]$ and $\mathcal{F}$ be a finite subset of $\boldsymbol{I}$. We say that $\mathcal{F}$ *generates* $\boldsymbol{I}$, and write $\boldsymbol{I} = \langle \mathcal{F} \rangle$, if any element of $\boldsymbol{I}$ can be written as a finite linear combination (with polynomial coefficients) of elements of $\mathcal{F}$.

*Definition 4:* A set $\mathcal{F} \subset \boldsymbol{I}$ is a *Gröbner basis* for $\boldsymbol{I}$ (with respect to the monomial order $\leq_T$) if $\Delta_{\leq_T}(\mathcal{F}) = \Delta_{\leq_T}(\boldsymbol{I})$.

In other words, the leading monomial $\boldsymbol{x}^{\boldsymbol{r}}$ of every polynomial $g(\boldsymbol{x}) \in \boldsymbol{I}$ is divisible by the leading monomial $\boldsymbol{x}^{\boldsymbol{s}}$ of some polynomial $f(\boldsymbol{x}) \in \mathcal{F}$. We have the following two basic results about Gröbner bases:

1) With respect to any monomial order $\leq_T$, an ideal $\boldsymbol{I}$ has a Gröbner basis $\mathcal{F}$. (In general, $\mathcal{F}$ depends on the choice of monomial order.)
2) A Gröbner basis $\mathcal{F}$ for $\boldsymbol{I}$ generates $\boldsymbol{I}$ as an ideal: $\boldsymbol{I} = \langle \mathcal{F} \rangle$.

Let an ideal $\boldsymbol{I}$ and a monomial order $\leq_T$ be given. If $\boldsymbol{r} \in \Delta_{\leq_T}(\boldsymbol{I})$, then $\boldsymbol{x}^{\boldsymbol{r}}$ is called a *standard monomial*; otherwise $\boldsymbol{x}^{\boldsymbol{r}}$ is called *nonstandard*. A polynomial which is composed of only standard monomials is said to be *in normal form*. Let $f(\boldsymbol{x}) \in \mathbb{F}[\boldsymbol{x}]$, and suppose there is a polynomial $\overline{f}(\boldsymbol{x})$ that is in normal form with the property that $f(\boldsymbol{x}) = \overline{f}(\boldsymbol{x}) \bmod \boldsymbol{I}$ (this means that $f(\boldsymbol{x}) = \overline{f}(\boldsymbol{x}) + g(\boldsymbol{x})$ for some $g(\boldsymbol{x}) \in \boldsymbol{I}$). Then $\overline{f}$ is called a *normal form* of $f$ with respect to the ideal $\boldsymbol{I}$ (and the monomial order $\leq_T$). It is not hard to prove that every polynomial $f$ has a unique normal form $\overline{f}$. Thus in the ring $\mathbb{F}[\boldsymbol{x}]/\boldsymbol{I}$, each coset of $\boldsymbol{I}$ has a unique representative $\overline{f}$ which is in normal form. In particular, the zero polynomial is in normal form and is a representative of $\boldsymbol{I}$, and so a polynomial is a member of $\boldsymbol{I}$ if and only if its normal form is zero.

## III. Algebraic–Geometric Codes

Before giving a definition of an algebraic-geometric code, we give a brief review of the notation and concepts from algebraic geometry we shall need later. We concentrate mainly on affine algebraic curves, since our goal is to apply a change of coordinates to a projective curve $X$ to obtain a curve $X'$ which is essentially affine in the sense that all of the calculations relevant to coding theory can be carried out using the affine description of the curve. Fulton [4] is an excellent introductory reference for the material in this section, and more advanced treatments may be found in [5]–[8].

An algebraic curve $X$ is usually presented as the solution set of a system of polynomial equations. A more precise definition is the following. Suppose that $\mathbb{F}$ is an algebraically closed field. For any ideal $\boldsymbol{I}$ in the ring $\mathbb{F}[\boldsymbol{x}]$ of polynomials, define the *variety* of $\boldsymbol{I}$, $\boldsymbol{V}(\boldsymbol{I})$, to be the set of $m$-tuples $P \in \mathbb{F}^m$ such that $f(P)$ evaluates to zero for every $f \in \boldsymbol{I}$. A set $X$ of the form $X = \boldsymbol{V}(\boldsymbol{I})$ for some ideal $\boldsymbol{I}$ in the ring $\mathbb{F}[\boldsymbol{x}]$ is called an *affine variety* defined over $\mathbb{F}$. (Terminology varies in the literature; here we follow the convention of [2].) In particular, *m-dimensional affine space*, which is the set of all $m$-tuples, $\mathbb{F}^m$, is the variety $\mathbb{F}^m = \boldsymbol{V}(\{0\})$. Corresponding to any affine variety $X$ is the ideal $\boldsymbol{I}(X)$ consisting of the set of polynomials $f(\boldsymbol{x})$ which vanish at every point of $X$. An affine variety $X$ is *irreducible* if it cannot be decomposed into the union $X = X_1 \cup X_2$ of two disjoint affine varieties $X_1$ and $X_2$. The ring $\mathbb{F}[X] = \mathbb{F}[\boldsymbol{x}]/\boldsymbol{I}(X)$ is called the *coordinate*

*ring* of $X$. A *polynomial function* on $X$ is a function $\phi(\boldsymbol{x})$ which maps points of $X$ to values in $\mathbb{F}$, and which can be represented as evaluation by a polynomial: $\phi(\boldsymbol{x}) = f(\boldsymbol{x})$ for some polynomial $f$. Two polynomials $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$ represent the same polynomial function if and only if $f(\boldsymbol{x}) = g(\boldsymbol{x}) \bmod \boldsymbol{I}(X)$, and so polynomial functions can be identified with elements in the coordinate ring $\mathbb{F}[X]$. Applying the results of the previous section, we find that every polynomial function is uniquely represented by a polynomial in normal form (once a monomial order has been fixed). Assuming that $X$ is irreducible, the coordinate ring $\mathbb{F}[X]$ is an integral domain, and its field of fractions is called the *field of rational functions on* $X$, denoted by $\mathbb{F}(X)$. The field $\mathbb{F}(X)$ of rational functions on $X$ consists of the set of all fractions $f(\boldsymbol{x})/g(\boldsymbol{x})$, where $f/g$ and $f'/g'$ are considered to be equivalent if $fg' - f'g \in \boldsymbol{I}(X)$. If $\phi \in \mathbb{F}(X)$ is a rational function on $X$ which can be represented as $f(\boldsymbol{x})/g(\boldsymbol{x})$ where $g(P) \neq 0$, then $\phi$ is *defined at P*, and we define $\phi(P) = f(P)/g(P)$. The set of all functions $\phi \in \mathbb{F}(X)$ defined at $P$ is a local ring $\mathcal{O}_P(X)$. The point $P$ on $X$ is *nonsingular* if and only if $\mathcal{O}_P(X)$ is a discrete valuation ring, and the variety $X$ is *smooth*, or *nonsingular*, if every point on $X$ is nonsingular. The field $\mathbb{F}(X)$ of rational functions on $X$ is a field containing $\mathbb{F}$ as a subfield, and the *dimension* of $X$ is the degree of transcendence of $\mathbb{F}(X)$ over $\mathbb{F}$. An *affine algebraic curve* is a one-dimensional irreducible affine variety, and a zero-dimensional affine variety is always a finite set of points.

Now let $\mathbb{F}_q$ be the finite field with $q$ elements, and let $\mathbb{F}$ be the algebraic closure of $\mathbb{F}_q$. Suppose $X$ is an affine algebraic variety defined over $\mathbb{F}$. If $\boldsymbol{I}(X)$ is generated by a set $\mathcal{F}$ which consists of polynomials with coefficients in $\mathbb{F}_q$, then $X$ is *defined over* $\mathbb{F}_q$. Define the *field of* $\mathbb{F}_q$*-rational functions on* $X$ to be the subset $\mathbb{F}_q(X)$ of $\mathbb{F}(X)$ consisting of all functions which can be written in the form $f(\boldsymbol{x})/g(\boldsymbol{x})$ where $f$ and $g$ have coefficients from $\mathbb{F}_q$. If $P$ is a point on $X$ with coordinates in $\mathbb{F}_q$ ($P \in X \cap \mathbb{F}_q^m$), then $P$ is called a *rational point* of $X$.

The proper setting for algebraic geometry is in $m$-dimensional projective space $\mathbb{P}^m$, which consists of points $P = (a_0\colon a_1\colon \cdots \colon a_m)$, in which the $a_i \in \mathbb{F}$ are not all zero, and with $(a_0\colon a_1\colon \cdots \colon a_m)$ and $(b_0\colon b_1\colon \cdots \colon b_m)$ representing the same point whenever there is a nonzero $\lambda \in \mathbb{F}$ such that $a_i = \lambda b_i$ for all $i = 0, 1, \cdots, m$. Throughout this paper, we identify a point $P$ in $m$-dimensional affine space $P = (a_1, \cdots, a_m) \in \mathbb{F}^m$ with the point $P = (1\colon a_1\colon \cdots \colon a_m) \in \mathbb{P}^m$ in $m$-dimensional projective space. The set of points $(a_0\colon a_1\colon \cdots \colon a_m)$ with $a_0 = 0$ forms the "hyperplane at infinity," and $m$-dimensional projective space is the result of adjoining the points at infinity to $m$-dimensional affine space. For any set $\mathcal{F}$ of homogeneous polynomials in the variables $x_0, x_1, \cdots, x_m$, we may define the *projective variety of* $\mathcal{F}$ to be the set $\boldsymbol{V}_p(\mathcal{F})$ of points $P \in \mathbb{P}^m$ such that $f(P) = 0$ for all $f \in \mathcal{F}$. A polynomial $f(x_1, \cdots, x_m)$ in $m$ variables can be made into a homogeneous polynomial $f^*(x_0, x_1, \cdots, x_m)$ in $m+1$ variables by multiplying each monomial of $f$ by the power of $x_0$ which yields a monomial whose degree is the same as the total degree of $f$. If $X_a$ is an affine curve, $X_a = \boldsymbol{V}(\boldsymbol{I}_a)$, then we may form the ideal $\boldsymbol{I} = \{f^*\colon f \in \boldsymbol{I}_a\}$, and define the *projective closure* $X$ of $X_a$ by $X = \boldsymbol{V}_p(\boldsymbol{I})$. The projective closure $X$ is the smallest projective variety containing $X_a$. For a complete development of algebraic geometry in projective space, consult any of the standard textbooks: for example, [2], [4], [6]–[8]. We remark that every rational function on $X$ corresponds to a unique rational function on $X_a$: $\mathbb{F}(X) \cong \mathbb{F}(X_a)$.

Let $X$ be a smooth irreducible projective curve defined over $\mathbb{F}_q$. A *divisor* on a curve $X$ is a formal sum

$$G = \sum_{P \in X} g_P P$$

with integer coefficients $g_P \in \mathbb{Z}$, ony finitely many of which are nonzero. The *support* of a divisor $G$ is the set $\{P\colon g_P \neq 0\}$. The *degree* of a divisor $G$ is the sum

$$\deg G = \sum_{P \in X} g_P.$$

A divisor is called effective, written $G \geq 0$, if $g_P \geq 0$ for all $P$. Since the curve is smooth, at any point $P$, $\mathcal{O}_P(X)$ is a discrete valuation ring, and thus there is a discrete valuation $\mathrm{ord}_P$ which gives the *order* $\mathrm{ord}_P\, \phi \in \mathbb{Z}$ of a rational function $\phi$ at $P$. If $\mathrm{ord}_P\, \phi = a > 0$, then $\phi$ is said to have a *zero of order* $a$ at $P$ (in particular, this means that $\phi(P) = 0$). If $\mathrm{ord}_P\, \phi = -a < 0$, then $\phi$ is said to have a *pole* of *order* at $P$. Associated with a nonzero rational function $\phi$ is the divisor

$$(\phi) = \sum_{P \in X} \mathrm{ord}_P\, \phi.$$

Associated with any divisor $G$ is the vector space $L(G)$ of rational functions on $X$ with poles "no worse than $G$"

$$L(G) = \{\phi \in \mathbb{F}_q(X)\colon (\phi) + G \geq 0\} \cup \{0\}.$$

In general, the dimension of the vector space $L(G)$ is given by the Riemann–Roch theorem, but usually the following will suffice:

*Theorem 5 (Riemann's Theorem):* If $\deg G > 2g - 2$, then

$$\dim L(G) = \deg G - g + 1$$

where $g$ is a nonnegative integer called the *genus* of the curve $X$.

There are several equivalent ways of defining the genus $g$ of a curve $X$, but perhaps the most elementary is to define $g$ to be the maximum value of $\deg G + 1 - \dim L(G)$ as $G$ ranges over all divisors on $X$.

Let $X$ be a projective curve, and let $Q$ be a point of $X$. For some values of the integer $j$, there are no functions $\phi$ in $L(jQ)$ whose pole order at $Q$ is exactly equal to $j$. In other words, $L(jQ) = L((j-1)Q)$. In this case, $j$ is called a *Weierstrass gap*, or simply a *gap*, of $Q$. Any integer $j \geq 0$ which is not a gap of $Q$ is called a *nongap*, and it follows from an elementary argument that in this case,

$$\dim L(jQ) = 1 + \dim L((j-1)Q).$$

By induction, it follows that $\dim L(aQ)$ is equal to the number of nongaps $j \leq a$. The following result is an immediate corollary of Riemann's theorem.

*Proposition 6:* For a curve $X$ with genus $g$, and a point $Q \in X$, there are exactly $g$ gaps, and each gap $j$ satisfies $j < 2g$.

Let $N(Q) \subset \mathbb{Z}$ be the set of nongaps of $Q$. It is always the case that $0 \in N(Q)$, since the constant functions are in $L(aQ)$ for all $a$. If $\phi \in L(aQ)$ is a function with pole order $a$, and $\psi \in L(bQ)$ is a function with pole order $b$, then $\phi\psi \in L((a+b)Q)$ is a function with pole order $a+b$. Thus $N(Q)$ is a *semigroup*: it is closed under addition (but not under subtraction). We say that a set of integers $\{o_1, o_2, \cdots, o_m\} \subset \mathbb{Z}$ generates $N(Q)$ as a semigroup, and write $N(Q) = \langle o_1, \cdots, o_m \rangle$, if any $a \in N(Q)$ can be written as

$$a = \sum_{i=1}^{m} r_i o_i$$

for some $\boldsymbol{r} \in \mathbb{Z}_+^m$. We say that $o_1, o_2, \cdots, o_m$ is a *minimal* set of generators for $N(Q)$ if $N(Q)$ is not generated by any set of cardinality less than $m$.

A minimal generating set for the semigroup $N(Q)$ has at most $g+1$ elements, because the set $\{o_1, o_2, \cdots, o_{g+1}\}$ of all nongaps $\leq 2g+1$ always generates the semigroup $N(Q)$ [9], [10]. The worst case, in which a minimal generating set actually has $g+1$ elements occurs only when the set of gaps is $\{1, 2, \cdots, g\}$. It will be desirable to minimize the size of the generating set for the semigroup $N(Q)$, and therefore it will be desirable to choose $Q$ so that its set of gaps is different from $\{1, 2, \cdots, g\}$.

We review briefly the definition of algebraic-geometric codes as introduced by Goppa [11], and subsequently detailed in [5], [9], [10], [12]–[16]. Let $X$ be a smooth irreducible projective curve defined over $\mathbb{F}_q$. Let $P_1, \cdots, P_n$ be rational points of $X$, and let $D = P_1 + \cdots + P_n$ and $G$ be divisors over $X$ with disjoint supports. Then we may define the algebraic-geometric codes $C_L(D, G)$ and $C_\Omega(D, G)$ as follows:

$$C_L(D, G) = \{(\phi(P_1), \cdots, \phi(P_n)) \colon \phi \in L(G)\}$$

$$C_\Omega(D, G) = \left\{ c \in \mathbb{F}_q^n \colon \sum_{j=1}^{n} c_j \phi(P_j) = 0 \quad \text{for all} \quad \phi \in L(G) \right\}.$$

(Here, we define $C_\Omega(D, G)$ simply as the dual code of $C_L(D, G)$, although it can be explicitly constructed in terms of differentials on $X$). Assuming that $\deg G = a$, with $2g - 2 < a < n$, where $g$ is the genus of the curve $X$, the parameters of these algebraic-geometric codes can be easily estimated by applying Riemann's theorem [12], [13]

$$\begin{aligned} &C_L(D, G): \quad (n, a-g+1, d \geq n-a) \\ &C_\Omega(D, G): \quad (n, n-a+g-1, d \geq a-2g+2). \end{aligned} \tag{1}$$

The unified theory presented in this paper does not encompass algebraic-geometric codes in their full generality: our results are restricted to the class of *one-point* algebraic codes $C_\Omega(D, aQ)$ defined by a divisor $G$ which is a multiple $G = aQ$ of a single point. However, this does not restrict our ability to design codes using (1), since the choice of divisor $G$ affects the estimated parameters only through its degree $a$.

## IV. Multidimensional Cyclic Codes

Let $\mathbb{F}_q^{(q-1)\times\cdots\times(q-1)}$ denote the set of $m$-dimensional arrays of size $(q-1) \times \cdots \times (q-1)$ with entries from $\mathbb{F}_q$. Let $\mathbb{Z}_{q-1}$ denote the set of integers $\{0, 1, \cdots, q-2\}$, and $\mathbb{Z}_{q-1}^m$ denote the collection of $m$-tuples formed from this set. Then each word $w \in \mathbb{F}_q^{(q-1)\times\cdots\times(q-1)}$ is an $m$-dimensional array with entries $w_{\boldsymbol{r}} \in \mathbb{F}_q$ indexed by integer $m$-tuples, $\boldsymbol{r} \in \mathbb{Z}_{q-1}^m$. Corresponding to the word $w$ is the polynomial $w(\boldsymbol{x})$ in $m$ variables

$$w(\boldsymbol{x}) = \sum_{\boldsymbol{r} \in \mathbb{Z}_{q-1}^m} w_{\boldsymbol{r}} x^{\boldsymbol{r}}.$$

The natural definition of an $m$-dimensional cyclic code is a subset $C$ of $\mathbb{F}_q^{(q-1)\times\cdots\times(q-1)}$ which is closed under $m$-dimensional cyclic shifts of its codewords. We opt to give an equivalent definition which is more suited for our purposes. Let $\alpha \in \mathbb{F}_q$ be a primitive root of unity of order $q-1$, and for any $\boldsymbol{r} \in \mathbb{Z}_{q-1}^m$, let $\alpha^{\boldsymbol{r}}$ denote the point

$$\alpha^{\boldsymbol{r}} = (\alpha^{r_1}, \cdots, \alpha^{r_m}) \in \mathbb{F}_q^m.$$

*Definition 7:* Let $M \subset \mathbb{Z}_{q-1}^m$ be a set of integer $m$-tuples. A subset $C$ of $\mathbb{F}_q^{(q-1)\times\cdots\times(q-1)}$ is an *$m$-dimensional cyclic code* of size $(q-1)\times\cdots\times(q-1)$ if the polynomials $a(\boldsymbol{x})$ associated with the words of $C$ vanish at the points $\alpha^{\boldsymbol{r}}$ associated with the elements $\boldsymbol{r} \in M$. In other words, for each $a \in C$ and $\boldsymbol{r} \in M$, we have $a(\alpha^{\boldsymbol{r}}) = 0$. This $m$-dimensional cyclic code is denoted by $C = \mathrm{Cyc}\,(M)$. The properties of multidimensional cyclic codes are studied in [17], [18].

An algebraic-geometric code is based on the evaluation of certain rational functions on a finite set of points lying on an algebraic curve. The following definition gives a notation for defining linear block codes based on arbitrary spaces of functions evaluated on arbitrary sets of points.

*Definition 8:* Let $\mathcal{P}$ be a finite set of points, $\mathcal{P} = \{P_1, \cdots, P_n\}$, and let $\mathcal{L}$ be a vector space of functions mapping $\mathcal{P}$ to $\mathbb{F}_q$. Then we define the codes

$$\mathcal{C}(\mathcal{P}, \mathcal{L}) = \{(\phi(P_1), \cdots, \phi(P_n)) \colon \quad \phi \in \mathcal{L}\}$$

$$\mathcal{C}^\perp(\mathcal{P}, \mathcal{L}) = \left\{ c \in \mathbb{F}_q^n \colon \quad \sum_{j=1}^{n} c_j \phi(P_j) = 0 \quad \text{for all} \quad \phi \in \mathcal{L} \right\}.$$

The enumeration $P_1, \cdots, P_n$ of the points in $\mathcal{P}$ is not important here, so it becomes more convenient to index the coordinates of codewords in $C^\perp(\mathcal{P}, \mathcal{L})$ by the points of $\mathcal{P}$ rather than by the integers $1, \cdots, n$. So we may write

$$\mathcal{C}^\perp(\mathcal{P}, \mathcal{L}) = \left\{ c \in (\mathbb{F}_q)^{\mathcal{P}} \colon \quad \sum_{P \in \mathcal{P}} c_P \phi(P) = 0 \quad \text{for all} \quad \phi \in \mathcal{L} \right\}.$$

Now we are ready to redefine multidimensional cyclic codes as codes defined by evaluation of functions over a set of points. Let $\mathbb{F}_q^*$ denote the set of nonzero elements of $\mathbb{F}_q$: $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$. Also for $M \subset \mathbb{Z}_{q-1}^m$, let $\mathcal{L}(\mathcal{M})$ denote the linear space of polynomials spanned by the monomials $\boldsymbol{x}^{\boldsymbol{r}}$ for $\boldsymbol{r} \in M$.

*Theorem 9:* $\mathrm{Cyc}\,(M) = \mathcal{C}^{\perp}((\mathbb{F}_q^*)^m, \mathcal{L}(M))$.

*Proof:* A word $w \in \mathbb{F}_q^n$ is a codeword in the $m$-dimensional cyclic code $\mathrm{Cyc}\,(M)$ if and only if $w(\alpha^{\boldsymbol{r}}) = 0$ for all $\boldsymbol{r} \in M$, and $w$ is a codeword in the code $\mathcal{C}^{\perp}((\mathbb{F}_q^*)^m, \mathcal{L}(M))$, if and only if

$$\sum_{P \in (\mathbb{F}_q^*)^m} w_P \boldsymbol{x}^{\boldsymbol{r}}(P) = 0$$

for all $\boldsymbol{r} \in M$. These are equivalent conditions, as the following calculation shows: for any $\boldsymbol{r} \in M$, we have

$$\begin{aligned} w(\alpha^{\boldsymbol{r}}) &= \sum_{\boldsymbol{s} \in \mathbb{Z}_{q-1}^m} w_{\boldsymbol{s}} \boldsymbol{x}^{\boldsymbol{s}}(\alpha^{\boldsymbol{r}}) \\ &= \sum_{\boldsymbol{s} \in \mathbb{Z}_{q-1}^m} w_{\boldsymbol{s}} \alpha^{\boldsymbol{s} \cdot \boldsymbol{r}} \\ &= \sum_{\boldsymbol{s} \in \mathbb{Z}_{q-1}^m} w_{\boldsymbol{s}} \boldsymbol{x}^{\boldsymbol{r}}(\alpha^{\boldsymbol{s}}) \\ &= \sum_{P \in (\mathbb{F}_q^*)^m} w_P \boldsymbol{x}^{\boldsymbol{r}}(P). \end{aligned} \tag{2}$$

where we have made the identification $w_P = w_{\boldsymbol{s}}$, when $P$ is the point $P = \alpha^{\boldsymbol{s}}$. ■

*Definition 10:* An *extended* multidimensional cyclic code is a code $\mathrm{Ext\,Cyc}\,(M)$ defined by

$$\mathrm{Ext\,Cyc}\,(M) = \mathcal{C}^{\perp}(\mathbb{F}_q^m, \mathcal{L}(M))$$

for some $M \subset \mathbb{Z}_{q-1}^m$. In the extended code, $\mathbb{F}_q^*$ is replaced by $\mathbb{F}_q$, and so codewords have length $q^m$ rather than $(q-1)^m$. Although the codewords of the extended code can be arranged in a fairly standard way as arrays of size $q \times \cdots \times q$, the code is no longer closed under cyclic shifts, and although the codewords can be interpreted as polynomials, the code is not characterized by the zero set of these polynomials.

The blocklength of an $m$-dimensional cyclic code $\mathrm{Cyc}(M)$ is $(q-1)^m$, and its dimension is $(q-1)^m - |M|$. The blocklength of an extended $m$-dimensional code $\mathrm{Ext\,Cyc}\,(M)$ is $q^m$, and its dimension is $q^m - |M|$. We are able to compute the minimum distance of these codes in the following special cases.

*Example 1 (Reed–Solomon Codes):* Let $m = 1$, and let $M = \{1, 2, \cdots, r\}$, $M^+ = \{0, 1, 2, \cdots, r\}$. Then $\mathrm{Cyc}\,(M)$ is a $(q-1, q-1-r, r+1)$ Reed–Solomon code, and $\mathrm{Ext\,Cyc}\,(M^+)$ is an $(q, q-1-r, r+2)$ extended Reed–Solomon code (obtained by extending $\mathrm{Cyc}\,(M)$).

*Example 2 (Hyperbolic Cascaded Reed–Solomon Codes):* An $m$-dimensional Hyperbolic Cascaded Reed–Solomon (HCRS) code is a code $\mathrm{Cyc}\,(H_d)$ and an extended HCRS code is a code $\mathrm{Ext\,Cyc}\,(H_d)$, defined from the set

$$H_d = \left\{ \boldsymbol{p} \in \mathbb{Z}_{q-1}^m : \prod_{i=1}^{m} (p_i - 1) < d \right\}.$$

An HCRS code $\mathrm{Cyc}\,(H_d)$ has minimum distance $d^* \geq d$, and $d^* > d$ if and only if $H_d = H_{d^*}$ [19]–[21]. (The same holds for extended HCRS codes.) One-dimensional HCRS codes are Reed–Solomon codes, and one-dimensional extended HCRS codes are extended Reed–Solomon codes.

Let $\mathcal{Q}$ be a subset of $\mathcal{P}$. The relationship between the codes $\mathcal{C}(\mathcal{P}, \mathcal{L})$ and $\mathcal{C}(\mathcal{Q}, \mathcal{L})$ is simple: the codewords of $\mathcal{C}(\mathcal{Q}, \mathcal{L})$ are obtained by *puncturing* the codewords of $\mathcal{C}(\mathcal{P}, \mathcal{L})$: take a codeword $c \in \mathcal{C}(\mathcal{P}, \mathcal{L})$ and omit the coordinates $c_P$ for each point $P \notin \mathcal{Q}$. Starting with the code $\mathcal{C}^{\perp}(\mathcal{P}, \mathcal{L})$, we may consider the subcode consisting of those codewords $c$ for which $c_P = 0$ for each point $P \notin \mathcal{Q}$. By deleting the coordinates $c_P$ for $P \notin \mathcal{Q}$ in each codeword in this subcode, we arrive at the code $\mathcal{C}^{\perp}(\mathcal{Q}, \mathcal{L})$. Following the terminology of MacWilliams and Sloane ([22, p. 29]), we say that $\mathcal{C}^{\perp}(\mathcal{Q}, \mathcal{L})$ is obtained from $\mathcal{C}^{\perp}(\mathcal{P}, \mathcal{L})$ by *taking a cross section.* Conversely, a codeword $c$ in the code $\mathcal{C}^{\perp}(\mathcal{Q}, \mathcal{L})$ can be extended to a codeword in $\mathcal{C}^{\perp}(\mathcal{P}, \mathcal{L})$ by setting $c_P = 0$ for each point $P \in \mathcal{P}$ not in $\mathcal{Q}$. In this way the code $\mathcal{C}^{\perp}(\mathcal{Q}, \mathcal{L})$ can be identified with the subcode of $\mathcal{C}^{\perp}(\mathcal{P}, \mathcal{L})$ consisting of those codewords $c$ for which $c_P = 0$ for each point $P \notin \mathcal{Q}$.

For any subset $\mathcal{P}$ of $\mathbb{F}_q^m$, we note that the code $\mathcal{C}^{\perp}(\mathcal{P}, \mathcal{L}(M))$ is obtained by taking a cross section of the extended multidimensional cyclic code $\mathrm{Ext\,Cyc}\,(M) = \mathcal{C}^{\perp}(\mathbb{F}_q^m, \mathcal{L}(M))$. In particular, $m$-dimensional cyclic codes are cross sections of extended $m$-dimensional cyclic codes.

## V. The Unified Theory

In this section, we introduce the term *special position* to describe a certain property of an algebraic curve. For an algebraic curve in special position, certain calculations of algebraic-geometric quantities are greatly simplified, and as we shall see in subsequent sections, certain techniques for the decoding problem associated with an algebraic-geometric code are possible only when the curve is in special position. Next, we give a construction by which any algebraic curve may be put into special position through an appropriate change of coordinates. The change of coordinates does not change any of the algebraic-geometric properties of the code, and in particular, algebraic-geometric codes derived from the curve are not altered in any way.

Suppose $X_a$ is a smooth affine curve in $m$-dimensional affine space, and let $X$ be the projective closure of $X_a$. Let $Q$ be a rational point of $X$, and let $\mathcal{P} = \{P_1, \cdots, P_n\}$ be a set consisting of other rational points of $X$, and let $D$ be the divisor $D = P_1 + \cdots + P_n$. In the code $C_\Omega(D, aQ)$, $Q$ has the interpretation as a "point at infinity," since we consider functions in the space $L(aQ)$ which blow up only at $Q$. On the other hand, the projective space $\mathbb{P}^m$ is regarded as the extension of affine space $\mathbb{F}_q^m$ by a "hyperplane at infinity" $x_0 = 0$. We examine the special case that arises when these two concepts of infinity coincide: that is, when the chosen point $Q$ is the only point (rational or otherwise) of $X$ lying on the hyperplane at infinity.

Although the affine curve $X_a$ is nonsingular, it is possible that the point $Q$ is singular on the projective curve $X$. Every curve $X$ has a *nonsingular model* which is a nonsingular projective curve $\overline{X}$ which is birationally isomorphic to the original curve. For details on birational isomorphisms and the existence of a nonsingular model, see [4], [6]–[8]. The points of $\overline{X}$ are called the *places* of $X$, and a place $\overline{Q}$ is said to be *centered* at $Q$ if $\overline{Q}$ is mapped to $Q$ by the birational

isomorphism. At every point is centered at least one and at most finitely many places. At any nonsingular point of $X$, there is precisely one place centered at that point, and it is usual to identify the point and the place in this situation. A singular point of $X$ is called a *cusp* if there is precisely one place centered there. We will adopt the convention of also identifying a cuspidal singularity with its unique place. Divisors, defined earlier for nonsingular curves, are defined for arbitrary curves as sums of places with integer coefficients. We shall assume that there is exactly one place centered at the point $Q$. This means that either $Q$ is nonsingular, or $Q$ is a cusp. In case $Q$ is a cuspidal singularity, our convention of identifying $Q$ and $\overline{Q}$ means that the space $L(aQ)$ is defined as the space of rational functions $\phi \in \mathbb{F}_q(X)$ which have poles only at $\overline{Q}$ with pole order $a$ or less. This allows us to define algebraic-geometric codes $C_L(D, aQ)$ and $C_\Omega(D, aQ)$ as usual.

*Definition 11:* We say that the projective curve $X$ is in *special position* with respect to the point $Q$ if

1) The hyperplane at infinity, $x_0 = 0$, intersects $X$ in precisely one point, $Q$.
2) The affine curve $X_a = X \backslash Q$ is nonsingular.
3) There is exactly one place centered at the point $Q$.
4) For $j = 1, \cdots, m$, let $o_j$ be the order of the pole of the function $x_j$ at $Q$ (recall that the function $x_j$ is written as $x_j/x_0$ in projective coordinates). Then the $o_j$ are distinct and ordered: $0 < o_1 < o_2 < \cdots < o_m$.
5) The $o_j$ generate the nongaps of $Q$ as a semigroup: each nongap $a$ may be written as

$$a = \Sigma r_j o_j$$

using nonnegative integer coefficients $r_j$.

Kamiya and Miura, in [23], characterized planar curves (curves in $\mathbb{P}^2$) which are in special position.

*Theorem 12:* Suppose the projective curve $X$ is in special position with respect to the point $Q$. Then the algebraic-geometric code $C_\Omega(D, aQ)$ is a cross section of an extended $m$-dimensional cyclic code

$$C_\Omega(D, aQ) = \mathcal{C}^\perp(\mathcal{P}, \mathcal{L}(M_a))$$

where $D = P_1 + \cdots + P_n$ and $\mathcal{P} = \{P_1, \cdots, P_n\}$.

*Proof:* The two codes are defined on the same set of points, so we only need to show that the two spaces of functions are the same: that is, we must show that $L(aQ) = \mathcal{L}(M_a)$. Recall that each of the coordinate functions $x_i$ has a pole at $Q$ of order $o_i$, and so a monomial function $\boldsymbol{x}^{\boldsymbol{r}}$ has a pole at $Q$ of order $\Sigma o_i r_i$. Thus the pole order of a monomial function is given by a weighted degree function, which we may use to define a monomial order. Let $\leq_\circ$ denote the weighted-degree monomial order which orders a monomial $\boldsymbol{x}^{\boldsymbol{r}}$ first according to its *order* $\Sigma o_i r_i$ and then lexicographically with $x_1 < \cdots < x_m$. Clearly, the set of monomial functions

$$\mathcal{L}(M_a) = \{\boldsymbol{x}^{\boldsymbol{r}}: \quad \Sigma o_i r_i \leq a\}$$

is a subset of $L(aQ)$, so the proof follows from the following proposition.

*Proposition 13:* Let $X$ be a projective curve in special position with respect to the point $Q$. Let $\phi(\boldsymbol{x})$ be a rational function in the space $L(aQ)$. Then there exists a polynomial $f(\boldsymbol{x})$ which is equivalent to $\phi(\boldsymbol{x})$ as a rational function on the curve $X$, and which is the sum of terms $\boldsymbol{x}^{\boldsymbol{r}}$ of order $\leq a$.

*Proof:* Proof is by induction on $a$. If $a = 0$, then $\phi(\boldsymbol{x})$ is a function with no poles on the projective curve $X$, which can only be a constant function. Therefore $\phi(\boldsymbol{x})$ is equivalent to a constant polynomial which is a term of order 0.

Now suppose the proposition is true for all functions in the space $L((a-1)Q)$. Let $\phi(\boldsymbol{x})$ be a function in the space $L(aQ)$. We may assume that the pole order of the function $\phi(\boldsymbol{x})$ at the point $Q$ is exactly $a$, for otherwise $\phi(\boldsymbol{x}) \in L((a-1)Q)$. The pole order $a$ is a nongap of $Q$, and since $X$ is in special position, this means that $a$ can be expressed as

$$a = \Sigma o_i r_i$$

for some integers $r_1, \cdots, r_m$. Therefore, the monomial function $\boldsymbol{x}^{\boldsymbol{r}}$ is another function in the space $L(aQ)$ which has pole order $a$ at $Q$. Since

$$\dim L(aQ) = 1 + \dim L((a-1)Q)$$

and

$$\boldsymbol{x}^{\boldsymbol{r}} \in L(aQ) \backslash L((a-1)Q)$$

it follows that $\phi(\boldsymbol{x})$ can be expressed as

$$\phi(\boldsymbol{x}) = \beta \boldsymbol{x}^{\boldsymbol{r}} + \psi(\boldsymbol{x}) \tag{3}$$

for some nonzero $\beta \in \mathbb{F}_q$, and some $\psi \in L((a-1)Q)$. Equation (3) is meant to be interpreted as an equality of rational functions, but the inductive assumption allows us to represent $\psi(\boldsymbol{x})$ as a polynomial which is the sum of terms of order $a-1$ or less. Thus (3) is actually an equality of polynomial functions in the coordinate ring $\mathbb{F}_q[X_a]$, and moreover, it expresses $\phi(\boldsymbol{x})$ as a polynomial which is the sum of terms of order $a$ or less, which concludes the inductive proof. ■

*Proposition 14:* Let $X$ be a projective curve that is in special position with respect to the point $Q$. The order of any polynomial function $f$ on $X_a$ may be calculated as follows. Let $\overline{f}$ be the normal form of $f$ with respect to the ideal $\boldsymbol{I}(X_a)$ and the order $\leq_\circ$. Then the order of $f$ is the order of the leading monomial of $\overline{f}$.

*Proof:* Suppose that there are two monomials $\boldsymbol{x}^{\boldsymbol{r}}$ and $\boldsymbol{x}^{\boldsymbol{s}}$ of the same order $a$, both of which are standard for the ideal $\boldsymbol{I}(X_a)$ with respect to the order $\leq_\circ$. We may suppose that $s \leq_\circ \boldsymbol{r}$. There exists some nonzero $\beta \in \mathbb{F}_q$ such that the polynomial $g(\boldsymbol{x}) = \boldsymbol{x}^{\boldsymbol{r}} - \beta \boldsymbol{x}^{\boldsymbol{s}}$ has order $a-1$ or less. Applying Proposition 13, it follows that $g(\boldsymbol{x})$ is equivalent to a polynomial $h(\boldsymbol{x})$ which is the sum of terms of order $a-1$ or less. Define

$$f(\boldsymbol{x}) = \boldsymbol{x}^{\boldsymbol{r}} - \beta \boldsymbol{x}^{\boldsymbol{s}} - h(\boldsymbol{x}). \tag{4}$$

Then $f(\boldsymbol{x}) = 0 \bmod \boldsymbol{I}(X_a)$, or in other words, $f(\boldsymbol{x}) \in \boldsymbol{I}(X_a)$. Since $f$ is a member of the ideal $\boldsymbol{I}(X_a)$, and its leading monomial is $\boldsymbol{x}^{\boldsymbol{r}}$, it follows that $\boldsymbol{x}^{\boldsymbol{r}}$ is a nonstandard monomial,

giving a contradiction. Thus we have proved that there is at most one standard monomial of any order.

Now assume that $f(\boldsymbol{x})$ is a polynomial, and let $\overline{f}(\boldsymbol{x})$ be its normal form (with respect to the ideal $\boldsymbol{I}(X_a)$ and the monomial order $\leq_\circ$). Then $\overline{f}$ is the sum of terms of distinct orders, and so the order of $\overline{f}$ is the order of its leading term. ■

*Example 3:* Let $X$ be the Hermitian curve given, in affine coordinates, by the equation $x^{r+1}-y^r-y=0$ over $\mathbb{F}_q$, where $q=r^2$. This curve is nonsingular and in special position. The unique point on the hyperplane $z=0$ at infinity is the point $Q=(0\colon\ 0\colon\ 1)$, expressed in projective coordinates as $(z\colon\ x\colon\ y)$. The coordinate functions $x/z$ and $y/z$ have orders $o_1=r$ and $o_2=r+1$. The Hermitian curve has $r^3+1$ rational points, so we may choose the divisor $D$ to be the formal sum of the $r^3$ rational points other than $Q$, and form an algebraic-geometric code $C_\Omega(D,\ aQ)$.

Because the Hermitian curve is in a special position, it has many nice properties, which explains why it is so widely used as an example in the literature of algebraic-geometric codes. The technique outlined in this paper of putting curves into special position can be seen as a means of making every algebraic-geometric code behave in a similarly nice fashion.

Theorem 12 allows us to relate algebraic-geometric codes with extended $m$-dimensional cyclic codes and their duals, as shown in the following diagram:

$$\begin{array}{ccc} \mathcal{C}(\mathbb{F}_q^m,\ \mathcal{L}(M_a)) & \overset{\text{dual}}{\leftrightarrow} & \mathcal{C}^\perp(\mathbb{F}_q^m,\ \mathcal{L}(M_a)) \\ \downarrow \text{ punc} & & \downarrow \text{ c-s} \\ C_L(D,\ aQ) & \overset{\text{dual}}{\leftrightarrow} & C_\Omega(D,\ aQ) \end{array}$$

Thus codes of the form $C_L(D,\ aQ)$ are obtained through puncturing (indicated in the diagram by "punc"), and codes of the form $C_\Omega(D,\ aQ)$ are obtained through the dual operation of taking a cross section (indicated in the diagram by "c-s").

Next, we will show that starting from an arbitrary projective curve $X$ and an arbitrary place $Q$ on $X$, there is a change of coordinates which puts $X$ in special position with respect to $Q$. We seek a projective curve $X'$ which is in special position, and a birational isomorphism $X\rightarrow X'$. Let $\overline{X}$ be a nonsingular model of $X$. (Computation of $\overline{X}$ is investigated in [24].) There is a birational isomorphism $X\rightarrow\overline{X}$, and thus it suffices to find a birational isomorphism $\overline{X}\rightarrow X'$. Hence, we may assume without loss of generality that $X$ is nonsingular.

Given a set of nongaps $\{o_1,\cdots,o_m\}$, $0<o_1<o_2<\cdots<o_m$, which generates the semigroup $N(Q)$ of all nongaps, choose rational functions $\phi_i\in L(o_iQ)$ such that the pole order of $\phi_i$ at $Q$ is exactly $o_i$. We do not assume that the $o_i$ are a minimal generating set. A standard construction in algebraic geometry is the mapping from $X\backslash\{Q\}$ to $\mathbb{F}_q^m$ given by

$$P\mapsto(\phi_1(P),\cdots,\phi_m(P)).$$

(This is the mapping associated with the linear system associated with the $\phi_i$.) Let $X_a'$ be the image of $X$ under this map, and let $X'\subset\mathbb{P}^m$ be the projective closure of $X_a'$. Porter [9] investigated the use of this mapping to put an algebraic curve in special position, and his results are summarized and extended in the following theorem.

*Theorem 15:* The map $P\mapsto(\phi_1(P),\cdots,\phi_m(P))$ extends to a birational isomorphism of $X$ and $X'$. The projective curve $X'$ is in special position with respect to the point $Q'\in X'$ which is the image of $Q$ under the extended map $X\rightarrow X'$. The algebraic-geometric codes defined from $X$ and $X'$ are identical when a point $P\in X$ is identified with its image $P'\in X'$. In particular

$$C_L(D',\ aQ')=C_L(D,\ aQ)$$

$$C_\Omega(D',\ aQ')=C_\Omega(D,\ aQ).$$

*Proof:* See Appendix I. ■

*Corollary 16:* Let $X$ be any projective curve, and let $Q$ be a place of $X$. Then the code $C_\Omega(D,\ aQ)$ is a cross section of an extended multidimensional cyclic code.

Note that in the map $X\rightarrow X'$, the curve $X'$ is embedded in $m$-dimensional projective space, where $m$ may be different from the dimension of the space in which the original curve $X$ is embedded. In fact, $m$ is equal to the number of semigroup generators for $N(Q)$.

If $\{o_1,\cdots,o_{g+1}\}$ is the complete set of nongaps $\leq 2g+1$, then the set $\{\phi_1,\cdots,\phi_{g+1}\}$ actually forms a basis for $L((2g+1)Q)$. Then $X'$ is the image of a complete linear system, and by a well-known result in algebraic geometry, this implies that $X'$ is nonsingular. This shows that $X'$ may always be embedded as a nonsingular curve in $\mathbb{P}^{g+1}$ which is in special position. However, to minimize the dimension $m$ of the space $\mathbb{P}^m$, we should not insist that $X'$ be nonsingular, as long as it is in special position.

In order to represent $X_a'$ in the usual way as an affine curve, we would like to find a set of polynomials $\mathcal{F}$ in $m$ variables whose solution set is the curve $X_a'=\boldsymbol{V}(\mathcal{F})$. From the proof of Theorem 15, $X_a'=\boldsymbol{V}(\boldsymbol{I})$, where $\boldsymbol{I}$ is the ideal consisting of all polynomials $f(\boldsymbol{y})\in\mathbb{F}_q[y_1,\cdots,y_m]$, such that $f(\phi_1,\cdots,\phi_m)\in\mathbb{F}_q(X)$ is equivalent to zero as a rational function on $X$. In other words, we want to find the ideal $\boldsymbol{I}$ of all polynomial relations satisfied by the rational functions $\phi_1,\cdots,\phi_m$. Computation of a generating set for the ideal $\boldsymbol{I}$ may be accomplished using a modified version of the Rational Implicitization algorithm described in [2, pp. 131–132].

*Example 4 (The Klein Quartic):* (Portions of this example are due to [9].) The Klein Quartic is a curve $X$ defined in the projective plane by the equation

$$x_0^3x_1+x_1^3x_2+x_2^3x_0=0.$$

We consider this curve over the field $\mathbb{F}_8$. We choose the point $Q=(0\colon\ 0\colon\ 1)$, and proceed to calculate the gaps of $Q$ and functions corresponding to the nongaps. This curve has genus $g=3$, and the three gaps of $Q$ are $\{1,\ 2,\ 4\}$. The semigroup $N(Q)$ is generated by 3, 5, and 7. Therefore, we seek functions $\phi_1$, $\phi_2$, $\phi_3\in L(7Q)$ whose pole orders are 3, 5, and 7, respectively. We may take

$$\phi_1(x_0\colon\ x_1\colon\ x_2)=\frac{x_2}{x_0}$$

$$\phi_2(x_0\colon\ x_1\colon\ x_2)=\frac{x_1x_2}{x_0^2}$$

$$\phi_3(x_0\colon\ x_1\colon\ x_2)=\frac{x_2^3}{x_0^2x_1}.$$

Thus we make a change of coordinates from $(x_0\colon\ x_1\colon\ x_2)$ to $(y_0\colon\ y_1\colon\ y_2\colon\ y_3)$ which maps the curve into projective 3-space. The ideal of the curve $X'$ is the collection of all polynomial relations satisfied by the functions $\phi_i$. The equations of the curve $X'_a$ are given by a generating set $\{g_1, g_2, g_3, g_4\}$ for this ideal

$$g_1(y_1, y_2, y_3) = y_1y_3 + y_2^2 + y_1$$

$$g_2(y_1, y_2, y_3) = y_2y_3 + y_1^4$$

$$g_3(y_1, y_2, y_3) = y_3^2 + y_1^3y_2 + y_3$$

$$g_4(y_1, y_2, y_3) = y_2^3 + y_1^5 + y_1y_2.$$

(These four polynomials form a Gröbner basis for $\boldsymbol{I}(X')$ with respect to the monomial order $\leq_\circ$ induced by the pole orders $(o_1, o_2, o_3) = (3, 5, 7)$.) The unique point on $X'$ in projective coordinates $(y_0\colon\ y_1\colon\ y_2\colon\ y_3)$ which intersects the hyperplane $y_0 = 0$ is the point $Q' = (0\colon\ 0\colon\ 0\colon\ 1)$. In the new coordinates, we may write any rational function in the space $L(aQ)$ as a polynomial in $y_1$, $y_2$, and $y_3$. Once we have computed the new coordinates $(y_1, y_2, y_3)$ of all of the points $P'_i$, we no longer need the functions $\phi_1$, $\phi_2$, and $\phi_3$.

In this example, the point $Q'$ is a cuspidal singularity, but this does not prevent us from defining algebraic-geometric codes. However, if it is preferable to have a nonsingular curve $X''$, then, according to the comments following Theorem 15, we can embed the curve in $\mathbb{P}^4$ by choosing $(o'_1, o'_2, o'_3, o'_4) = (3, 5, 6, 7)$ to be the complete list of nongaps $\leq 2g + 1$. Then we may set $\phi'_1 = \phi_1$, $\phi'_2 = \phi_2$, $\phi'_3 = \phi_1^2$, $\phi'_4 = \phi_3$. The equations defining $X''$ will then be $\{g'_1, g'_2, g'_3, g'_4, g'_5\}$, where $g'_i(y_1, y_2, y_3, y_4) = g_i(y_1, y_2, y_4)$, for $i = 1, 2, 3, 4$ and $g'_5(y_1, y_2, y_3, y_4) = y_3 + y_1^2$.

## VI. The Generalized Transform

In this section, we define a transform which is useful in studying a code $C$ which is a cross section of an extended $m$-dimensional cyclic code $C = \mathcal{C}^\perp(\mathcal{P}, \mathcal{L}(M))$. When $\mathcal{P} = (\mathbb{F}_q^*)^m$, $C$ is a multidimensional cyclic code, and in this situation, the transform is the usual $m$-dimensional discrete Fourier transform. Thus the transform we present here can be viewed as a generalization of the discrete Fourier transform.

*Definition 17:* Assume that $\mathcal{P} \subset \mathbb{F}_q^m$. The *transform* on $(\mathbb{F}_q)^\mathcal{P}$ is the map which takes a word $w \in (\mathbb{F}_q)^\mathcal{P}$ to an (infinite) $m$-dimensional array $W \in (\mathbb{F}_q)^{(\mathbb{Z}_+^m)}$ defined by

$$W_{\boldsymbol{s}} = \sum_{P\in\mathcal{P}} w_P \boldsymbol{x}^{\boldsymbol{s}}(P), \qquad \boldsymbol{s} \in \mathbb{Z}_+^m.$$

Note that the transform is defined for a collection $\mathcal{P}$ of points in affine, not projective, space. Associated with the finite set of points $\mathcal{P}$, there is the ideal $\boldsymbol{I}(\mathcal{P})$ in the polynomial ring $\mathbb{F}_q[\boldsymbol{x}] = \mathbb{F}_q[x_1, \cdots, x_m]$ consisting of polynomials which vanish at these points. Since $\mathcal{P}$ consists of points with coordinates in $\mathbb{F}_q$, the polynomial $x_j^q - x_j$ will also be a member of the ideal $\boldsymbol{I}(\mathcal{P})$ for $j = 1, \cdots, m$. In case $\mathcal{P}$ is a set of rational points on a curve $X$, the polynomials which define the curve $X$ will also be members of the ideal $\boldsymbol{I}(\mathcal{P})$. Let $\leq_T$ be a fixed monomial order. Define $\Delta_\mathcal{P} = \Delta_{\leq_T}(\boldsymbol{I}(\mathcal{P}))$ to be the set of integer vectors $\boldsymbol{s}$ such that $\boldsymbol{x}^{\boldsymbol{s}}$ is a standard monomial with respect to $\boldsymbol{I}(\mathcal{P})$.

*Definition 18:* The *proper transform* is a map from $(\mathbb{F}_q)^\mathcal{P}$ to $(\mathbb{F}_q)^{\Delta_\mathcal{P}}$, which takes a word $w \in (\mathbb{F}_q)^\mathcal{P}$ to the finite "subarray" $W|_{\Delta_\mathcal{P}}$ of its full transform $W$.

Now we state an important result which says that the delta set of an ideal counts the points of the ideal's zero set.

*Theorem 19:* Let $\boldsymbol{I} = \boldsymbol{I}(\mathcal{P})$ be the ideal of a finite set of points $\mathcal{P} \subset \mathbb{F}_q^m$. Then the following quantities are equal:

1) The dimension of $\mathbb{F}_q[\boldsymbol{x}]/\boldsymbol{I}$ as a vector space over $\mathbb{F}_q$.
2) The number of standard monomials $|\Delta_{\leq_T}(\boldsymbol{I})|$ with respect to any monomial order $\leq_T$.
3) The number of points $|\mathcal{P}|$.

*Proof:* The fact that every polynomial $f \in \mathbb{F}_q[\boldsymbol{x}]$ has a unique normal form shows that the standard monomials form a basis for $\mathbb{F}_q[\boldsymbol{x}]/\boldsymbol{I}$. Another basis for $\mathbb{F}_q[\boldsymbol{x}]/\boldsymbol{I}$ is obtained by considering a set of polynomials $\{f_P(\boldsymbol{x})\colon\ P \in \mathcal{P}\}$ with the property that $f_P(P) = 1$, and $f_P(Q) = 0$ for each $Q \in \mathcal{P}\backslash\{P\}$. Clearly, each $f_P$ is in a distinct coset of $\mathbb{F}_q[\boldsymbol{x}]/\boldsymbol{I}$ and if $g(\boldsymbol{x})$ is any polynomial, then

$$g(\boldsymbol{x}) = \sum_{P\in\mathcal{P}} g(P) f_P(\boldsymbol{x}) \bmod \boldsymbol{I}. \qquad \blacksquare$$

*Theorem 20:* The transform $w \mapsto W$ is a one-to-one linear map from $(\mathbb{F}_q)^\mathcal{P}$ to $(\mathbb{F}_q)^{\mathbb{Z}_+^m}$ and the proper transform $w \mapsto W|_{\Delta_\mathcal{P}}$ is one-to-one and is a surjection onto the space $(\mathbb{F}_q)^{\Delta_\mathcal{P}}$ (i.e., invertible on $(\mathbb{F}_q)^{\Delta_\mathcal{P}}$).

*Proof:* The linearity of the transforms follows directly from the definitions. First we prove that the proper transform is one-to-one. Let $w$ be a word whose proper transform $W|_{\Delta_\mathcal{P}}$ is identically zero. Let $P$ be any point in $\mathcal{P}$. Choose a polynomial $A(\boldsymbol{x}) \in \mathbb{F}_q[\boldsymbol{x}]$ which vanishes at every point of $\mathcal{P}$ except $P$. Now, reduce $A(\boldsymbol{x})$ to its normal form $\overline{A}(\boldsymbol{x})$ which is a polynomial made up of monomials $\boldsymbol{x}^{\boldsymbol{r}}$ for $\boldsymbol{r} \in \Delta_\mathcal{P}$, and we have the following equality:

$$\begin{aligned} 0 &= \Sigma_{\boldsymbol{r}\in\Delta_\mathcal{P}} \overline{A}_{\boldsymbol{r}} W_{\boldsymbol{r}} = \Sigma_{\boldsymbol{r}} \overline{A}_{\boldsymbol{r}} \Sigma_{Q\in\mathcal{P}} w_Q \boldsymbol{x}^{\boldsymbol{r}}(Q) \\ &= \Sigma_{Q\in\mathcal{P}} w_Q \overline{A}(Q) = w_P A(P). \end{aligned}$$

Since $P$ was arbitrary, we may conclude that $w = 0$. Since the proper transform is a linear map, this shows that it is one-to-one. Thus the full transform is also one-to-one, since the proper transform is a subarray of the full transform.

By Theorem 19, the cardinality of $\Delta_\mathcal{P}$ is the same as the cardinality of $\mathcal{P}$. Thus the proper transform is a linear map between vector spaces of the same finite dimension. Since the proper transform is one-to-one, the dimension of the image of $(\mathbb{F}_q)^\mathcal{P}$ under the transform is $|\mathcal{P}|$, which shows that the proper transform is a surjection. $\blacksquare$

*Example 5:* Let $\mathcal{P} = (\mathbb{F}_q^*)^m$. Then a Gröbner basis (with respect to any monomial order) for $\boldsymbol{I}(\mathcal{P})$ is given by $\{x_1^{q-1} - 1, \cdots, x_m^{q-1} - 1\}$. Then $\Delta_\mathcal{P} = \{\boldsymbol{s}\colon\ s_j \leq q - 2 \text{ for all } j\}$, and the proper transform $w \mapsto W|_{\Delta_\mathcal{P}}$ can be evaluated by interpreting $w$ as a polynomial $w(\boldsymbol{x})$ and evaluating: $W_s = w(\alpha^{\boldsymbol{s}})$. This is the $m$-dimensional discrete Fourier transform. (See [25] for

details of the one- and two-dimensional versions of the discrete Fourier transform.)

*Example 6:* Consider the Hermitian curve $X_a \subset \mathbb{F}_{16}^2$ defined by $x^5 - y^4 - y = 0$ over $\mathbb{F}_{16}$. Let $Q$ be the unique point on $X$ at infinity, and let $\mathcal{P}$ be the set consisting of the other 64 rational points. Let $\leq_\circ$ be the weighted-degree orders which orders a monomial $x^i y^j$ first according to its weighted degree $4i+5j$, and orders monomials with the same weighted degree according to the exponent $j$. One can check that a Gröbner basis for $\boldsymbol{I}(\mathcal{P})$ with respect to the weighted-degree order $\leq_\circ$ is given by $\{y^4 - x^5 + y, x^{16} - x\}$. The set of standard monomials is given by the set

$$\Delta_{\mathcal{P}} = \{(i, j): \quad 0 \leq i < 16, 0 \leq j < 4\}$$

and the proper transform $w \mapsto W|_{\Delta_{\mathcal{P}}}$ is a isomorphism of 64-dimensional vector spaces over $\mathbb{F}_{16}$.

## VII. The Error Locator Ideal

In the decoding problem, we assume that a codeword $c$ in a cross section of an extended $m$-dimensional cyclic code $\mathcal{C}^\perp(\mathcal{P}, \mathcal{L}(M))$ is transmitted over a noisy channel and corrupted by an error word $e \in (\mathbb{F}_q)^{\mathcal{P}}$, so that the word $w = c + e$ is received by the decoder. The decoder seeks to determine the error word $e$, and at least conceptually, this task may be accomplished by first determining the *error locations* and then the *error values*. The error locations, or *support* of the word $e \in (\mathbb{F}_q)^{\mathcal{P}}$ is defined as the set $\operatorname{supp}(e) = \{P \in \mathcal{P}: e_P \neq 0\}$. In this section, we relate the set of error locations with an ideal which describes the linear recursion relations satisfied by the syndrome array.

Another, equivalent, way of posing the decoding problem is to determine the transform $E$ of the error word. By definition of the code $\mathcal{C}^\perp(\mathcal{P}, \mathcal{L}(M))$, whenever $\boldsymbol{s} \in M$, the corresponding entry $C_{\boldsymbol{s}}$ of the transform $C$ of the codeword $c$ vanishes: $C_{\boldsymbol{s}} = 0$. Therefore, for $\boldsymbol{s} \in M$, the entry $E_{\boldsymbol{s}}$ of the transform of the error word may be obtained directly by computing the entry $W_{\boldsymbol{s}} = E_{\boldsymbol{s}}$ of the transform $W$ of the received word $w = c + e$. The entries $E_{\boldsymbol{s}}$, $\boldsymbol{s} \in M$, are thus the *syndromes* of the error word. The values of the remaining entries of the array $E$ are initially unknown to the decoder, and although these unknown entries are not syndromes in the usual sense, we shall refer to them also as syndromes, and refer to $E$ as the *syndrome array*.

*Example 7:* Consider again the Hermitian curve over $\mathbb{F}_{16}$ as in Example 6. Consider the (64, 46, 13) algebraic-geometric code $C_\Omega(D, 23Q) = \mathcal{C}(\mathcal{P}, \mathcal{L}(M_{23}))$. Let $\alpha$ be a primitive element of $\mathbb{F}_{16}$ satisfying the equation $\alpha^4 + \alpha + 1 = 0$. Let $e$ be an error word of Hamming weight 6

$$\begin{aligned} e_{(1,\alpha^8)} &= \alpha^{11} \\ e_{(\alpha^2,\alpha^{12})} &= \alpha^{14} \\ e_{(\alpha^3,\alpha^2)} &= \alpha^2 \\ e_{(\alpha^{11},\alpha^3)} &= \alpha \\ e_{(\alpha^{12},\alpha^4)} &= \alpha^{14} \\ e_{(\alpha^{14},\alpha^{11})} &= \alpha^3 \\ e_P &= 0, \qquad \text{otherwise.} \end{aligned}$$

The entries $E_{ij}$ of the two-dimensional syndrome array associated with this error are

| $i$ \ $j$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | $\cdots$ |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | $\alpha^6$ | 1 | 0 | $\alpha^5$ | $*$ | $*$ | $\cdots$ |
| 1 | $\alpha^{12}$ | $\alpha^3$ | $\alpha^4$ | $\alpha^6$ | $*$ | $*$ | $\cdots$ | |
| 2 | 1 | $\alpha^7$ | 1 | $\alpha^2$ | $*$ | $*$ | $\cdots$ | |
| 3 | $\alpha$ | $\alpha^8$ | $\alpha^5$ | $*$ | $*$ | $\cdots$ | | |
| 4 | 0 | 1 | $*$ | $*$ | $*$ | $\cdots$ | | |
| 5 | $\alpha^9$ | $*$ | $*$ | $*$ | $\vdots$ | | | |
| 6 | $*$ | $*$ | $\vdots$ | $\vdots$ | | | | |
| $\vdots$ | $\vdots$ | $\vdots$ | | | | | | |

(5)

The syndromes $E_{ij}$ are known only for $4i + 5j \leq 23$, and unknown syndromes are indicated by the symbol $*$.

*Definition 21:* Let

$$f(\boldsymbol{x}) = \Sigma f_{\boldsymbol{s}} x^{\boldsymbol{s}} \in \mathbb{F}[x_1, \cdots, x_m]$$

be a polynomial in $m$ variables. The $m$-dimensional array $E$ is said to satisfy the *$m$-dimensional linear recursion relation* with characteristic polynomial $f(\boldsymbol{x})$ if

$$\sum_{\boldsymbol{s}} f_{\boldsymbol{s}} E_{\boldsymbol{s}+\boldsymbol{r}} = 0, \qquad \text{for all } \boldsymbol{r} \geq 0. \tag{6}$$

(Note that $\boldsymbol{r}, \boldsymbol{s} \in \mathbb{Z}_+^m$ are vectors of nonnegative integers, and that the sum is finite since the polynomial $f(\boldsymbol{x})$ has only finitely many nonzero coefficients $f_{\boldsymbol{s}}$). The $m$-dimensional linear recursion relation represented by the polynomial $f(\boldsymbol{x})$ is said to be *valid* for the $m$-dimensional array $E$ if (6) holds.

*Definition 22:* The set of characteristic polynomials of all valid $m$-dimensional linear recursion relations for the syndrome array $E$ is called the *error locator ideal*, and is denoted by $V(E)$.

*Theorem 23:* The syndrome array $E$ satisfies the $m$-dimensional linear recursion relation with characteristic polynomial $f(\boldsymbol{x})$ if and only if $f(P) = 0$ for all error locations $P \in \operatorname{supp}(e)$. In other words, $V(E) = \boldsymbol{I}(\operatorname{supp}(e))$.

*Proof:* First note the following identity for any $\boldsymbol{r} \in \mathbb{Z}_+^m$:

$$\begin{aligned} \sum_{\boldsymbol{s}} f_{\boldsymbol{s}} E_{\boldsymbol{s}+\boldsymbol{r}} &= \sum_{\boldsymbol{s}} f_{\boldsymbol{s}} \sum_{P \in \mathcal{P}} e_P \boldsymbol{x}^{\boldsymbol{s}+\boldsymbol{r}}(P) \\ &= \sum_{P \in \operatorname{supp}(e)} e_P \boldsymbol{x}^{\boldsymbol{r}}(P) \sum_{\boldsymbol{s}} f_{\boldsymbol{s}} \boldsymbol{x}^{\boldsymbol{s}}(P) \\ &= \sum_{P \in \operatorname{supp}(e)} e_P f(P) \boldsymbol{x}^{\boldsymbol{r}}(P) \end{aligned} \tag{7}$$

The identity (7) shows that if $f(P) = 0$ for $P \in \operatorname{supp}(e)$, then $f(\boldsymbol{x})$ is the characteristic polynomial of an $m$-dimensional linear recursion relation satisfied by the syndrome array $E$.

To prove the converse, assume that the $m$-dimensional linear recursion relation defined by $f(\boldsymbol{x})$ is a valid relation for $E$. Define the word $a$ by $a_P = e_P f(P)$. Then identity (7) implies that

$$\sum_{P \in \mathcal{P}} a_P \boldsymbol{x}^{\boldsymbol{r}}(P) = 0, \qquad \text{for all } \boldsymbol{r} \in \mathbb{Z}_+^m$$

or in other words, the transform $A$ of $a$ is identically zero. From this it follows that the word $a$ is identically zero, and so for each error location $P \in \text{supp}(e)$, we have $e_P \neq 0$, and therefore $f(P) = 0$. ■

It is interesting to note that since all words are supported on the set $\mathcal{P}$, the polynomials in the ideal $\boldsymbol{I}(\mathcal{P})$ give $m$-dimensional linear recursion relations which are automatically satisfied by any transform array. In other words, $\boldsymbol{I}(\mathcal{P}) \subset \boldsymbol{I}(\text{supp}(e)) = V(E)$. In order for the decoder to take this information into account, a Gröbner basis $\mathcal{F}$ for the ideal $\boldsymbol{I}(\mathcal{P})$ should be available. Using the $m$-dimensional linear recursion relations determined by the polynomials in the set $\mathcal{F}$, the (redundant) entries of any transform array may be computed from the entries of the proper transform. We also emphasize that in the case of an algebraic-geometric code defined over a curve $X$, the equations of the curve determine the ideal $\boldsymbol{I}(X)$ which is also a subset of $V(E)$, but the ideal of the points $\boldsymbol{I}(\mathcal{P}) \supset \boldsymbol{I}(X)$ gives slightly more refined information about what is known about the syndrome array.

## VIII. Sakata's Algorithm

As a consequence of Theorem 23, the error locations $\text{supp}(e)$ may be determined from the set of $m$-dimensional linear recursion relations valid on the transform $E$ of the error. Although the decoder does not know the full array $E$, it does know a large enough portion of the array to determine some valid recursion relations. This idea is a generalization of the Berlekamp–Massey algorithm [26], [27] which determines the error locations for a Reed–Solomon code by computing a minimal recursion relation (or shift register) which is satisfied by the syndromes.

Sakata [28], [29] developed an algorithm for determining the set of linear recursion relations satisfied by a multidimensional array. Sakata's algorithm forms a framework for a decoding algorithm, but we must also make some extensions to the original algorithm since we are ultimately interested in relations satisfied by the infinite array $E$, and also because we want to take into account the additional information that the members of the ideal $\boldsymbol{I}(\mathcal{P})$ give relations which are automatically valid for the array.

Choose a monomial order $\leq_T$ on the monomials in $m$ variables. Associated with the error locator ideal $V(E)$ is the delta set $\Delta_{\leq_T}(V(E))$. A minimal Gröbner basis $\mathcal{F}$ for the ideal $V(E)$ consists of characteristic polynomials of $m$-dimensional linear recursion relations that are satisfied by the $m$-dimensional array $E$ and have minimal leading monomials. Thus $\mathcal{F}$ is a *minimal polynomial set*, in the terminology of Sakata, for the array $E$.

According to Definition 21, an $m$-dimensional linear recursion relation represented by a polynomial $f(\boldsymbol{x}) \in \mathbb{F}[\boldsymbol{x}]$ is valid for the $m$-dimensional array $E$ if the equation

$$\Sigma f_{\boldsymbol{s}} E_{\boldsymbol{r}+\boldsymbol{s}} = 0$$

holds for *all* $\boldsymbol{r} \geq 0$, but now we shall consider the case in which the equation

$$\Sigma f_{\boldsymbol{s}} E_{\boldsymbol{r}+\boldsymbol{s}} = 0$$

is satisfied on some subarray of $E$. We regard the entries of the $m$-dimensional array $E$ as being ordered according to the order $\leq_T$. Then we may rewrite (6) to express the largest entry of $E$ (this is the entry $E_{\boldsymbol{u}}$ where $\boldsymbol{u} = \boldsymbol{r} + \text{lead}(f)$) as a linear combination of the previous entries $E_{\boldsymbol{p}}$, $\boldsymbol{p} <_T \boldsymbol{u}$

$$E_{\boldsymbol{u}} = \frac{-1}{\text{lc}(f)} \sum_{\boldsymbol{p} <_T \boldsymbol{u}} f_{\text{lead}(f)-\boldsymbol{u}+\boldsymbol{p}} E_{\boldsymbol{p}}. \tag{8}$$

*Definition 24:* The $m$-dimensional linear recursion relation represented by the polynomial $f(\boldsymbol{x})$ is said to be *invalid for the $m$-dimensional array $E$ at entry $E_{\boldsymbol{u}}$* if $\boldsymbol{u} \geq \text{lead}(f)$ (compared according to the divisibility order) and

$$E_{\boldsymbol{u}} \neq \frac{-1}{\text{lc}(f)} \sum_{\boldsymbol{p} <_T \boldsymbol{u}} f_{\text{lead}(f)-\boldsymbol{u}+\boldsymbol{p}} E_{\boldsymbol{p}}.$$

Otherwise, the $m$-dimensional linear recursion relation represented by the polynomial $f(\boldsymbol{x})$ is said to be *valid for the $m$-dimensional array $E$ at entry $E_{\boldsymbol{u}}$*.

Note that this definition leads to the convention that whenever $\boldsymbol{u} \not\geq \text{lead}(f)$, the $m$-dimensional linear recursion relation represented by the polynomial $f(\boldsymbol{x})$ is *automatically* valid at entry $E_{\boldsymbol{u}}$. This is because when $\boldsymbol{u} \not\geq \text{lead}(f)$, it is not possible to relate the elements $E_{\boldsymbol{p}}$ for $\boldsymbol{p} \leq_T \boldsymbol{u}$ according to the $m$-dimensional linear recursion relation represented by the polynomial $f(\boldsymbol{x})$. However, when $\boldsymbol{u} \geq \text{lead}(f)$, it is required that (8) holds for the $m$-dimensional linear recursion relation represented by the polynomial $f(\boldsymbol{x})$ to be valid at entry $E_{\boldsymbol{u}}$. It should be stressed that in the rearrangement of (6) as (8), we isolate the entry $E_{\boldsymbol{u}}$ which is greatest according to the particular monomial order $\leq_T$ which has been chosen. Therefore, the notion that a $m$-dimensional linear recursion relation is valid or invalid at a particular entry $E_{\boldsymbol{u}}$ depends implicitly on the choice of monomial order.

*Definition 25:* We say that the $m$-dimensional linear recursion relation represented by the polynomial $f(\boldsymbol{x})$ *is valid for the $m$-dimensional array $E$ up to entry $E_{\boldsymbol{u}}$* if it is valid at each entry $E_{\boldsymbol{r}}$, for all $\boldsymbol{r} \leq_T \boldsymbol{u}$. The collection of characteristic polynomials of all $m$-dimensional linear recursion relations valid for the $m$-dimensional array $E$ up to entry $E_{\boldsymbol{u}}$ is denoted by $V_{\boldsymbol{u}}(E)$.

Rewriting (8), we see that a polynomial $f(\boldsymbol{x})$ is in the set $V_{\boldsymbol{u}}(E)$ if and only if

$$\sum_{\boldsymbol{s}} f_{\boldsymbol{s}} E_{\boldsymbol{r}+\boldsymbol{s}} = 0, \quad \text{for all } \boldsymbol{r} \in \mathbb{Z}_+^m \text{ such that } \boldsymbol{r} + \text{lead}(f) \leq_T \boldsymbol{u}. \tag{9}$$

Note that validity of an $m$-dimensional linear recursion relation at an entry $E_u$, or validity for all entries up to entry $E_{\boldsymbol{u}}$ depends only on the entries $E_{\boldsymbol{r}}$ of the $m$-dimensional array $E$ up to entry $E_{\boldsymbol{u}}$: the entries $E_{\boldsymbol{p}}$, for $\boldsymbol{u} <_T \boldsymbol{p}$ can be changed arbitrarily without affecting the validity of an $m$-dimensional linear recursion relation up to entry $E_{\boldsymbol{u}}$.

The set $V_{\boldsymbol{u}}(E)$ fails to be an ideal because it is not closed under addition. On the other hand, the set $V_{\boldsymbol{u}}(E)$ is closed under monomial multiplication:

*Theorem 26:* Suppose $f(\boldsymbol{x}) \in V_{\boldsymbol{u}}(E)$, and let $g(\boldsymbol{x}) = \boldsymbol{x}^{\boldsymbol{p}} f(\boldsymbol{x})$. Then $g(\boldsymbol{x}) \in V_{\boldsymbol{u}}(E)$.

Note that any relation valid on the entire array is valid on a subarray, so $V(E) \subseteq V_{\boldsymbol{u}}(E)$ for any $\boldsymbol{u}$. Furthermore, if $\boldsymbol{r} \leq_T \boldsymbol{s}$, then any relation valid up to entry $\boldsymbol{s}$ is also valid up to entry $\boldsymbol{r}$, and so $V_{\boldsymbol{s}}(E) \subseteq V_{\boldsymbol{r}}(E)$. Letting $\boldsymbol{u}^+$ denote the successor to $\boldsymbol{u}$ in the monomial order $\leq_T$, we have

$$\begin{array}{ccccccc} \mathbf{0} & <_T & \boldsymbol{u} & <_T & \boldsymbol{u}^+ & <_T & \infty \\ \mathbb{F}_q[\boldsymbol{x}] & \supseteq & V_{\boldsymbol{u}}(E) & \supseteq & V_{\boldsymbol{u}^+}(E) & \supseteq & V(E) \\ \varnothing & \subseteq & \Delta(V_{\boldsymbol{u}}(E)) & \subseteq & \Delta(V_{\boldsymbol{u}^+}(E)) & \subseteq & \Delta(V(E)). \end{array}$$

In other words, as $\boldsymbol{u}$ increases according to the monomial order $\leq_T$, the delta set $\Delta(V_{\boldsymbol{u}}(E))$ increases in size, starting from the empty set, until its final value $\Delta(V(E))$. The size of this delta set measures the number of errors which have occurred.

*Theorem 27:* Assume that $\{E_{\boldsymbol{r}}: \quad \boldsymbol{r} \in \mathbb{Z}_+^m\}$ is the syndrome array for an error pattern $e$. Then the size of the delta set $\Delta(V(E))$ is equal to the number of errors which have occurred

$$|\Delta(V(E))| = \|e\|_H$$

(this is the Hamming weight of the word $e$) and

$$|\Delta(V_{\boldsymbol{u}}(E))| \leq \|e\|_H, \qquad \text{for all } \boldsymbol{u} \in \mathbb{Z}_+^m.$$

*Proof:* By the Error Location Theorem (Theorem 23), the error locator ideal $V(E)$ is the ideal $V(E) = \boldsymbol{I}(\text{supp}\,(e))$ corresponding to the set $\text{supp}\,(e)$) of points. Each of these points $P \in \text{supp}\,(e)$ identifies a distinct error location, and hence the number of points, is equal to the number of errors which have occurred: $|\text{supp}\,(e)| = \|e\|_H$. But in Theorem 19, it was shown that the size of the delta set associated with an ideal of the form $\boldsymbol{I}(\text{supp}\,(e))$ equals the cardinality of the point set $\text{supp}\,(e)$, and so $|\Delta(V(E))| = \|e\|_H$. For all $\boldsymbol{u} \in \mathbb{Z}_+^m$, $\Delta(V_{\boldsymbol{u}}(E)) \subseteq \Delta(V(E))$ and thus $|\Delta(V_{\boldsymbol{u}}(E))| \leq \|e\|_H$.

The definition of a minimal polynomial set for the set $V_{\boldsymbol{u}}(E)$ is the same as the definition of a Gröbner basis (Definition 4), the only difference being that the set $V_{\boldsymbol{u}}(E)$ is not an ideal.

*Definition 28:* Let $\Delta(V_{\boldsymbol{u}}(E))$ be the delta set associated with the set $V_{\boldsymbol{u}}(E)$. A set $\mathcal{F} \subset V_{\boldsymbol{u}}(E)$ is called a *minimal polynomial set* for $V_{\boldsymbol{u}}(E)$ if $\Delta(\mathcal{F}) = \Delta(V_{\boldsymbol{u}}(E))$.

The delta set $\Delta(V_{\boldsymbol{u}}(E))$ consists of the monomials which do *not* occur as the leading term of any polynomial in the set $V_{\boldsymbol{u}}(E)$. For this reason, Sakata called $\Delta(V_{\boldsymbol{u}}(E))$ the *excluded point set.*

The output of Sakata's algorithm is a minimal polynomial set $\mathcal{F}$, consisting of the characteristic polynomials of $m$-dimensional linear recursion relations which are valid for the array $E$ up to some specified entry $E_{\boldsymbol{u}}$. The validity of the polynomials in the set $\mathcal{F}$ can be checked by applying (9), but the minimality of their leading monomials is not self-evident. Therefore, it will be necessary to provide additional information, in the form of another set $\mathcal{G}$ of polynomials, called a *witness set*, which will serve to verify that the leading monomials of the polynomials in the set $\mathcal{F}$ are indeed minimal.

*Definition 29:* Let $f(\boldsymbol{x})$ be the characteristic polynomial of an $m$-dimensional linear recursion relation which is valid for all entries $E_{\boldsymbol{r}}$ up to, but not necessarily including entry $E_{\boldsymbol{u}}$. Define the *predicted value* for the entry $E_{\boldsymbol{u}}$ associated with $f(\boldsymbol{x})$

$$P_{\boldsymbol{u}}(f) = \frac{-1}{\text{lc}\,(f)} \sum_{p <_T \boldsymbol{u}} f_{\text{lead}\,(f)-\boldsymbol{u}+\boldsymbol{p}} E_{\boldsymbol{p}}. \tag{10}$$

The value $P_{\boldsymbol{u}}(f)$ predicted for the entry $E_{\boldsymbol{u}}$ by a polynomial $f(\boldsymbol{x})$ is just the right-hand side of (8), and therefore the $m$-dimensional linear recursion relation represented by the polynomial $f(\boldsymbol{x})$ is valid at entry $E_{\boldsymbol{u}}$ of the $m$-dimensional array $E$ if and only if the actual value of entry $E_{\boldsymbol{u}}$ is equal to the predicted value $P_{\boldsymbol{u}}(f)$.

*Theorem 30 (Agreement Theorem):* Suppose that the $m$-dimensional linear recursion relations represented by the polynomials $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$ are valid for the $m$-dimensional array $E$ at all entries $E_{\boldsymbol{q}}$ preceding entry $E_{\boldsymbol{u}}$ (that is, for $\boldsymbol{q} <_T \boldsymbol{u}$), and suppose $\boldsymbol{u} \geq \text{lead}\,(f) + \text{lead}\,(g)$. Then the polynomials $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$ agree in their prediction for the value of the array entry $E_{\boldsymbol{u}}$

$$P_{\boldsymbol{u}}(f) = P_{\boldsymbol{u}}(g).$$

*Proof:* See Appendix II. ∎

*Definition 31:* Let $g(\boldsymbol{x})$ be the characteristic polynomial of an $m$-dimensional linear recursion relation which is valid for the $m$-dimensional array $E$ at all entries preceding the entry $E_{\boldsymbol{u}}$, but which is invalid at entry $E_{\boldsymbol{u}}$. The *span* of $g(\boldsymbol{x})$ is the vector

$$\text{Span}\,(g) = \boldsymbol{u} - \text{lead}\,(g)$$

and the *discrepancy* of $g(\boldsymbol{x})$ is the quantity

$$\delta_g = \text{lc}\,(g)[E_{\boldsymbol{u}} - P_{\boldsymbol{u}}(g)] = \sum_{\boldsymbol{s}} g_{\boldsymbol{s}} E_{\boldsymbol{s}+\text{Span}\,(g)} \neq 0.$$

Theorem 32, first proved by Sakata in his original paper [28], is the $m$-dimensional generalization of a theorem originally proved by Massey [27].

*Theorem 32:* Suppose $g \notin V_{\boldsymbol{u}}(E)$. Then $\text{Span}\,(g) \in \Delta(V_{\boldsymbol{u}}(E))$.

*Proof:* See Appendix II. ∎

*Example 8:* Consider again the syndrome array in Example 7. Let

$$g(x, y) = xy + \alpha^{11}x^2 + \alpha^{13}y + \alpha^{11}x + \alpha^6.$$

Then the two-dimensional linear recursion relation

$$E_{i,j} = \alpha^{11}E_{i+1,j-1} + \alpha^{13}E_{i-1,j} + \alpha^{11}E_{i,j-1} + \alpha^6 E_{i-1,j-1}$$

associated with the polynomial $g(x, y)$ is valid for all syndromes prior to entry $(2, 2)$, but is invalid at entry $(i, j) = (2, 2)$. In other words, the recursion relation is valid for $(i, j) = (2, 1), (1, 2), (3, 1)$ (all $(i, j)$ satisfying $\text{lead}\,(g) = (1, 1) \leq (i, j) <_T (2, 2)$), but is invalid for $(i, j) = (2, 2)$. Thus $\text{Span}\,(g) = (2, 2) - (1, 1) = (1, 1)$, and so Theorem 32 implies that $(1, 1) \in \Delta(V_{2,2}(E))$; there is no polynomial with lead term $xy$ which defines a recursion relation which is valid up to entry $(2, 2)$.

*Definition 33:* Let $g(\boldsymbol{x}) \in \mathbb{F}[\boldsymbol{x}] \backslash V(E)$. Then the polynomial $g(\boldsymbol{x})$ is called a *witness* for the point $\text{Span}\,(g)$.

The idea behind Definition 33 is that the polynomial $g(\boldsymbol{x})$ verifies, through Theorem 32, the fact that $\text{Span}\,(g)$ is a member of the delta set $\Delta(V(E))$.

*Definition 34:* Let $\mathcal{G} \subset \mathbb{F}[\boldsymbol{x}] \backslash V(E)$ be a set of polynomials. The set $\mathcal{G}$ is called a *witness set* for the delta set $\Delta$ if $\mathcal{G}$ contains a witness for each interior corner of the delta set $\Delta$. We write $\Delta = \text{Span}(\mathcal{G})$. If $\mathcal{G}$ is a witness set for the delta set $\Delta$, then we know immediately that the interior corners of $\Delta$ are members of the set $\Delta(V(E))$. Since $\Delta(V(E))$ is a delta set, this implies that $\Delta \subseteq \Delta(V(E))$.

The following theorem shows how a set $\mathcal{F}$ can be verified to be a minimal polynomial set, given an appropriate witness set $\mathcal{G}$. The idea is that the witness set $\mathcal{G}$ determines certain points which must be inside the delta set $\Delta(V_{\boldsymbol{u}}(E))$, and the polynomial set $\mathcal{F}$ determines points which must be outside $\Delta(V_{\boldsymbol{u}}(E))$, and when the two boundaries match, the delta set is known exactly.

*Theorem 35:* Suppose $\mathcal{F} \subset V_{\boldsymbol{u}}(E)$ and suppose that $\mathcal{G} \subset \mathbb{F}[\boldsymbol{x}] \backslash V_{\boldsymbol{u}}(E)$ is a witness set for the delta set $\Delta(\mathcal{F})$. Then $\Delta(\mathcal{F}) = \Delta(V_{\boldsymbol{u}}(E))$, which implies that $\mathcal{F}$ is a minimal polynomial set for $V_{\boldsymbol{u}}(E)$.

*Proof:* Because $\mathcal{G}$ is a witness set for $\Delta(\mathcal{F})$, we have $\Delta(\mathcal{F}) \subseteq \Delta(V_{\boldsymbol{u}}(E))$. On the other hand, $\mathcal{F}$ is a subset of $V_{\boldsymbol{u}}(E)$, and so it follows that $\Delta(V_{\boldsymbol{u}}(E)) \subseteq \Delta(\mathcal{F})$.

*Theorem 36:* Suppose $\mathcal{F} \subset V(E)$ and suppose that $\mathcal{G} \subset \mathbb{F}[\boldsymbol{x}] \backslash V(E)$ is a witness set for the delta set $\Delta(\mathcal{F})$. Then $\Delta(\mathcal{F}) = \Delta(V(E))$, which implies that $\mathcal{F}$ is a Gröbner basis for the ideal $V(E)$.

*Proof:* The proof is the same as the proof of Theorem 35.

The basic data used by Sakata's algorithm is a pair of sets $\mathcal{F}$ and $\mathcal{G}$, where $\mathcal{F}$ is a minimal polynomial set, and $\mathcal{G}$ is a witness set. A single iteration in Sakata's algorithm takes a minimal polynomial set $\mathcal{F}$ for the set $V_{\boldsymbol{u}}(E)$ and a witness set $\mathcal{G}$ for the delta set $\Delta(V_{\boldsymbol{u}}(E))$ and produces a minimal polynomial set $\mathcal{F}^+$ for the set $V_{\boldsymbol{u}^+}(E)$ and a witness set $\mathcal{G}^+$ for the delta set $\Delta(V_{\boldsymbol{u}}(E))$. Note that the output is just an updated version of the input, so the algorithm in Fig. 1 can be iterated. In fact, in Fig. 1 we have actually extracted the inner loop of the algorithm originally presented by Sakata.

Sakata's algorithm (Fig. 1) breaks down into three stages. In the first stage (lines 1–4), the polynomials in the set $\mathcal{F}$, which are known to give valid $m$-dimensional linear recursion relations for all entries of the array up to entry $E_{\mathbf{u}}$, are tested for validity at the next entry $E_{\mathbf{u}^+}$. Any polynomial which fails to be valid for the next entry $E_{\mathbf{u}^+}$ may be used as a witness, and these new witnesses are collected in the set $\mathcal{N}$.

In the second stage (lines 5–8 of Fig. 1), the excluded point set $\Delta = \Delta(V_{\boldsymbol{u}}(E))$ is updated using the new witnesses from the set $\mathcal{N}$. The updated delta set $\Delta^+$ consists of the original delta set $\Delta$ of excluded points witnessed by the polynomials in the set $\mathcal{G}$, along with any new excluded points which have been discovered by the new witnesses. It should be noted that it frequently occurs that one or more of the new witnesses $f(\boldsymbol{x}) \in \mathcal{N}$ is a witness to a excluded point Span $(f)$ which is already in the delta set $\Delta$. Furthermore, the operation of appending a new excluded point $\boldsymbol{r}$ to the delta set $\Delta$ must take into account that all points $\boldsymbol{s} \leq \boldsymbol{r}$ must be appended to the delta set as well, so that the updated set $\Delta^+$ is also a delta set.

By the end of the second stage, an updated witness set $\mathcal{G}^+$ has been constructed which is a witness set for the updated delta set $\Delta^+$. The third stage (lines 9–29 of Fig. 1) consists of computing an updated set $\mathcal{F}^+$ of polynomials which are valid for the $m$-dimensional array up to entry $E_{\mathbf{u}^+}$: $\mathcal{F}^+ \subset V_{\mathbf{u}^+}(E)$, and for which $\Delta(\mathcal{F}^+) = \Delta^+$. Once this is done, it follows

**Input:**

$E$, an $m$-D array,
$\mathbf{u}$, an index $\mathbf{u} \in \mathbb{Z}_+^m$,
$\mathcal{F}$, a minimal polynomial set for $V_{\mathbf{u}}(E)$,
$\mathcal{G}$, a witness set for $V_{\mathbf{u}}(E)$

**Output:**

$\mathcal{F}^+$, a minimal polynomial set for $V_{\mathbf{u}+}(E)$,
$\mathcal{G}^+$, a witness set for $V_{\mathbf{u}+}(E)$

1 Let $\mathcal{F}' = \{ f \in \mathcal{F} : \text{lead}(f) \leq \mathbf{u}^+ \}$
2 for each $f \in \mathcal{F}'$, do
3 Compute $P_{\mathbf{u}+}(f) = \frac{-1}{\text{lc}(f)} \sum_{\mathbf{p} <_T \mathbf{u}^+} f_{\text{lead}(f)-\mathbf{u}^+ + \mathbf{p}} E_{\mathbf{p}}$
4 Let $\mathcal{N} = \{ f \in \mathcal{F}' : P_{\mathbf{u}+}(f) \neq E_{\mathbf{u}+} \}$
5 Let $\mathcal{G}^+ = \mathcal{G} \cup \mathcal{N}$
6 Let $\Delta^+ = \text{Span}(\mathcal{G}^+)$
7 for each $f \in \mathcal{N}$, do
8 Compute $\delta_f = \text{lc}(f)\,[E_{\mathbf{u}+} - P_{\mathbf{u}+}(f)]$
9 for each $\mathbf{s} \in \text{Ext}\,\Delta^+$, do
10 begin
11 if there exists $f \in \mathcal{F} \setminus \mathcal{N}$ with $\text{lead}(f) = \mathbf{s}$,
12 then
13 Let $h^{(\mathbf{s})}(\mathbf{x}) = f(\mathbf{x})$
14 elseif $\mathbf{s} \not\leq \mathbf{u}^+$,
15 then
16 begin
17 Find $f \in \mathcal{N}$ with $\text{lead}(f) \leq \mathbf{s}$
18 Let $h^{(\mathbf{s})}(\mathbf{x}) = \mathbf{x}^{\mathbf{s}-\text{lead}(f)} f(\mathbf{x})$
19 end
20 else
21 begin
22 Find $f \in \mathcal{N}$ with $\text{lead}(f) \leq \mathbf{s}$,
23 Find $g \in \mathcal{G}$ with $\text{Span}(g) \geq \mathbf{u}^+ - \mathbf{s}$,
24 Let $\mathbf{q} = \mathbf{s} - \text{lead}(f)$
25 Let $\mathbf{p} = \text{Span}(g) - \mathbf{u}^+ + \mathbf{s}$
26 Let $h^{(\mathbf{s})}(\mathbf{x}) = \mathbf{x}^{\mathbf{q}} f(\mathbf{x}) - \left(\frac{\delta_f}{\delta_g}\right) \mathbf{x}^{\mathbf{p}} g(\mathbf{x})$
27 end
28 end
29 Let $\mathcal{F}^+ = \{ h^{(\mathbf{s})}(\mathbf{x}) : \mathbf{s} \in \text{Ext}\,\Delta^+ \}$

Fig. 1. Sakata's algorithm.

TABLE I
OUTPUT OF SAKATA'S AGORITHM

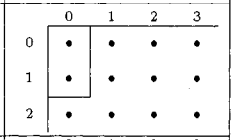
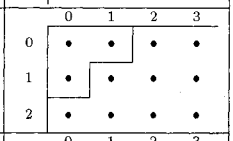
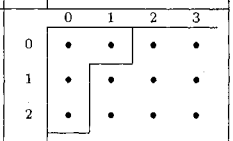
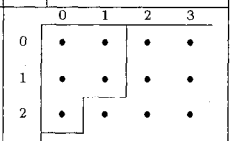
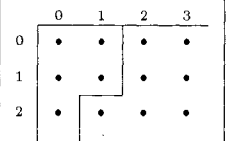
| $(i,j)$ | $4i+5j$ | $\mathcal{F}$ | $\mathcal{G}$ | $\Delta$ |
|---|---|---|---|---|
| (0,0) | 0 | $\{f_0\}$ | $\emptyset$ | $\emptyset$ |
| (1,0) | 4 | $\{f_1, f_2\}$ | $\{f_0\}$ |  |
| (0,1) | 5 | $\{f_3, f_2\}$ | | |
| (2,0) | 8 | $\{f_3, f_4\}$ | | |
| (1,1) | 9 | $\{f_5, f_4\}$ | | |
| (0,2) | 10 | $\{f_6, f_7, f_4\}$ | $\{f_5, f_0\}$ |  |
| (3,0) | 12 | $\{f_6, f_7, f_8\}$ | | |
| (2,1) | 13 | $\{f_6, f_9, f_{10}\}$ | | |
| (1,2) | 14 | $\{f_{11}, f_{12}, f_{10}\}$ | | |
| (0,3) | 15 | $\{f_{13}, f_{12}, f_{10}\}$ | | |
| (4,0) | 16 | $\{f_{13}, f_{12}, f_{14}\}$ | $\{f_5, f_{10}\}$ |  |
| (3,1) | 17 | $\{f_{13}, f_{15}, f_{16}\}$ | | |
| (2,2) | 18 | $\{f_{13}, f_{17}, f_{16}\}$ | $\{f_{15}, f_{10}\}$ |  |
| (1,3) | 19 | $\{f_{18}, f_{17}, f_{16}\}$ | | |
| (5,0) | 20 | $\{f_{18}, f_{17}, f_{19}\}$ | | |
| (0,4) | 20 | $\{f_{18}, f_{17}, f_{19}\}$ | | |
| (4,1) | 21 | $\{f_{18}, f_{20}, f_{21}\}$ | | |
| (3,2) | 22 | $\{f_{18}, f_{22}, f_{21}\}$ | | |
| (2,3) | 23 | $\{f_{18}, f_{22}, f_{21}\}$ | | |
| (6,0) | 24 | $\{f_{18}, f_{22}, f_{23}\}$ | $\{f_{15}, f_{21}\}$ |  |
| (1,4) | 24 | $\{f_{18}, f_{22}, f_{23}\}$ | | |
| (5,1) | 25 | $\{f_{18}, f_{24}, f_{25}\}$ | | |
| (0,5) | 25 | $\{f_{18}, f_{24}, f_{25}\}$ | | |
| (4,2) | 26 | $\{f_{18}, f_{24}, f_{25}\}$ | | |
| (3,3) | 27 | $\{f_{18}, f_{24}, f_{25}\}$ | | |
| (7,0) | 28 | $\{f_{18}, f_{24}, f_{26}\}$ | | |
| (2,4) | 28 | $\{f_{18}, f_{24}, f_{26}\}$ | | |
| (6,1) | 29 | $\{f_{18}, f_{24}, f_{26}\}$ | | |
| (1,5) | 29 | $\{f_{18}, f_{24}, f_{26}\}$ | | |
| ⋮ | ⋮ | ⋮ | | |

TABLE II
POLYNOMIALS USED IN THE OUTPUT OF SAKATA'S ALGORITHM

$$
\begin{aligned}
f_0(x,y) &= 1\\
f_1(x,y) &= y\\
f_2(x,y) &= x^2\\
f_3(x,y) &= y+\alpha^9x\\
f_4(x,y) &= x^2+\alpha^3x\\
f_5(x,y) &= y+\alpha^9x+\alpha^4\\
f_6(x,y) &= y^2+\alpha^9xy+\alpha^4y+\alpha^2x\\
f_7(x,y) &= xy+\alpha^9x^2+\alpha^4x\\
f_8(x,y) &= x^2+\alpha^3x+\alpha^{12}\\
f_9(x,y) &= xy+\alpha^9x^2+\alpha^4x+1\\
f_{10}(x,y) &= x^2+\alpha^{13}y+\alpha^4x+\alpha^7\\
f_{11}(x,y) &= y^2+\alpha^9xy+\alpha^4y+\alpha^2x+\alpha^{14}\\
f_{12}(x,y) &= xy+\alpha^9x^2+\alpha^6y+\alpha x+\alpha^5\\
f_{13}(x,y) &= y^2+\alpha^9xy+\alpha^6y+\alpha^3x+\alpha^7\\
f_{14}(x,y) &= x^3+\alpha^{13}xy+\alpha^4x^2+\alpha^7x+\alpha^{10}\\
f_{15}(x,y) &= xy+\alpha^{11}x^2+\alpha^{13}y+\alpha^{11}x+\alpha^6\\
f_{16}(x,y) &= x^3+\alpha^{13}xy+\alpha^4x^2+\alpha^{10}y+\alpha^3x+\alpha^{11}\\
f_{17}(x,y) &= x^2y+\alpha^{11}x^3+\alpha^{13}xy+\alpha^{11}x^2+\alpha^3y+\alpha^4x+\alpha^7\\
f_{18}(x,y) &= y^2+\alpha^{10}xy+\alpha^9x^2+\alpha y+\alpha x+\alpha^3\\
f_{19}(x,y) &= x^3+\alpha^{13}xy+\alpha^8x^2+\alpha^{12}y+\alpha x+1\\
f_{20}(x,y) &= x^2y+\alpha^{11}x^3+\alpha^{13}xy+\alpha^7x^2+\alpha^2y+\alpha^6x+\alpha^9\\
f_{21}(x,y) &= x^3+\alpha^{12}x^2+y+\alpha^3x+\alpha\\
f_{22}(x,y) &= x^2y+\alpha^{11}x^3+\alpha^5xy+\alpha^4x^2+\alpha y+\alpha^2x+\alpha^{10}\\
f_{23}(x,y) &= x^4+\alpha^{12}x^3+xy+\alpha^{13}x^2+\alpha^6y+\alpha^{13}x+1\\
f_{24}(x,y) &= x^2y+\alpha x^3+\alpha^5xy+\alpha^7x^2+\alpha^{11}y+\alpha^{11}x+\alpha^6\\
f_{25}(x,y) &= x^4+\alpha^{12}x^3+\alpha xy+\alpha^6x^2+\alpha^3y+\alpha^6x+\alpha^5\\
f_{26}(x,y) &= x^4+\alpha^4x^3+\alpha xy+\alpha^2x^2+\alpha^2y+\alpha^5x+\alpha^{13}
\end{aligned}
$$

from Theorem 35 that $\mathcal{F}^+$ is a minimal polynomial set for $V_{\boldsymbol{u}^+}(E)$, and that $\mathcal{G}^+$ is a witness set for $\Delta(V_{\boldsymbol{u}^+}(E))$.

In order to satisfy the condition $\Delta(\mathcal{F}^+) = \Delta^+$, polynomials $h^{(\boldsymbol{s})}(\boldsymbol{x})$ are computed whose leading monomials are the exterior corners $\boldsymbol{s}$ of the delta set $\Delta^+$. Therefore, in order to prove the correctness of the algorithm, we need to prove the following lemma:

*Lemma 37:* Each polynomial $h^{(\boldsymbol{s})}(\boldsymbol{x})$ computed in lines 9–28 of Fig. 1 satisfies

$$\text{lead}\,(h^{(\boldsymbol{s})}) = \boldsymbol{s}$$

$$h^{(\boldsymbol{s})}(\boldsymbol{x}) \in V_{\boldsymbol{u}^+}(E).$$

*Proof:* See Appendix II. ∎

*Example 9:* Table I lists the output of Sakata's algorithm when it is applied to the syndrome array given in (5). Each row of Table I is labeled with a pair $(i, j)$ corresponding to an entry $E_{i,j}$ in the syndrome array. The syndromes are ordered according to their weighted degree $4i + 5j$, and when the weighted degrees are the same, they are ordered by the largest value of $j$. For each $(i, j)$, Table I lists a minimal polynomial set $\mathcal{F}$ and a witness set $\mathcal{G}$ for the delta set $\Delta = \Delta(V_{i,j}(E))$. (In some cases, the same witness set $\mathcal{G}$ and delta set $\Delta$ applies to several rows of Table I.) The polynomials $f_k(x, y)$ referred to in Table I are listed in Table II.

To illustrate, consider entry $(3, 1)$ of Table I. The table indicates that the set $\mathcal{F} = \{f_{13}, f_{15}, f_{16}\}$ is a minimal polynomial set for the delta set $\Delta(V_{3,1}(E))$. In other words, these three polynomials represent two-dimensional linear recursion relations which are valid for the syndrome array $E$ for all entries up to $E_{3,1}$, and their leading terms, $y^2$, $xy$, and $x^3$, respectively, correspond to the exterior corners $(0, 2)$, $(1, 1)$, and $(3, 0)$ of the delta set $\Delta(V_{3,1}(E))$. A witness set for the delta set $\Delta(V_{3,1}(E))$ is listed as $\mathcal{G} = \{f_5, f_{10}\}$. Thus the polynomials $f_5(x, y)$ and $f_{10}(x, y)$ represent two-dimensional linear recursion relations which have failed to be valid at some entry of the syndrome array preceding $E_{3,1}$, and they satisfy $\text{Span}\,(f_5) = (0, 1)$ and $\text{Span}\,(f_{10}) = (2, 0)$, corresponding to the interior corners $(0, 1)$ and $(2, 0)$ of the delta set $\Delta(V_{3,1}(E))$.

The successor to $\boldsymbol{u} = (3, 1)$ in the monomial order $\leq_\circ$ is $\boldsymbol{u}^+ = (2, 2)$, and Sakata's algorithm is applied to find $\mathcal{F}^+$ and $\mathcal{G}^+$. Since $\text{lead}\,(f_{16}) = (3, 0) \not\leq (2, 2)$, it is not possible to predict the value of $E_{2,2}$ using the two-dimensional linear recursion defined by the polynomial $f_{16}$, and so this two-dimensional linear recursion relation is (by definition) valid for all entries up to $(2, 2)$. The recursion relation defined by $f_{13}$ predicts that $E_{2,2} = 1$, and the recursion relation defined by $f_{15}$ predicts that $E_{2,2} = \alpha^8$. The true value of $E_{2,2}$ is 1, and thus

$$\mathcal{N} = \{f_{15}\}, \quad \mathcal{G}^+ = \{f_5, f_{10}, f_{15}\}$$

$$\text{Span}\,(f_{15}) = (2, 2) - (1, 1) = (1, 1)$$

and

$$\Delta^+ = \Delta \cup \{(1, 1)\}.$$

(Note that $f_{15}(x, y)$ is the same as the polynomial $g(x, y)$ considered in Example 8.) Since the polynomial $f_{15}$ is a witness for the point $(1, 1)$, the polynomial $f_5$, which was a witness for the point $(0, 1)$, may be discarded from the set

```
1  begin
2    Initialize:  u = 0, F = {1}, G = ∅
3    Repeat :
4      if syndrome E_u is unknown,
5        Compute E_u (SYNDROME EXTENSION)
6      Run Sakata's algorithm to obtain (F+, G+)
7      Update:
8        F ← F+
9        G ← G+
10       u ← u+, according to MONOMIAL ORDER
11   until TERMINATION CRITERIA are satisfied
12 end
```

Fig. 2. General decoding algorithm.

$\mathcal{G}^+$. The exterior corners of $\Delta^+$ are $(0, 2)$, $(2, 1)$, and $(3, 0)$, and so we must find polynomials with leading terms $y^2$, $x^2y$, and $x^3$, respectively, which give relations valid for all entries up to $(2, 2)$. Since the polynomials $f_{13}$ and $f_{16}$ are valid up to $(2, 2)$, we need only find a polynomial $f_{17}(x, y)$ with leading term $x^2y$. Using the computation described in line 26 of Fig. 1, we find

$$\begin{aligned} f_{17} &= xf_{15}(x, y) + (\delta_{15}/\delta_5)f_5(x, y) \\ &= xf_{15}(x, y) + \alpha^3 f_5(x, y) \\ &= x^2y + \alpha^{11}x^3 + \alpha^{13}xy + \alpha^{11}x^2 + \alpha^3 y + \alpha^4 x + \alpha^7. \end{aligned}$$

Thus we have a minimal polynomial set $\mathcal{F}^+ = \{f_{13}, f_{17}, f_{16}\}$ and a witness set $\mathcal{G}^+ = \{f_{15}, f_{10}\}$ for the delta set $\Delta(V_{2,2}(E))$, as listed in Table I.

## IX. Decoding Methods

In the decoding problem for a cross section of an extended multidimensional cyclic code, we have seen that the error locations correspond to the zeros of an error locator ideal $V(E)$ and that Sakata's algorithm may be used to determine $V(E)$. However, the use of Sakata's algorithm requires full knowledge of each syndrome, and in the decoding problem, some of the syndromes are unknown. Therefore, decoding algorithms which have been developed for multidimensional cyclic codes [19], [20] and algebraic-geometric codes [30]–[32] have had to rely on a supplementary procedure for computing the values of additional syndromes.

In this section, we look at the general decoding problem for cross sections of extended multidimensional cyclic codes, and consider the issues which must be addressed in order to create a decoding algorithm for a specific code. Fig. 2 shows a template which may be used to describe a general decoding algorithm for cross sections of extended mutidimensional cyclic codes. In order to obtain a concrete algorithm from this template, one needs to specify which monomial order is used, what syndrome extension rule is used, and what termination criteria are used. We show how the known decoding algorithms for multidimensional cyclic codes [19], [20] and algebraic-geometric codes [30]–[32] can be fit into this template.

We have defined a broad class of codes $\mathcal{C}^{\perp}(\mathcal{P}, \mathcal{L}(M))$, defined by an arbitrary collection $\mathcal{P}$ of points, and an arbitrary collection $M$ of monomials, but aside from the two examples of HCRS codes and algebraic-geometric codes, we do not know how to determine, or design, the minimum distance of a general code in this class. If, in the future, other codes of the form $\mathcal{C}^{\perp}(\mathcal{P}, \mathcal{L}(M))$ are designed, then the template in Fig. 2 may be useful in creating a decoding algorithm for these codes. Another possible avenue for exploration is to invent a specific decoding method based on the template, and then try to determine how the code must be designed to fit the decoding method.

Whether or not the template decoding algorithm has any future application, it at least serves to make a comparison of the known decoding algorithms for HCRS codes and algebraic-geometric codes. The most prominent feature in these algorithms has been the use of a syndrome extension method which in both cases led to a significant improvement in the error-correcting capability over previously known algorithms. These syndrome extension methods operate according to the same principles: when an unknown syndrome is encountered, the algorithm makes a "guess" at its value, and proceeds as if the syndrome were known to have that value. At some later point in the algorithm, it becomes apparent if the guess was correct or not, and if it was incorrect, the decoding algorithm reverts back to the point at which the guess was made, and tries another guess in its place. If this is to be an efficient procedure, we must ensure that the candidate values for the unknown syndrome may be chosen from a fairly short list, and that the correctness of the candidate value may be decided fairly quickly. As we shall see, the known decoding algorithms for algebraic-geometric codes and HCRS codes succeed on both of these counts.

A Hyperbolic Cascaded Reed–Solomon code is a multidimensional cyclic code of the form $\mathrm{Cyc}(H_d)$ where $H_d$ is the set defined in Example 2. In the decoding algorithm for HCRS codes, any monomial order $\leq_T$ may be used to govern the iterations of Sakata's algorithm. The pure lexicographic order is an interesting choice because it gives detailed information on the configuration of the error, and facilitates solving for the error locations. In [19]–[21], it is shown that syndrome extension may be performed by the procedure shown in Fig. 3. The resulting decoding algorithm is able to correct all error patterns of weight $t$ or less for the HCRS code $\mathrm{Cyc}(H_{2t+1})$.

In order to use the algorithm of Fig. 2 for an algebraic-geometric code $C_\Omega(D, aQ)$, the curve $X$ must be put into special position with respect to $Q$. The monomial order used must be the weighted-degree monomial order $\leq_\circ$ (as defined in Theorem 12), induced by the orders of the coordinate functions. Whenever an unknown syndrome $E_{\boldsymbol{r}}$ is encountered, the syndrome must be considered as part of a *block* of syndroimes, defined by monomials $\boldsymbol{x}^{\boldsymbol{s}}$ of the same weighted degree

$$B = \left\{ E_{\boldsymbol{s}} : \quad \sum_{i=1}^{m} s_i o_i = \sum_{i=1}^{m} r_i o_i \right\}.$$

Recall that the polynomials in the ideal $\boldsymbol{I}(\mathcal{P})$ give $m$-dimensional linear recursion relations which are automatically

```
1  begin
2    for each f(x) ∈ F,
3      begin
4        Compute the predicted value P_{u+}(f)
5      end
6    Let V = { P_{u+} : f ∈ F }
7    for each candidate value v ∈ V,
8      begin
9        Assume that E_{u+} = v
10       Run Sakata's algorithm for a single iteration
11       if |Δ+| > t,
12         reject the candidate value v
13       if |Δ+| ≤ t,
14         accept the candidate value v,
15         (and reject any remaining candidates)
16     end
17 end
```

Fig. 3. Syndrome extension for HCRS codes.

```
1  begin
2    Form a block B of unknown syndromes
3    for each f(x) ∈ F,
4      for each r ∈ B,
5        begin
6          Compute P_r(f)
7          Extend to a predicted block
8        end
9    for each candidate block
10     begin
11       Run Sakata's algorithm
12         until the end of the block B
13       if |Δ+| > t,
14         reject the candidate block
15       if |Δ+| ≤ t,
16         accept the candidate block
17         (and reject any remaining candidates)
18     end
19 end
```

Fig. 4. Syndrome extension for algebraic-geometric codes.

satisfied by any transform array. It can be shown that these linear recursion relations can be used to determine any syndrome within a block $B$ from any other syndrome in the same block, assuming all syndromes previous to the block are known. Thus the assignment of a candidate value to a single syndrome in the block $B$ implies a unique assignment of the other syndromes in the block, resulting in a candidate block. This leads to the syndrome extension scheme shown in Fig. 4, which is based on the original idea of Feng and Rao [30], [32]. The resulting decoding algorithm is able to correct all error patterns of weight $t$ or less for the algebraic-geometric code $C_\Omega(D, aQ)$ with designed distance at least $2t + 1$.

We consider the case of bounded distance decoding, in which the decoder is only required to correct errors of Hamming weight less than a given parameter $t$. In the course of Sakata's algorithm, the delta set $\Delta = \Delta(V_{\mathbf{u}}(E))$ grows until its cardinality is equal to the Hamming weight of the error word (Theorem 27). Thus if the assignment of a candidate value to an unknown syndrome leads to growth of the delta set $\Delta$ so that its cardinality exceeds $t$, it may be concluded that either the candidate value is incorrect, or the error pattern has weight exceeding $t$, and is therefore considered undecodable. This makes it clear that the procedures in Figs. 3 and 4 perform correctly when they decide to reject certain candidates. The real issue is the correctness of their decisions to accept certain candidates. The reader should consult the original references ([19]–[21] for HCRS codes, and [30], [32] for algebraic-geometric codes) for proofs of the validity of these syndrome extension rules.

In the decoding of HCRS codes (Fig. 3), it can be shown that any incorrect candidate value for the unknown syndrome can be rejected, in the manner described above, on the next iteration of Sakata's algorithm. This means that a candidate value may be accepted as the true value of the unknown syndrome if the delta set $\Delta$ does not grow to a size exceeding $t$ on the next iteration. In the decoding of algebraic-geometric codes (Fig. 4), it is known that any incorrect candidate value for the unknown syndrome will be rejected within a fixed number of iterations, corresponding to a block of unknown syndromes. Therefore, a candidate value may be accepted as the true value of the unknown syndrome if after the specified number of iterations, the size of the delta set still does not exceed $t$.

The choice of termination criteria in Fig. 2 depends on a choice between two strategies for performing the overall decoding. One decoding strategy is for the decoder to fill in syndromes until the proper transform has been completed. Then the inverse transform may be applied, yielding the error word itself. A second strategy is to perform the syndrome decoding algorithm until we are certain that $\mathcal{F}$ is a Gröbner basis for the error locator ideal $V(E)$. At this point, the error locations are found by solving for the common zeros of the polynomials in $\mathcal{F}$, and the error values are found by interpolation.

*Example 10:* We continue the decoding example with the syndrome array in (5) for a Hermitian code $C_\Omega(D, 23Q)$, which is capable of correcting any pattern of six or fewer errors. The last known entry of the syndrome array is $E_{2,3}$, and after processing this syndrome the decoder has produced a minimal polynomial set $\mathcal{F} = \{f_{18}, f_{22}, f_{21}\}$, and a witness set $\mathcal{G} = \{f_{15}, f_{21}\}$, for $V_{2,3}(E)$, as listed in Table I. Next, the decoder encounters the unknown syndrome $E_{6,0}$. This unknown syndrome must be processed as part of a block of syndromes of order 24

$$B = \{(6, 0), (1, 4)\}.$$

The two-dimensional linear recursion relation represented by $f_{21}$ predicts that $E_{6,0} = \alpha^{13}$, and the two-dimensional linear recursion relation represented by $f_{18}$ predicts that $E_{1,4} = \alpha^2$. According to the two-dimensional linear recursion relation represented by the polynomial $y^4 - x^5 - y$, the relation

$$E_{1,4} - E_{6,0} - E_{1,1} = 0$$

is satisfied by every syndrome array, and so either of the two unknown syndromes in the block $B$ is determined by the other. Thus the values for the two unknown syndromes may be extended to two *predicted blocks* $B_1$ and $B_2$: these are predictions for the simultaneous values of the entire block $B$ of syndromes.

$$B_1: \quad (E_{6,0} = \alpha^{13},\ E_{1,4} = \alpha^8)$$

$$B_2: \quad (E_{6,0} = \alpha^{6},\ E_{1,4} = \alpha^2).$$

Assume that the first candidate block $B_1$ is correct, and continue Sakata's algorithm. Under this assumption, the two-dimensional linear recursion relation represented by $f_{21}$ remains valid at the syndrome $E_{6,0}$, so no change takes place on the first iteration. Proceeding to syndrome $E_{1,4}$, we find that according to our assumption, the two-dimensional linear recursion relation represented by $f_{18}$ is invalid at $(1, 4)$, and so the point $\mathrm{Span}(f_{18}) = (1, 2)$ must be appended to $\Delta$, and $(0, 2)$ must be appended as well (to make a well-formed delta set). Hence, $\Delta$ will have seven elements. Since we assume that no more than six errors have occurred, we reject this candidate block. Return to syndrome $E_{6,0}$ and consider the other candidate block $B_2$ instead. Now, the two-dimensional linear recursion relation represented by $f_{21}$ is invalid at $(6, 0)$, and so the point $\mathrm{Span}(f_{21}) = (3, 0)$ must be appended to $\Delta$. The new minimal polynomial set is then $\mathcal{F}^+ = \{f_{18}, f_{22}, f_{23}\}$, where

$$\begin{aligned} f_{23} &= xf_{21} + \alpha^8 f_{21} \\ &= x^4 + \alpha^{12}x^3 + xy + \alpha^{13}x^2 + \alpha^6 y + \alpha^{13}x + 1 \end{aligned}$$

and the new witness set is $\mathcal{G}^+ = \{f_{15}, f_{21}\}$. Proceeding to syndrome $E_{1,4}$, we find that the two-dimensional linear recursion relation represented by $f_{18}$ remains valid at the syndrome $E_{1,4}$, so no change takes place on this iteration. The code $C_\Omega(D, 23Q)$ is capable of correcting six errors, and the delta set $\Delta$ has six points upon completion of the block $B$, so according to the syndrome extension rule (Fig. 4, the predicted block $B_2$ is accepted and the values $E_{6,0} = \alpha^6$ and $E_{1,4} = \alpha^2$ are assigned to the unknown syndromes.

All further syndromes must be computed in the same way, by using predicted values, and deciding the correct candidate based on the size of the delta set. After a few more iterations, the minimal polynomial set converges to a Gröbner basis for the error locator ideal $V(E)$. This Gröbner basis is given by the set $\mathcal{F} = \{f_{18}, f_{24}, f_{26}\}$, where

$$\begin{aligned} f_{18} &= y^2 + \alpha^{10}xy + \alpha^9 x^2 + \alpha y + \alpha x + \alpha^3 \\ f_{24} &= x^2 y + \alpha x^3 + \alpha^5 xy + \alpha^7 x^2 + \alpha^{11} y + \alpha^{11} x + \alpha^6 \\ f_{26} &= x^4 + \alpha^4 x^3 + \alpha xy + \alpha^2 x^2 + \alpha^2 y + \alpha^5 x + \alpha^{13}. \end{aligned}$$

In principle, the six error locations may be found as the common roots of these three polynomials. In practice, however, it may be more efficient to continue generating syndromes until it becomes possible to apply an inverse transform.

## Appendix I
## Proof of Theorem 15

*Theorem 15:* Let $X$ be a smooth projective curve, let $Q$ be a point on $X$, and let $N(Q)$ be the set of nongaps for $Q$. Assume that we have a set of integers $\{o_1, \cdots, o_m\}$, $0 < o_1 < o_2 < \cdots < o_m$, which generates $N(Q)$ as a semigroup, and rational functions $\phi_i \in L(o_m Q)$ such that the pole order of $\phi_i$ at $Q$ is exactly $o_i$, for each $i = 1, \cdots, m$. Define the map from $X \backslash \{Q\}$ to $\mathbb{F}_q^m$

$$P \mapsto (\phi_1(P), \cdots, \phi_m(P)).$$

Let $X'_a$ be the image of $X$ under this map, and let $X' \subset \mathbb{P}^m$ be the projective closure of the affine curve $X'_a$.

1) The map $P \mapsto (\phi_1(P), \cdots, \phi_m(P))$ extends to a birational isomorphism of $X$ and $X'$.

*Proof:* For a function $\phi$, write its divisor as $(\phi) = (\phi)_0 - (\phi)_\infty$ where $(\phi)_0$, the divisor of zeros, and $(\phi)_\infty$, the divisor of poles, are effective divisors. On the set $U_1 = X \backslash Q$, we map

$$P \mapsto P' = (1: \quad \phi_1(P) : \cdots : \phi_m(P)).$$

On the set $U_2 = X \backslash (\phi_m)_0$, we map

$$P \mapsto P' = (1/\phi_m(P): \quad \phi_1(P)/\phi_m(P) : \cdots : 1).$$

The two maps are consistent on $U_1 \cap U_2$, and $Q$ is mapped to the point $Q' = (0 : 0 : \cdots : 1)$. Thus the map extends to a map on all of $X$.

Let $L(\infty Q)$ be the set of all rational functions on $X$ with poles only at $Q$

$$L(\infty Q) = \bigcup_{a=0}^{\infty} L(aQ).$$

Since $L(\infty Q)$ is closed under sums and products, it is a subring of the field of rational functions $\mathbb{F}_q(X)$. We show that the field of fractions of $L(\infty Q)$ is the function field $\mathbb{F}_q(X)$. Suppose $\phi \in \mathbb{F}_q(X)$. Riemann's theorem (Theorem 5) implies that for $a$ sufficiently large, $L(aQ - (\phi)_\infty)$ is nonempty. Thus there is a function $\psi \in L(aQ)$ with $(\psi)_0 \geq (\phi)_\infty$. Let $\chi = \psi\phi$. Then $\chi$ has poles only at $Q$, and hence $\chi \in L(\infty Q)$. This shows that the original function $\phi$ was a fraction $\phi = \chi/\psi$.

Now we show that $X \to X'$ is a birational isomorphism by showing that their function fields are isomorphic: $\mathbb{F}_q(X) \cong \mathbb{F}_q(X')$. Since $\dim L(aQ) \leq 1 + \dim L((a-1)Q)$ for each $a$, we see (by induction) that a basis for $L(aQ)$ is obtained by choosing, for each nongap $j \leq a$, a rational function $\chi_j \in L(jQ)$ whose pole order at $Q$ is exactly $j$. Since the $o_i$ generate $N(Q)$ as a semigroup, each nongap $j$ is obtained as the sum $j = \Sigma r_i o_i$ for some $\boldsymbol{r} \in \mathbb{Z}_+^m$, and hence the "monomial" $\phi^{\boldsymbol{r}} = \phi_1^{r_1} \cdots \phi_m^{r_m}$ can be taken as the function $\chi_j$. Thus certain monomials in the $\phi_i$ form a basis for $L(aQ)$, and hence any function in $L(aQ)$ is a polynomial

in the $\phi_i$. Since $a$ is arbitrary, every function $\phi \in L(\infty Q)$ can be expressed as a polynomial in the $\phi_i$. Define a ring homomorphism $\sigma$: $\mathbb{F}_q[y_1, \cdots, y_m] \to L(\infty Q)$ which maps $y_1 \mapsto \phi_1, \cdots, y_m \mapsto \phi_m$. Then the above argument shows that $\sigma$ is surjective.

Now suppose that a polynomial $f(y_1, \cdots, y_m)$ is in the kernel of the map $\sigma$. Then $f(\phi_1, \cdots, \phi_m)$ is a function in $\mathbb{F}_q(X)$ which is equivalent to the zero function, and thus for any point $P' \in X'_a$, $f(P') = 0$. Hence $f \in \boldsymbol{I}(X'_a)$. Conversely, if $f \in \boldsymbol{I}(X'_a)$, then $f(\phi_1, \cdots, \phi_m)$ is a function in $\mathbb{F}_q(X)$ which vanishes at every point (rational or otherwise) of $X \backslash \{Q\}$. The only rational function which can vanish on an infinite set of points is the zero function, so $f$ is in the kernel of $\sigma$. This shows that the kernel of the map $\sigma$ is the ideal $\boldsymbol{I}(X'_a)$.

Thus $L(\infty Q)$ is isomorphic to the quotient ring $\mathbb{F}_q[\boldsymbol{y}]/\boldsymbol{I}(X'_a)$. But this is in fact the coordinate ring $\mathbb{F}_q[X'_a]$. Since these two rings are isomorphic, their fields of fractions are isomorphic, proving that $\mathbb{F}_q(X) \cong \mathbb{F}_q(X')$. Thus $X \to X'$ is a birational isomorphism. ∎

2) The projective curve $X'$ is in special position with respect to the point $Q' \in X'$ which is the image of $Q$ under the extended map $X \to X'$.

*Proof:* By construction, $Q'$ is the unique point on the hyperplane at infinity. Note that since $X$ is a smooth curve, it is a nonsingular model of $X'$, and so the points of $X$ are the places of $X'$. Thus $Q$ is the only place centered at $Q'$. Also, the orders of the coordinate functions $y_1, \cdots, y_m$ are just the orders of the rational functions $\phi_i$, so they are distinct and ordered, and generate the semigroup $N(Q) = N(Q')$ of nongaps for the point $Q'$.

The only thing remaining to show is that the points $P'$ of $X'_a$ are nonsingular. To do this, we show that the local ring $\mathcal{O}_{P'}(X')$ is a discrete valuation ring, by showing that it is isomorphic to $\mathcal{O}_P(X)$, where $P$ is a place of $X$ centered at $P'$. The isomorphism between function fields maps a rational function

$$f(y_1, \cdots, y_m)/g(y_1, \cdots, y_m) \in \mathbb{F}_q(X'_a)$$

to a rational function

$$\phi = f(\phi_1, \cdots, \phi_m)/g(\phi_1, \cdots, \phi_m) \in \mathbb{F}_q(X).$$

If $f/g \in \mathcal{O}_{P'}(X')$, then we may assume that $g(P') \neq 0$, and hence $g(\phi_1(P), \cdots, \phi_m(P)) \neq 0$, and thus $\phi$ does not have a pole at $P$. Thus we have a (one-to-one) map from $\mathcal{O}_{P'}(X')$ to $\mathcal{O}_P(X)$.

Suppose now that $\phi$ is an arbitrary element of $\mathcal{O}_P(X)$. Consider its divisor $(\phi)_\infty$ of poles. If we choose $a$ large enough, Riemann's theorem implies that

$$\dim L(aQ - (\phi)_\infty) = 1 + \dim L(aQ - (\phi)_\infty - P)$$

and so there is a function $\psi \in L(\infty Q)$ with $(\psi)_0 \geq (\phi)_\infty$ and $\psi(P) \neq 0$. Now let $\chi = \psi\phi$. Then $\chi$ has poles only at $Q$, and so $\chi \in L(\infty Q)$. Since any element of $L(\infty Q)$ is a polynomial in the $\phi_i$, write

$$\psi = g(\phi_1, \cdots, \phi_m), \quad \chi = f(\phi_1, \cdots, \phi_m).$$

Then

$$g(P') = g(\phi_1(P), \cdots, \phi_m(P)) = \psi(P) \neq 0$$

and hence $f/g$ is an element of the local ring $\mathcal{O}_{P'}(X')$ which corresponds to the element $\chi/\psi = \phi$ of the local ring $\mathcal{O}_P(X)$. Thus we have shown that the two local rings are isomorphic, and hence $P'$ is nonsingular. This completes the proof that $X'$ is in special position with respect to $Q'$. ∎

3) The algebraic-geometric codes defined from $X$ and $X'$ are identical when a point $P \in X$ is identfied with its image $P' \in X'$. In particular

$$C_L(D', aQ') = C_L(D, aQ)$$
$$C_\Omega(D', aQ') = C_\Omega(D, aQ).$$

*Proof:* Any codeword in $C_L(D, aQ)$ is of the form

$$c = (\phi(P_1), \cdots, \phi(P_n))$$

for some $\phi \in L(aQ)$. But $\phi = f(\phi_1, \cdots, \phi_m)$ for some $f(y_1, \cdots, y_m)$, and $f \in L(aQ')$. Thus

$$c = (f(P'_1), \cdots, f(P'_n))$$

is a codeword in $C_L(D', aQ')$. Conversely, if $f \in L(aQ')$, then $\phi = f(\phi_1, \cdots, \phi_m) \in L(aQ)$, and so the codewords

$$c = (f(P'_1), \cdots, f(P'_n))$$

of $C_L(D', aQ')$ are codewords

$$c = (\phi(P_1), \cdots, \phi(P_n))$$

of $C_L(D, aQ)$. Since these two codes are the same, their dual codes are also the same. ∎

## Appendix II
## Verification of Sakata's Algorithm

*Theorem 30 (Agreement Theorem):* Suppose $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$ are valid up to all entries $\boldsymbol{q} <_T \boldsymbol{u}$, and suppose $\boldsymbol{u} \geq \text{lead}\,(f) + \text{lead}\,(g)$. Then $f$ and $g$ agree in their prediction for the value of $E_{\boldsymbol{u}}$

$$P_{\boldsymbol{u}}(f) = P_{\boldsymbol{u}}(g).$$

*Proof:* By changing variables, we may rewrite (10) as

$$P_{\boldsymbol{u}}(f) = \frac{-1}{\text{lc}\,(f)} \sum_{\boldsymbol{s} <_T \text{lead}\,(f)} f_{\boldsymbol{s}} E_{\boldsymbol{s}+\boldsymbol{u}-\text{lead}\,(f)}. \tag{11}$$

By hypothesis, $E_{\boldsymbol{q}} = P_{\boldsymbol{q}}(g)$, for $\text{lead}\,(g) \leq \boldsymbol{q} <_T \boldsymbol{u}$. Note that $\boldsymbol{u} - \text{lead}\,(f) \geq \text{lead}\,(g)$, and so whenever $\boldsymbol{s} <_T \text{lead}\,(f)$, it follows that $\boldsymbol{s} \leq (\boldsymbol{s} + \boldsymbol{u} - \text{lead}\,(f)) <_T \boldsymbol{u}$, and therefore $E_{\boldsymbol{s}+\boldsymbol{u}-\text{lead}\,(f)} = P_{\boldsymbol{s}+\boldsymbol{u}-\text{lead}\,(f)}(g)$. Thus we may apply (11) to obtain

$$\begin{aligned} P_{\boldsymbol{u}}(f) &= \frac{-1}{\text{lc}\,(f)} \sum_{\boldsymbol{s} <_T \text{lead}\,(f)} f_{\boldsymbol{s}} E_{\boldsymbol{s}+\boldsymbol{u}-\text{lead}\,(f)} \\ &= \frac{-1}{\text{lc}\,(f)} \sum_{\boldsymbol{s} <_T \text{lead}\,(f)} f_{\boldsymbol{s}} P_{\boldsymbol{s}+\boldsymbol{u}-\text{lead}\,(f)} \\ &= \frac{1}{\text{lc}\,(f)\,\text{lc}\,(g)} \\ &\quad \cdot \sum_{\boldsymbol{s} <_T \text{lead}\,(f)} f_{\boldsymbol{s}} \sum_{\boldsymbol{r} <_T \text{lead}\,(g)} g_{\boldsymbol{r}} E_{\boldsymbol{r}+(\boldsymbol{s}+\boldsymbol{u}-\text{lead}\,(f))-\text{lead}\,(g)}. \end{aligned}$$

By symmetry, the same expression must hold true when we reverse the roles of $f$ and $g$

$$P_{\boldsymbol{u}}(g) = \frac{1}{\mathrm{lc}\,(f)\,\mathrm{lc}\,(g)} \cdot \sum_{\boldsymbol{r} <_T \mathrm{lead}\,(g)} g_{\boldsymbol{r}} \sum_{\boldsymbol{s} <_T \mathrm{lead}\,(f)} f_{\boldsymbol{s}} E_{\boldsymbol{s}+(\boldsymbol{r}+\boldsymbol{u}-\mathrm{lead}\,(g))-\mathrm{lead}\,(f)}.$$

Careful examination of these two expressions shows that they are just rearrangements of the same sum, and so we have proved that $P_{\boldsymbol{u}}(f) = P_{\boldsymbol{u}}(g)$. ∎

*Theorem 32:* Suppose $g \notin V_{\boldsymbol{u}}(E)$. Then $\mathrm{Span}\,(g) \in \Delta(V_{\boldsymbol{u}}(E))$.

*Proof:* Let $\boldsymbol{r} = \mathrm{lead}\,(g) + \mathrm{Span}\,(g)$. Then the $m$-dimensional linear recursion relation represented by $g(\boldsymbol{x})$ is valid for all entries $E_{\boldsymbol{q}}$, for $\boldsymbol{q} <_T \boldsymbol{r}$, and is invalid at entry $E_{\boldsymbol{r}}$

$$P_{\boldsymbol{r}}(g) \neq E_{\boldsymbol{r}}. \tag{12}$$

Moreover, $\boldsymbol{r} <_T \boldsymbol{u}$, since the $m$-dimensional linear recursion relation represented by $g(\boldsymbol{x})$ is not valid for all entries up to $E_{\boldsymbol{u}}$. Suppose there exists a polynomial $f(\boldsymbol{x}) \in V_{\boldsymbol{u}}(E)$ with $\mathrm{lead}\,(f) = \mathrm{Span}\,(g)$. The $m$-dimensional linear recursion represented by the polynomial $f(\boldsymbol{x})$ is valid at entry $E_{\boldsymbol{r}}$, and so $P_{\boldsymbol{r}}(f) = E_{\boldsymbol{r}}$. Putting this together with (12), we find that $P_{\boldsymbol{r}}(f) \neq P_{\boldsymbol{r}}(g)$. On the other hand, the polynomials $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$ satisfy the hypotheses of the agreement theorem (Theorem 30), which implies that $P_{\boldsymbol{r}}(f) = P_{\boldsymbol{r}}(g)$, and so we have reached a contradiction. Thus there does not exist any polynomial $f(\boldsymbol{x}) \in V_{\boldsymbol{u}}(E)$ with $\mathrm{lead}\,(f) = \mathrm{Span}\,(g)$. ∎

*Lemma 37:* Each polynomial $h^{(\boldsymbol{s})}(\boldsymbol{x})$ computed in lines 9–28 of Fig. 1 satisfies

$$\mathrm{lead}\,(h^{(\boldsymbol{s})}) = \boldsymbol{s}$$

$$h^{(\boldsymbol{s})}(\boldsymbol{x}) \in V_{\boldsymbol{u}^+}(E).$$

*Proof:* The computations of the polynomials $h^{(\boldsymbol{s})}(\boldsymbol{x})$ in lines 9–28 break down into three mutually exclusive cases: In case a) (lines 11–13), there exists a polynomial $f(\boldsymbol{x}) \in \mathcal{F} \backslash \mathcal{N}$ with $\mathrm{lead}\,(f) = \boldsymbol{s}$. In case b) (lines 14–19) there does not exist a polynomial $f(\boldsymbol{x}) \in \mathcal{F} \backslash \mathcal{N}$ with $\mathrm{lead}\,(f) = \boldsymbol{s}$, and $\boldsymbol{s} \not\leq \boldsymbol{u}^+$. Finally, in case c) (lines 20–27) there does not exist a polynomial $f(\boldsymbol{x}) \in \mathcal{F} \backslash \mathcal{N}$ with $\mathrm{lead}\,(f) = \boldsymbol{s}$, and $\boldsymbol{s} \leq \boldsymbol{u}^+$.

*Case a):* The polynomial $h^{(\boldsymbol{s})}(\boldsymbol{x}) = f(\boldsymbol{x})$ has the required leading monomial $\mathrm{lead}\,(f) = \boldsymbol{s}$. The polynomial $f(\boldsymbol{x})$ is a member of $V_{\boldsymbol{u}}(E)$, so $f(\boldsymbol{x})$ represents an $m$-dimensional linear recursion relation which is valid for all entries up to $E_{\boldsymbol{u}}$. Moreover, the fact that $f(\boldsymbol{x}) \notin \mathcal{N}$ shows that the $m$-dimensional linear recursion relation represented by $f(\boldsymbol{x})$ is still valid at the entry $E_{\boldsymbol{u}^+}$. Therefore

$$h^{(\boldsymbol{s})}(\boldsymbol{x}) = f(\boldsymbol{x}) \in V_{\boldsymbol{u}^+}(E).$$

*Cases b) and c):* In both cases b) and c), it is required to find a polynomial $f \in \mathcal{N}$ with $\mathrm{lead}\,(f) \leq \boldsymbol{s}$. We show that this is possible, before proceeding to analyze cases b) and c) individually.

The point $\boldsymbol{s}$ is an exterior corner of the updated delta set $\Delta^+$, which contains the original delta set $\Delta(V_{\boldsymbol{u}}(E)) = \Delta(\mathcal{F})$. First, we assume that $\boldsymbol{s}$ is not an exterior corner of the delta set $\Delta(\mathcal{F})$. The point $\boldsymbol{s}$ is nonetheless a point on the exterior of $\Delta(\mathcal{F})$, and so there exists a polynomial $f(\boldsymbol{x}) \in \mathcal{F}$ whose leading monomial $\mathrm{lead}\,(f)$ is an exterior corner of $\Delta(\mathcal{F})$, satisfying $\mathrm{lead}\,(f) \leq \boldsymbol{s}$. The fact that $\boldsymbol{s}$ is an exterior corner of the new delta set $\Delta^+$ thus implies that $\mathrm{lead}\,(f)$ must be in the interior of $\Delta^+$, for otherwise $\mathrm{lead}\,(f)$, and not $\boldsymbol{s}$ would be an exterior corner of $\Delta^+$. Since

$$\mathrm{lead}\,(f) \in \Delta^+ \subseteq \Delta(V_{\boldsymbol{u}^+}(E))$$

there is no polynomial with leading term $\mathrm{lead}\,(f)$ which is valid for the $m$-dimensional array $E$ up to entry $E_{\boldsymbol{u}^+}$. Thus we can conclude that $f(\boldsymbol{x})$ was found to be invalid at entry $\boldsymbol{E}_{\boldsymbol{u}^+}$, and therefore $f(\boldsymbol{x}) \in \mathcal{N}$, as required.

Now, we assume that $\boldsymbol{s}$ is an exterior corner of the delta set $\Delta(\mathcal{F})$. Thus there is a polynomial $f(\boldsymbol{x}) \in \mathcal{F}$ with $\mathrm{lead}\,(f) = \boldsymbol{s}$. Moreover, $f(\boldsymbol{x})$ must be in the set $\mathcal{N}$, or else case a) would apply. Therefore, in cases b) and c), it is always possible to find a polynomial $f(\boldsymbol{x}) \in \mathcal{N}$, with $\mathrm{lead}\,(f) \leq \boldsymbol{s}$.

*Case b):* Clearly, $h^{(\boldsymbol{s})}(\boldsymbol{x})$ has $\mathrm{lead}\,(h^{(\boldsymbol{s})}) = \boldsymbol{s}$, and since $\boldsymbol{s} \not\leq \boldsymbol{u}^+$, it is not possible to predict entry $E_{\boldsymbol{u}^+}$ using the $m$-dimensional linear recursion relation represented by $h^{(\boldsymbol{s})}(\boldsymbol{x})$. Thus $h^{(\boldsymbol{s})}(\boldsymbol{x})$ will be valid up to entry $E_{\boldsymbol{u}^+}$ if and only if it is valid up to entry $E_{\boldsymbol{u}}$. But $h^{\boldsymbol{s}}(\boldsymbol{x})$ is a monomial multiple of $f(\boldsymbol{x})$, and so by Theorem 26, $h^{\boldsymbol{s}}(\boldsymbol{x}) \in V_{\boldsymbol{u}}(E)$. Therefore, $h^{\boldsymbol{s}}(\boldsymbol{x}) \in V_{\boldsymbol{u}^+}(E)$.

*Case c):* First, we must show that it is possible to find $g \in \mathcal{G}$ with $\mathrm{Span}\,(g) \geq \boldsymbol{u}^+ - \boldsymbol{s}$. Suppose that it is not possible. This means that $\boldsymbol{u}^+ - \boldsymbol{s}$ is in the exterior of $\Delta(\mathcal{F})$, and therefore, $\boldsymbol{u}^+ - \boldsymbol{s} \geq \boldsymbol{p}$ for some exterior corner $\boldsymbol{p}$ of $\Delta(\mathcal{F})$. There exists a polynomial $f'(\boldsymbol{x}) \in \mathcal{F}$ with leading monomial $\mathrm{lead}\,(f') = \boldsymbol{p}$. Then we have $\mathrm{lead}\,(f') + \mathrm{lead}\,(f) \leq \boldsymbol{p} + \boldsymbol{s} \leq \boldsymbol{u}^+$, and so by the agreement theorem (Theorem 30), the polynomials $f'(\boldsymbol{x})$ and $f(\boldsymbol{x})$ must have made the same (incorrect) prediction for $E_{\boldsymbol{u}^+}$. Thus $f'(\boldsymbol{x}) \in \mathcal{N}$ and hence $\mathrm{Span}\,(f') = \boldsymbol{u}^+ - \boldsymbol{p}$ was one of the new excluded points used to form the set $\Delta^+$, and therefore, $\boldsymbol{u}^+ - \boldsymbol{p} \in \Delta^+$. But now $\boldsymbol{s} \leq \boldsymbol{u}^+ - \boldsymbol{p}$ implies that $\boldsymbol{s}$ is in the interior of $\Delta^+$, which means that we have arrived at a contradiction. Thus it is always possible to find $g \in \mathcal{G}$ with $\mathrm{Span}\,(g) \geq \boldsymbol{u}^+ - \boldsymbol{s}$.

Next, we verify that the polynomial $h^{(\boldsymbol{s})}(\boldsymbol{x})$, given in line 26, has the required leading term. The polynomial $h^{(\boldsymbol{s})}(\boldsymbol{x})$ is given as the sum of two polynomials. The first polynomial is

$$\boldsymbol{x}^{\boldsymbol{s}-\mathrm{lead}\,(f)} f(\boldsymbol{x})$$

which has leading monomial $\boldsymbol{s}$. Note that $g$ is not valid up to entry $E_{\boldsymbol{u}}$, and thus

$$\mathrm{lead}\,(g) + \mathrm{Span}\, g \leq_T \boldsymbol{u} \;_T\; \boldsymbol{u}^+$$

In the expression for $h^{(\boldsymbol{s})}(\boldsymbol{x})$, the second polynomial is

$$\boldsymbol{x}^{\mathrm{Span}(g)-\boldsymbol{u}^+ + \boldsymbol{s}} g(\boldsymbol{x})$$

which has leading monomial

$$\mathrm{Span}\, g - \boldsymbol{u}^+ + \boldsymbol{s} + \mathrm{lead}\,(g) \;_T\; \boldsymbol{s}.$$

Thus $\mathrm{lead}\,(h^{(\boldsymbol{s})}) = \boldsymbol{s}$.

To see that $h^{(\boldsymbol{s})}$ is valid up to entry $E_{\boldsymbol{u}^+}$, we assume that $\boldsymbol{q}$ satisfies $\boldsymbol{q} \geq \text{lead}\,(h^{\boldsymbol{s}}) = \boldsymbol{s}$, and $\boldsymbol{q} \leq_T \boldsymbol{u}^+$, and compute

$$\begin{aligned}\text{lc}\,(h)\Big(E_{\boldsymbol{q}} - P_{\boldsymbol{q}}(h^{(\boldsymbol{s})})\Big) &= \sum_{\boldsymbol{p}} h_{\boldsymbol{p}} E_{\boldsymbol{p}+\boldsymbol{q}-\boldsymbol{s}} \\ &= T_1 - \left(\frac{\delta_f}{\delta_g}\right) T_2\end{aligned}$$

where the two terms $T_1$ and $T_2$ are obtained from the expansion of the coefficients $h_{\boldsymbol{p}}$

$$\begin{aligned}T_1 &= \sum_{\boldsymbol{p}} f_{\boldsymbol{p}-\boldsymbol{s}+\text{lead}(f)} E_{\boldsymbol{p}+\boldsymbol{q}-\boldsymbol{s}} \\ &= \sum_{\boldsymbol{t}} f_{\boldsymbol{t}} E_{\boldsymbol{t}+\boldsymbol{q}-\text{lead}(f)} \\ &= \text{lc}\,(f)\Big[E_{\boldsymbol{q}} - P_{\boldsymbol{q}}(f)\Big] \\ &= \begin{cases} 0, & \text{for } \boldsymbol{q} \leq_T \boldsymbol{u} \\ \delta_f, & \text{for } \boldsymbol{q} = \boldsymbol{u}^+ \end{cases}\end{aligned}$$

$$\begin{aligned}T_2 &= \sum_{\boldsymbol{p}} g_{\boldsymbol{p}-\text{Span}(g)+\boldsymbol{u}^+-\boldsymbol{s}} E_{\boldsymbol{p}+\boldsymbol{q}-\boldsymbol{s}} \\ &= \sum_{\boldsymbol{t}} g_{\boldsymbol{t}} E_{\boldsymbol{t}+\boldsymbol{q}+\text{Span}(g)-\boldsymbol{u}^+} \\ &= \text{lc}\,(g)\Big[E_{\boldsymbol{q}'} - P_{\boldsymbol{q}'}(g)\Big] \\ &= \begin{cases} 0, & \text{for } \boldsymbol{q}' \;{}_T\; \text{lead}\,(g) + \text{Span}\, g, \\ \delta_g, & \text{for } \boldsymbol{q}' = \text{lead}\,(g) + \text{Span}\, g. \end{cases}\end{aligned}$$

Here, we have made the substitution

$$\boldsymbol{q}' = \boldsymbol{q} + \text{Span}\, g - \boldsymbol{u}^+ + \text{lead}\,(g)$$

and so

$$T_2 = \begin{cases} 0, & \text{for } \boldsymbol{q} \leq_T \boldsymbol{u} \\ \delta_g, & \text{for } \boldsymbol{q} = \boldsymbol{u}^+. \end{cases}$$

Putting the two terms back together, we find

$$\text{lc}\,(h)\Big(E_{\boldsymbol{q}} - P_{\boldsymbol{q}}(h^{(\boldsymbol{s})})\Big) = \begin{cases} 0, & \text{for } \boldsymbol{q} \leq_T \boldsymbol{u} \\ 0, & \text{for } \boldsymbol{q} = \boldsymbol{u}^+ \end{cases}$$

proving that $h^{(\boldsymbol{s})}(x)$ is valid at entry $E_{\boldsymbol{u}^+}$. ■

## ACKNOWLEDGMENT

The authors wish to thank J. Little for many helpful comments and suggestions.

## REFERENCES

[1] B. Buchberger, "Gröbner bases: An agorithmic method in polynomial ideal theory," in *Multidimensional Systems Theory: Progress, Directions and Open Problems in Multidimensional Systems*, N. K. Bose, Ed. Dordrecht, The Netherlands: Reidel, 1985.

[2] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms.* New York: Springer-Verlag, 1992.

[3] T. Becker and V. Weispfenning, *Gröbner Bases.* New York: Springer-Verlag, 1992.

[4] W. Fulton, *Algebraic Curves: An Introduction to Algebraic Geometry.* Redwood City, CA: Addson-Wesley, 1989.

[5] C. J. Moreno, *Algebraic Curves over Finite Fields.* Cambridge, England: Univ. Press, 1991.

[6] I. R. Shafarevich, *Basic Algebraic Geometry.* Berlin, Germany: Springer, 1977.

[7] J. Harris, *Algebraic Geometry: A First Course.* New York: Springer-Verlag, 1992.

[8] R. Hartshorne, *Algebraic Geometry.* New York: Springer, 1977.

[9] S. C. Porter, "Decoding codes arising from Goppa's construction on algebraic curves," Ph.D. dissertation, Yale Univ., New Haven, CT, Dec. 1988.

[10] S. C. Porter, B.-Z. Shen, and R. Pellikaan, "Decoding geometric Goppa codes using an extra place," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1663–1676, Nov. 1992.

[11] V. D. Goppa, "Codes associated with divisors," *Probl. Inform. Transm.*, vol. 13, pp. 33–39, 1977.

[12] ——, *Geometry and Codes.* Dordrecht, The Netherlands: Kluwer, 1988.

[13] J. H. van Lint, "Algebraic geometric codes," in *Coding Theory and Design Theory*, D. Ray-Chaudhuri, Ed. New York: Springer-Verlag, 1990.

[14] J. H. van Lint and G. van der Geer, *Introduction to Coding Theory and Algebraic Geometry* (DMV Lecture Notes). Basel, Switzerland: Birkhauser, 1988.

[15] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic Geometric Codes.* Dordrecht, The Netherlands: Kluwer, 1991.

[16] H. Stichtenoth, *Algebraic Function Fields and Codes.* Berlin, Germany: Springer, 1993.

[17] H. Imai, "A theory of two-dimensional cyclic codes," *Inform. Contr.*, vol. 34, pp. 1–21, 1977.

[18] A. Poli and L. Huguet, *Error Correcting Codes: Theory and Applications.* Hemel Hempstead, England: Prentice-Hall, 1992.

[19] K. Saints and C. Heegard, "On hyperbolic cascaded Reed–Solomon codes," in *Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes: Proc. AAECC-10*, G. Cohen, T. Mora, and O. Moreno, Eds., no. 673 in *Lecture Notes in Computer Science.* Berlin, Germany: Springer, 1993.

[20] K. Saints and C. Heegard, "Hyperbolic cascaded Reed–Solomon codes," submitted to *IEEE Trans. Inform. Theory*, 1995.

[21] K. Saints, "Algebraic methods for the encoding and decoding problems for multidimensional cyclic codes and algebraic-geometric codes," Ph.D. dissertation, Cornell Univ., Ithaca, NY, 1995.

[22] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* Amsterdam, The Netherlands: North-Holland, 1977.

[23] S. Miura and N. Kamiya, "Geometric-Goppa codes on some maximal curves and their minimum distance," in *Proc. 1993 IEEE Information Theory Workshop*, 1993.

[24] D. Polemi, C. J. Moreno, and O. J. Moreno, "Search and construction of good a.g. Goppa codes," manuscript, 1993.

[25] R. E. Blahut, *Theory and Practice of Error Control Codes.* Reading, MA: Addison-Wesley, 1983.

[26] E. R. Berlekamp, *Algebraic Coding Theory.* New York: McGraw-Hill, 1968.

[27] J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 122–127, Jan. 1969.

[28] S. Sakata, "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.

[29] S. Sakata, "Extension of the Berlekamp–Massey algorithm to $n$ dimensions," *Inform. Comput.*, vol. 84, pp. 207–239, 1989.

[30] G.-L. Feng and T. R. N. Rao, "Decoding algebraic–geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, vol. 39, pp. 37–45, Jan. 1993.

[31] S. Sakata, "Decoding binary 2-D cyclic codes by the 2-D Berlekamp–Massey algorithm," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1200–1203, July 1991.

[32] S. Sakata, J. Justesen, Y. Madelung, H. E. Jensen, and T. Høholdt, "Fast decoding of AG-codes up to the designed minimum distance," Tech. Rep. MAT-1993-12, Tech. Univ. of Denmark, Lyngby, 1993.