Designs, Codes and Cryptography, 13, 147–158 (1998)

Decoding Affine Variety Codes Using Gröbner Bases

J. FITZGERALD* fitzgewj@jmu.edu
Department of Mathematics, James Madison University, Harrisonburg, VA 22807

R. F. LAX lax@math.lsu.edu
Department of Mathematics, LSU, Baton Rouge, LA 70803

Communicated by: E.F. Assmus, Jr.
Received July 15, 1996; Revised December 30, 1996; Accepted January 17, 1997

Abstract. We define a class of codes that we call affine variety codes. These codes are obtained by evaluating functions in the coordinate ring of an affine variety on all the $\mathbf{F}_q$-rational points of the variety. We show that one can, at least in theory, decode these codes up to half the true minimum distance by using the theory of Gröbner bases. We extend results of A. B. Cooper and of X. Chen, I. S. Reed, T. Helleseth, and T. K. Truong.

Keywords: linear code, Gröbner basis, affine variety

1. Affine Variety Codes

We define a class of codes that we call affine variety codes. These codes are obtained by evaluating functions in the coordinate ring of an affine variety on all the $\mathbf{F}_q$-rational points of the variety. The motivation for this definition comes from algebraic-geometric Goppa codes and the "improved" geometric Goppa codes considered by Feng and Rao [10].

As a result of this definition, one can use ideals in polynomial rings to answer questions about a linear code, even if the code itself does not form an ideal. We will show that one can, at least in theory, decode these codes up to (and possibly beyond) half the true minimum distance by using the theory of Gröbner bases. Our theorems generalize work of X. Chen *et al.* [4,5] and A. Brinton Cooper [7]. We thank Heinz Kredel for help with his software MAS, Jean-Charles Faugère for help with his software Gb, and David Bayer for help with his software Macaulay.

Let $I \subseteq \mathbf{F}_q[X_1, X_2, \ldots, X_s]$ be an ideal, where $\mathbf{F}_q$ denotes the field with q elements. Put

$$I_q = I + (X_1^q - X_1, X_2^q - X_2, \ldots, X_s^q - X_s).$$

Then it is easy to see that the points of the affine variety defined by I_q (over an algebraic closure of $\mathbf{F}_q$) are the $\mathbf{F}_q$-rational points of the affine variety defined by I. Let $P_1, P_2, \ldots, P_n$ denote these points.

Since I_q contains the polynomials $X_i^q - X_i, i = 1, \ldots, s$, it is an ideal of dimension 0, and we know, from Seidenberg's Lemma 92 [19], that it is a radical ideal. It follows that the coordinate ring

$$R = \mathbf{F}_q[X_1, X_2, \ldots, X_s]/I_q$$

* Most of these results are contained in the first author's LSU Ph.D. dissertation.

of the affine variety defined by I_q is an Artin ring of length n and that we have an isomorphism of $\mathbf{F}_q$-vector spaces

$$\begin{aligned} \phi : R &\rightarrow \mathbf{A}^n \\ \bar{f} &\mapsto (f(P_1), \ldots, f(P_n)), \end{aligned}$$

where f is any preimage of $\bar{f}$ in the polynomial ring and $\mathbf{A}^n$ denotes affine n-space over $\mathbf{F}_q$. Let $L \subseteq R$ be an $\mathbf{F}_q$-vector subspace of R.

Definition 1. We define the affine variety code $C(I, L)$ to be $\phi(L)$, the image of L under the evaluation map ϕ, and the affine variety code $C^{\perp}(I, L)$ to be the orthogonal complement of $C(I, L)$ with respect to the usual inner product on $\mathbf{A}^n$.

Remarks.

1) A different ordering of the P_i would yield an equivalent code.

2) If $\bar{f}_1, \bar{f}_2, \ldots, \bar{f}_k$ is a basis for L, then the matrix

$$[f_i(P_j)] \quad i = 1, \ldots, k; j = 1, \ldots, n$$

is a generator matrix for $C(I, L)$ and a parity check matrix for $C^{\perp}(I, L)$.

3) Affine variety codes are essentially the same as the evaluation codes considered in [11,section 3.2], and [3,section 8], (also see Saints [20]). Let $\bar{f}_1, \ldots, \bar{f}_k$ be a basis for the vector subspace L of R/I_q. Let $\tilde{f}_i$ be a preimage in $\tilde{R} = \mathbf{F}_q[X_1, \ldots, X_s]/I$ of $\bar{f}_i, i = 1, \ldots, k$, under the canonical map from $\tilde{R}$ to R. If $\tilde{f}_1, \ldots, \tilde{f}_k$ are the first k elements in an $\mathbf{F}_q$-basis for $\tilde{R}$, then it is easy to see that the affine variety code $C(I, L)$ is the evaluation code E_k of [11], and the affine variety code $C^{\perp}(I, L)$ is the code C_k of [11].

4) If $\mathbf{F}_0$ is a subfield of $\mathbf{F}_q$, then we may consider the subfield subcodes obtained by taking the intersections $C(I, L) \cap \mathbf{F}_0^n$ or $C^{\perp}(I, L) \cap \mathbf{F}_0^n$.

Below, we will show that every linear code may be represented as an affine variety code, but first, we describe how some well-known classes of codes may be viewed naturally as affine variety codes.

Examples:

1) Let $I = (X^{q-1} - 1) \subset \mathbf{F}_q[X]$. Then $I_q = I$, and $V(I)$ consists of the nonzero points on $\mathbf{A}^1$. Take $L = \langle 1, x, x^2, \ldots, x^{k-1} \rangle$, where x is the residue class of X in $\mathbf{F}_q[X]/I$. Then $C(I, L)$ is the Reed-Solomon code of dimension k over $\mathbf{F}_q$. If we start with $I = (0)$, then $I_q = (X^q - X), V(I_q) = \mathbf{A}^1$, and, with L as above, we get the extended Reed-Solomon code of dimension k.

2) Let $I = (0) \subset \mathbf{F}_q[X_1, \ldots, X_s]$ and take $L = \langle$ polynomials of deg $<$ some $\nu \rangle$. Then $C(I, L)$ is a generalized Reed-Muller code, as in [9].

3) Let X be a nonsingular, absolutely irreducible, projective curve of genus g defined over $\mathbf{F}_q$. A one-point algebraic geometric code is a geometric Goppa code of the form $C_L(mP, D)$, where P is an $\mathbf{F}_q$-rational point on X and D is a divisor on X defined over $\mathbf{F}_q$ (see [13]). Embed the curve into a projective space using a linear system of the form

$|NP|$, with N sufficiently high ($N \geq 2g+1$ will certainly suffice) so that the only point at infinity of the embedded curve X' is the image of P. Let I denote the ideal of the affine curve obtained by deleting the image of P from X'. If D denotes the sum of the other $\mathbf{F}_q$-rational points besides P, then $C_L(mP, D)$ is the affine variety curve $C(I, L)$, where L consists of the polynomials that give a basis of $L(mP)$, the space of rational functions over $\mathbf{F}_q$ that have a pole of order at most m at P and no other poles.

PROPOSITION 1 *Every $\mathbf{F}_q$-linear code may be represented as an affine variety code.*

Proof: Let C be an $\mathbf{F}_q$-code of dimension k and length n. Let $[c_{ij}]$, for $i = 1, \ldots, k$ and $j = 1, \ldots, n$, be a generator matrix for C. Choose s so that $q^s \geq n$. (In practice, one would want to choose the least s with this property.) Let $Y = \{P_1, P_2, \ldots, P_n\} \subseteq \mathbf{A}_s$ and let I denote the ideal of Y in $\mathbf{F}_q[X_1, \ldots, X_s]$. (We note that there is an algorithm for finding a Gröbner basis for such an ideal I in [15].) Let $P_j = (a_{j1}, \ldots, a_{js})$ for $j = 1, \ldots, n$. We have the following lemma from [9, p. 406]:

LEMMA 1 *The polynomial*

$$\chi_j(X_1, \ldots, X_s) = \prod_{l=1}^{s} [1 - (X_l - a_{jl})^{q-1}]$$

has value zero at every point of $\mathbf{A}^s$ except at P_j where it assumes the value 1.

Let $\bar{\chi}_j, j = 1, \ldots, n$, denote the residue class of χ_j in $\mathbf{F}_q[X_1, \ldots, X_s]/I_q$. Put

$$\bar{f}_i = \sum_{j=1}^{n} c_{ij} \bar{\chi}_j$$

for $i = 1, \ldots, k$ and take $L = \langle \bar{f}_1, \ldots, \bar{f}_k \rangle$. Then $C = C(I, L)$. ■

Remarks.

1) We could have started with a parity check matrix for C instead of a generator matrix in the proof of Proposition 1.4, and thus have shown that C is of the form $C^{\perp}(I, L)$ for suitable I and L.

2) Proposition 1 also follows from Example 3 above and the proof of Theorem 2 in [16].

EXAMPLE: A parity check matrix for the ternary Golay code is:

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 2 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 1 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 1 & 2 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 2 & 2 & 1 & 1 \end{pmatrix}$$

We order the points of $\mathbf{F}_3^3$ as follows:

$$P_1 = (0,0,0), P_2 = (0,0,1), P_3 = (0,0,2), P_4 = (0,1,0), \ldots, P_{27} = (2,2,2).$$

Consider the first eleven points $P_1 = (0,0,0), \ldots, P_{11} = (1,0,1)$.

The ideal $I \subseteq \mathbf{F}_3[X,Y,Z,]$ such that $V(I_3) = \{P_1, \ldots, P_{11}\}$ is generated by the polynomials $\chi_{12}, \ldots \chi_{27}$ from Lemma 1. For example,

$$\chi_{12} = (1-(X-1)^2)(1-(Y-0)^2)(1-(Z-2)^2) = (2X^2+2X)(1+2Y^2)(2Z^2+Z).$$

If we want, we can use software to find a smaller generating set for I, or in this case, inspection and some experimentation reveal that we may take I to be the ideal

$$I = (XY, X+2X^2, XZ^2+2XZ).$$

Next, we construct the polynomials $\chi_1, \ldots, \chi_{11}$, then calculate the polynomial f_i giving the i-th row of the matrix M by

$$f_i = \sum_{j=1}^{11} a_{ij}\chi_j,$$

where a_{ij} is the i,j entry of the matrix M above. We obtain

$$\begin{aligned}
f_1 &= 1 + X + Y - XZ + Y^2 - Z^2 + Y^2Z \\
f_2 &= Y - Z + XZ - Y^2 + YZ - Z^2 + Y^2Z \\
f_3 &= X - Y + Z + XZ + Y^2 + YZ - Z^2 - Y^2Z + YZ^2 - Y^2Z^2 \\
f_4 &= -X + Y - XZ + Y^2Z - YZ^2 - Y^2Z^2 \\
f_5 &= X + YZ^2.
\end{aligned}$$

Thus the ternary Golay code is $C^{\perp}(I,L)$, where $L = \langle \bar{f}_1, \bar{f}_2, \bar{f}_3, \bar{f}_4, \bar{f}_5 \rangle$. □

2. Decoding Using Gröbner Bases

In this section, we generalize results of X. Chen *et al.* [4,5] to show how Gröbner bases may be used to decode affine variety codes. Let C be an affine variety code of the form $C^{\perp}(I,L)$, where

$$\begin{aligned}
I &= (g_1, g_2, \ldots, g_m) \subseteq \mathbf{F}_q[X_1, X_2, \ldots, X_s] \\
L &= \langle \bar{f}_1, \bar{f}_2, \ldots, \bar{f}_r \rangle \\
V(I_q) &= \{P_1, P_2, \ldots, P_n\}.
\end{aligned}$$

Let $\hat{y} = (y_1, y_2, \ldots, y_n)$ be a received word. The syndrome of $\hat{y}$ is $(s_1, s_2, \ldots, s_r)$, where

$$s_i = \sum_{j=1}^{n} y_j f_i(P_j).$$

Let $\hat{y} = \hat{c} + (e_1, e_2, \ldots, e_n)$, where $\hat{c} \in C^{\perp}(I,L)$. Then

$$s_i = \sum_{j=1}^{n} e_j f_i(P_j).$$

We need to find the values of the nonzero e_i and their positions. We will assume that precisely t errors have occurred and that there is a unique n-tuple $\hat{e}$ such that $\hat{y} - \hat{e} \in C$ and such that the weight of $\hat{e}$ at most t. This is always true if t is at most $\frac{1}{2}(d(C) - 1)$, where $d(C)$ denotes the minimum distance of the code C.

Consider the polynomial ring

$$T = \mathbf{F}_q[X_{11}, \ldots, X_{1s}, \ldots, X_{t1}, \ldots, X_{ts}, E_1, \ldots, E_t].$$

Here, we have introduced indeterminates $X_{k1}, \ldots, X_{ks}$, where $k = 1, \ldots, t$, for the coordinates at each of the t points at which errors have occurred, and indeterminates $E_1, \ldots, E_t$ corresponding to the values of those errors.

For $i = 1, 2, \ldots, r$, put

$$h_i = \sum_{k=1}^{t} E_k f_i(X_{k1}, X_{k2}, \ldots, X_{ks}) \; - s_i.$$

Let $E_{\hat{y}} \subseteq T$ be the following ideal:

$$E_{\hat{y}} = (g_l(X_{k1}, X_{k2}, \ldots, X_{ks}), h_i, E_k^{q-1} - 1)_q,$$

where $i = 1, \ldots, r; k = 1, \ldots, t; l = 1, 2, \ldots, m$. Notice that $E_{\hat{y}}$ contains the polynomials $X_{kj}^q - X_{kj}$ for $k = 1, \ldots, t$ and $j = 1, \ldots, s$.

PROPOSITION 2 *Suppose the errors occur at the positions corresponding to the points P_{u_k} and that the error value e_{u_k} corresponds to P_{u_k} for $k = 1, \ldots, t$. Then there are precisely $t!$ points in $V(E_{\hat{y}})$. These points are*

$$\{(P_{u_{\sigma(1)}}, \ldots, P_{u_{\sigma(t)}}, e_{u_{\sigma(1)}}, \ldots, e_{u_{\sigma(t)}}) | \sigma \in Sym(t)\},$$

where $Sym(t)$ denotes the symmetric group on t objects (and where we write P_{u_k} in place of the s coordinates of that point).

Proof: It is easy to see, from the symmetry of the polynomials generating $E_{\hat{y}}$, that each of these points is in $V(E_{\hat{y}})$. The existence of any other point in $V(E_{\hat{y}})$ would contradict the assumption that there is a unique n-tuple $\hat{e}$ of weight at most t such that $\hat{y} - \hat{e} \in C$. ■

We now define a term order on the monomials in T that will be useful for our purposes. Let $<_1$ be the lexicographic term order on the monomials involving only $X_{11}, \ldots, X_{1s}, E_1$, which extends the ordering $X_{11} <_1 X_{12} <_1 \cdots <_1 X_{1s} <_1 E_1$. Let $<_2$ be any term order on the monomials involving only the variables $X_{21}, \ldots, X_{2s}, \ldots, X_{t1}, \ldots, X_{ts}, E_2, \ldots, E_t$. Let $<$ be an elimination order with the variables $X_{11}, \ldots, X_{1s}, E_1$ less than all the other variables. Specifically, if M_1, M_2 are monomials in $X_{11}, \ldots, X_{1s}, E_1$ and N_1, N_2 are monomials in $X_{21}, \ldots, X_{2s}, \ldots, X_{t1}, \ldots, X_{ts}, E_2, \ldots, E_t$, then

$$M_1 N_1 < M_2 N_2 \Leftrightarrow \begin{cases} M_1 <_1 M_2 \\ \textit{or} \\ M_1 = M_2 \text{ and } N_1 <_2 N_2. \end{cases}$$

We assume a familiarity with elimination theory, as developed in Chapter 3 of [8].

THEOREM 1 *Let G be a Gröbner basis for $E_{\hat{y}}$ with respect to the order $<$. Then we may solve for the error locations and values by applying elimination theory to the polynomials in G.*

Proof: By Proposition 2, it suffices to find the coordinates corresponding to the variables $X_{11}, \ldots, X_{1s}, E_1$ of each point in $V(E_{\hat{y}})$. Put

$$\begin{aligned} J &= E_{\hat{y}} \cap \mathbf{F}_q[X_{11}, \ldots, X_{1s}, E_1] \\ J_j &= E_{\hat{y}} \cap \mathbf{F}_q[X_{11}, \ldots, X_{1j}], \end{aligned}$$

for $j = 1, \ldots, s$.

Since $<$ is an elimination order, the set $G' = G \cap J$ is a Gröbner basis for the ideal J by [1, Theorem 2.3.4]. It follows from the definition of $<$ that G' is therefore a Gröbner basis for J with respect to the order $<_1$. Notice that, for any j, $1 < j \leq s$, the order $<_1$, being a lexicographic ordering, is an elimination order with the variables $X_{11}, \ldots, X_{1j}$ less than the variables $X_{1,j+1}, \ldots, X_{1s}, E_1$. It follows that $G \cap J_j$ is a Gröbner basis for J_j for $j = 1, \ldots, s$.

Since $V(E_{\hat{y}})$ is a finite set of points, the projection of $V(E_{\hat{y}})$ onto the coordinates corresponding to the variables $X_{11}, \ldots, X_{1j}$ is a closed set. Hence the ideal J_j is the ideal of the projection of $V(E_{\hat{y}})$ onto the coordinates corresponding to the variables $X_{11}, \ldots, X_{1j}$ by [1, Theorem 2.5.3]. (We remark that we are actually working over the algebraic closure of $\mathbf{F}_q$, but the points of $V(E_{\hat{y}})$ are all rational over $\mathbf{F}_q$.)

Now, $G \cap J_1 = G \cap \mathbf{F}_q[X_{11}]$ is a generator $f_1(X_{11})$ of the principal ideal J_1. The zeros of $f_1(X_{11})$ in $\mathbf{F}_q$ are then all the first coordinates of points in $V(E_{\hat{y}})$. By substituting each of these first coordinates for X_{11} in the set $G \cap J_2$, we obtain univariate polynomials in X_{12}. By finding the zeros of these univariate polynomials in $\mathbf{F}_q$, we have now found the first two coordinates of (precisely) each point in $V(E_{\hat{y}})$. (Here we use the fact that the ideal J_2 is the ideal of the projection of $V(E_{\hat{y}})$ onto the first two coordinates.) By continuing in this manner, we may find all the coordinates corresponding to the variables $X_{11}, \ldots, X_{1s}, E_1$ of each point of $V(E_{\hat{y}})$. ■

Remark. Theorem 1 generalizes results of X. Chen *et al* [4,5]. We note that these authors use a pure lexicographic ordering on all the variables, while our elimination order allows one to use a more efficient order, such as graded reverse lex (cf. [8, p. 57]), on the variables to be "eliminated." Also note that in Theorem 5 of [5], the authors recommend finding a univariate polynomial in each of the variables $X_{11}, \ldots, X_{1s}$ to find the coordinates of the error points. One would still need to find the precise points involved from all the possible combinations of the zeros of these univariate polynomials and their suggestion would involve more Gröbner basis calculations than the elimination theory described above.

EXAMPLE: Take $I = (Y^2 + Y - X^3) \subset \mathbf{F}_4[X, Y]$. Put $\mathbf{F}_4[x, y] = \mathbf{F}_4[X, Y]/I_4$. The eight points of I_4 are

$$\begin{aligned} P_1 &= (0,0), P_2 = (0,1), P_3 = (1,\alpha), P_4 = (1,\alpha^2), \\ P_5 &= (\alpha,\alpha), P_6 = (\alpha,\alpha^2), P_7 = (\alpha^2,\alpha), P_8 = (\alpha^2,\alpha^2), \end{aligned}$$

where $\alpha^2 = \alpha + 1$.

Take $L = \langle 1, x, y, x^2, xy \rangle$. The code $C = C^{\perp}(L, I)_4$ is the same as the geometric Goppa code

$$C_{\Omega}(P_1 + \cdots P_8, 5P_{\infty}),$$

a Hermitian code. The minimum distance of C is 5 (by [21] or by using Goppa's bound). A parity check matrix for C is:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha^2 & \alpha^2 \\ 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & \alpha^2 & \alpha^2 & \alpha & \alpha \\ 0 & 0 & \alpha & \alpha^2 & \alpha^2 & 1 & 1 & \alpha \end{pmatrix}$$

Suppose one receives the word

$$\hat{y} = (0, 0, 1, 0, 0, \alpha, 0, 0).$$

The syndrome of this word is

$$(\alpha^2, \alpha, \alpha^2, 0, 0).$$

To decode, one needs to find a Gröbner basis for the ideal in $\mathbf{F}_4[X_1, Y_1, X_2, Y_2, E_1, E_2]$ generated by:

$$\begin{array}{l} X_1^4 - X_1, Y_1^4 - Y_1, E_1^3 - 1, X_2^4 - X_2, Y_2^4 - Y_2, E_2^3 - 1 \\ Y_1^2 + Y_1 - X_1^3, Y_2^2 + Y_2 - X_2^3 \\ E_1 + E_2 - \alpha^2 \\ E_1 X_1 + E_2 X_2 - \alpha \\ E_1 Y_1 + E_2 Y_2 - \alpha^2 \\ E_1 X_1^2 + E_2 X_2^2 \\ E_1 X_1 Y_1 + E_2 X_2 Y_2. \end{array}$$

One can do this using the program MAS [12]. This program, unlike Gb or Macaulay, can handle polynomials with coefficients that are not in the prime field $\mathbf{F}_p$. We compute a Gröbner basis of this ideal with respect to the lexicographic order that extends the following order on the variables:

$$X_1 < Y_1 < E_1 < X_2 < Y_2 < E_2.$$

We find that a Gröbner basis is:

$$\{X_1^2 + \alpha^2 X_1 + \alpha, Y_1 + \alpha X_1, E_1 + X_1, X_2 + X_1 + \alpha^2, Y_2 + \alpha X_1 + 1, E_2 + X_1 + \alpha^2\}.$$

The first coordinates of the error points are the roots of $X_1^2 + \alpha^2 X_1 + \alpha$, namely 1 and α. When we substitute 1 for X_1 in the polynomial $Y_1 + \alpha X_1$, we find that the corresponding Y_1 value is α. When we substitute α for X_1 in $Y_1 + \alpha X_1$, we find that the corresponding Y_1 value is α^2. Thus the two error points are $P_3 = (1, \alpha)$ and $P_6 = (\alpha, \alpha^2)$, which correspond to positions 3 and 6 in our received word. From the third polynomial in the Gröbner basis, we see that the error value at each point is the same as the first coordinate at that point.

□

3. Precomputation of Locators and Evaluators

To use Theorem 1, or the results in [4,5], to decode words with exactly t errors, one would need to compute a Gröbner basis each time such a word was received. This would certainly take too much time to be practical. Instead of computing a Gröbner basis for every such word, it would be desirable to compute a Gröbner basis one time, and then use that result to decode every received message with exactly t errors (with t at most $\frac{1}{2}(d(C)-1)$). We describe a method that accomplishes this, at least in theory. Our method generalizes results of A. B. Cooper [7], who showed how one could find a "universal" error locator polynomial for a binary BCH code by computing a Gröbner basis. The idea is simply to replace the syndromes s_i in Section 2 by variables S_i. The advantage of this is that now one only needs to compute a single Gröbner basis for decoding words with exactly t errors. The disadvantage is that one now must deal with a polynomial ring that involves more variables. This results in an increase in the time and storage required for the Gröbner basis calculation and the resulting Gröbner basis may be quite complicated; however, one must only do such a computation once for a given code and a given t. Similar extensions of the ideas of Cooper appear in [3, 6, 14, 17, 18].

As in Section 2, let C be an affine variety code of the form $C^{\perp}(I, L)$, where

$$\begin{aligned} I &= (g_1, g_2, \ldots, g_m) \subseteq \mathbf{F}_q[X_1, X_2, \ldots, X_s] \\ L &= \langle \bar{f}_1, \bar{f}_2, \ldots, \bar{f}_r \rangle \\ V(I_q) &= \{P_1, P_2, \ldots, P_n\}. \end{aligned}$$

Consider the polynomial ring

$$\mathcal{T} = T[S_1, S_2, \ldots, S_r],$$

where we have now introduced variables $S_1, \ldots, S_r$ for the syndromes of a received message (and the ring T is the ring from Section 2). For $i = 1, \ldots, r$, put

$$h_i = \sum_{k=1}^{t} E_k f_i(X_{k1}, X_{k2}, \ldots, X_{ks}) - S_i.$$

Let $\mathcal{E} \subseteq \mathcal{T}$ be the ideal

$$(g_l(X_{k1}, X_{k2}, \ldots, X_{ks}), h_i, E_k^{q-1} - 1)_q,$$

where $i = 1, \ldots, r; k = 1, \ldots, t; l = 1, 2, \ldots, m$. Notice that the polynomials $S_i^q - S_i, i = 1, \ldots, r$, are in $\mathcal{E}$.

Let $<_s$ be any term order on the variables $S_1, \ldots, S_r$. Let $<$ be the (elimination) order defined on the variables $X_{11}, \ldots, X_{1s}, \ldots, X_{t1}, \ldots, X_{ts}, E_1, \ldots, E_t$ in Section 2. Let $<'$ be the elimination order on the monomials in $\mathcal{T}$ with the variables from the ring T larger than the variables $S_1, \ldots, S_r$. Specifically, if M_1, M_2 are monomials in $S_1, \ldots, S_r$ and N_1, N_2 are monomials in $X_{11}, \ldots, X_{ts}, E_1, \ldots, E_t$, then

$$M_1 N_1 <' M_2 N_2 \Leftrightarrow \begin{cases} M_1 <_s M_2 \\ \textit{or} \\ M_1 = M_2 \text{ and } N_1 < N_2. \end{cases}$$

We may view $V(\mathcal{E})$ as being a family of varieties of the form $V(E_{\hat{y}})$ that we considered in the previous section as follows. Let $\mathcal{S}_t \subset \mathbf{F}_q^r$ denote the set of all syndromes of words $\hat{y}$ such that there exists a unique n-tuple $\hat{e}$ of weight t with $\hat{y} - \hat{e} \in C$. Then projection on the first r coordinates defines a mapping $\pi : V(\mathcal{E}) \to \mathcal{S}_t$, and if $s \in \mathcal{S}_t$ is the syndrome of $\hat{y}$, then we have $\pi^{-1}(s) = V(E_{\hat{y}})$.

THEOREM 2 *Let $\mathcal{G}$ be a Gröbner basis for $\mathcal{E}$ with respect to the order $<'$. Let $\hat{y}$ be any received word such that precisely t errors have occurred. Assume that there is a unique n-tuple $\hat{e}$ such that $\hat{y} - \hat{e} \in C$ and such that the weight of $\hat{e}$ is at most t. Then we may solve for the error locations and values by substituting the coordinates of the syndrome of $\hat{y}$ for the variables $S_1, \ldots, S_r$ in the polynomials in $\mathcal{G}$ and applying elimination theory.*

Proof: As in Theorem 1, we need to find the coordinates corresponding to the variables $X_{11}, \ldots, X_{1s}, E_1$ of the points in $V(\mathcal{E})$ that lie over the point $s \in \mathcal{S}_t$.

Put

$$\begin{aligned} J_0 &= \mathcal{E} \cap \mathbf{F}_q[S_1, \ldots, S_r] \\ J_j &= \mathcal{E} \cap \mathbf{F}_q[S_1, \ldots, S_r, X_{11}, \ldots, X_{1j}] \\ J &= \mathcal{E} \cap \mathbf{F}_q[S_1, \ldots, S_r, X_{11}, \ldots, X_{1s}, E_1] \end{aligned}$$

for $j = 1, \ldots, s$. Similarly, put $G_j = G \cap J_j$ for $j = 0, 1, \ldots, s$. Since $<'$ is an elimination order and we are using lexicographic ordering on $X_{11}, \ldots, X_{1s}, E_1$, we have that G_j is a Gröbner basis for $J_j, j = 0, 1, \ldots, s$, and $G \cap J$ is a Gröbner basis for J.

When we substitute the coordinates of the syndrome s of $\hat{y}$ for the variables $S_1, \ldots, S_r$, we are obtaining a "partial solution," using the terminology in [8, p. 116], in $V(J_0)$ for a point in $V(\mathcal{E})$ that lies over the point $s \in \mathcal{S}_t$. Because we are dealing with a finite number of points, the projection of $V(\mathcal{E})$ onto the coordinates corresponding to the variables $S_1, \ldots, S_r, X_{11}, \ldots, X_{1j}$ is precisely $V(J_j)$ and the projection onto the coordinates corresponding to the variables $X_{11}, \ldots, X_{1s}, E_1$ is precisely $V(J)$. It follows, as in the proof of Theorem 1, that this partial solution extends to give the required coordinates of all the points of $V(\mathcal{E})$ that lie over $s \in \mathcal{S}_t$ (cf. Theorems 2 and 3 of [8, pp. 122-123]) . ■

EXAMPLE: We return to the Hermitian code C of the example in Section 2. We will obtain a set of polynomials that can be used to decode any two errors. The ideal $\mathcal{E}$ is generated by

$$\begin{aligned} &X_1^4 - X_1, Y_1^4 - Y_1, E_1^3 - 1, X_2^4 - X_2, Y_2^4 - Y_2, E_2^3 - 1 \\ &Y_1^2 + Y_1 - X_1^3, Y_2^2 + Y_2 - X_2^3 \\ &E_1 + E_2 - S_1 \\ &E_1X_1 + E_2X_2 - S_2 \\ &E_1Y_1 + E_2Y_2 - S_3 \\ &E_1X_1^2 + E_2X_2^2 - S_4 \\ &E_1X_1Y_1 + E_2X_2Y_2 - S_5 \end{aligned}$$

(compare with the ideal in the example in Section 2). We find a Gröbner basis for this ideal with respect to the term order $<'$ (taking $<_s$ and $<_2$ to be graded reverse lex) using the program Macaulay [2]. (Note that the computations may be done over the prime field $\mathbf{F}_2$ here, since all the coefficients of all the polynomials in the ideal lie in the prime field

and Gröbner bases are well-behaved under field extension.) The Gröbner basis found by Macaulay comprises 119 polynomials! However, most of these polynomials are not useful for our purposes. Indeed, the first 39 polynomials in the Gröbner basis only involve the syndrome variables $S_1, \ldots, S_5$. While these polynomials could potentially be used to determine if a computed syndrome in fact comes from a received word with exactly two errors, we will not make use of them here.

Next, there is a set of 30 polynomials that involve the variables $S_1, \ldots, S_5$ and X_1. Since we are assuming two errors have occurred, the most interesting polynomials in this set are the polynomials of degree two in X_1. There are five such polynomials, one with leading coefficient S_i for each $i = 1, \ldots, 5$. The polynomial of this type with leading coefficient S_1 is

$$Q_1 = S_1X_1^2+(S_1^3S_2+S_1^2S_4^2)X_1+S_1S_2^2S_3+S_1^3S_4+S_2^3S_4+S_1^2S_3S_4+S_1S_3^2S_4+S_1^2S_5^2+S_4.$$

From these polynomials, one can find each of the first coordinates of the error points.

Next, there is a set of 20 polynomials involving the variables $S_1, \ldots, S_5, X_1, Y_1$. Of course, one of these polynomials is $Y_1^2 + Y_1 - X_1^3$. All the other polynomials in this set of polynomials are linear in Y_1. Two of the simpler polynomials that occur in this set of polynomials are:

$$\begin{aligned} Q_2 &= (S_2^2 + S_1S_4)Y_1 + X_1(S_2S_3 + S_1S_5) + S_3S_4 + S_2S_5 \\ Q_3 &= (S_2S_3 + S_1S_4)Y_1 + X_1^2(S_2^2 + S_1S_4) + X_1(S_1S_3 + S_3^2 + S_2S_4) \\ &\quad +S_2S_3 + S_4^2 + S_3S_5. \end{aligned}$$

Next comes a set of 27 polynomials involving E_1 and the above variables. Some of the simpler polynomials occurring in this set are

$$\begin{aligned} Q_4 &= S_1E_1^2 + S_1^2E_1 + S_1^3 \\ Q_5 &= (S_1X_1 + S_2)E_1 + S_1S_2 + S_4^2 \\ Q_6 &= (S_1Y_1 + S_2X_1^2 + S_4X_1 + S_3)E_1 + S_1S_3 + S_3^2 + S_2S_4. \end{aligned}$$

The final three polynomials in the Gröbner basis are: $E_2+E_1+S_1, Y_2+S_3E_1^2+(S_1^2E_1+1)Y_1+S_1^2S_3$, and $X_2 + S_2E_1^2 + (S_1^2E_1 + 1)X_1 + S_1^2S_2$.

To illustrate how one might use these polynomials, consider the syndrome

$$(\alpha^2, \alpha, \alpha^2, 0, 0)$$

from the example in Section 2. Substituting the syndrome into the polynomial Q_1 above, we get the polynomial $\alpha^2X_1^2 + \alpha X_1 + 1$, which has roots 1 and α. Substituting the syndrome into Q_2 yields the polynomial $\alpha^2Y_1 - X_1$, so we find that when $X_1 = 1, Y_1 = \alpha$ and when $X_1 = \alpha, Y_1 = \alpha^2$. Finally, substituting the syndrome and $X_1 = 1$ into Q_5 yields $E_1 = 1$, and substituting the syndrome and $X_1 = \alpha$ into Q_5 yields $E_1 = \alpha$. □

It is not clear if it will be practical to apply Theorem 2. We remark that even though the Gröbner basis in the example above consists of 119 polynomials, a relatively small set of these polynomials can be used to decode all occurrences of two errors, and fewer than ten

of these polynomials could be used to decode almost all occurrences of two errors. Notice that once a subset of polynomials from the Gröbner basis has a small number of common roots, then these roots can be checked in the original system of equations to see which of them correspond to the actual errors.

The usual algorithm used to find Gröbner bases can vary doubly exponentially with the maximum degree of the polynomials generating the ideal (cf. [8, p. 110]). The presence of the polynomials $X_i^q - X_i$ in our ideals means that computations can be massive over large fields. In examples we have computed, we have been able to deal with some small codes over $\mathbf{F}_{16}$, but not with larger fields.

References

1. W. W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, American Mathematical Society (1994).
2. D. Bayer and M. Stillman, Macaulay: A system for computation in algebraic geometry and commutative algebra.
3. M. de Boer and R. Pellikaan, Gröbner bases for error-correcting codes, EIDMA/Galois Minicourse on Computer Algebra, Eindhoven University of Techonology, September 27–30 (1995).
4. X. Chen, I. S. Reed, T. Helleseth, and T. K. Truong, Use of Gröbner bases to decode binary cyclic codes up to the true minimum distance *IEEE Transactions on Information Theory*, Vol. 40, No. 5 (1995) pp. 1654-1661.
5. X. Chen, I. S. Reed, T. Helleseth, and T. K. Truong, General principles for the algebraic decoding of cyclic codes, *IEEE Transactions on Information Theory*, Vol. 40, No. 5 (1995) pp. 1661-1663.
6. X. Chen, I. S. Reed, T. Helleseth, and T. K. Truong, Algebraic decoding of cyclic codes: A polynomial ideal point of view, *Finite Fields: Theory, Applications, and Algorithms (Las Vegas, NV, 1993)*, Contemp. Math. 168, Amer. Math. Soc., Providence (1994) pp.15–22.
7. A. B. Cooper, Toward a new method of decoding algebraic codes using Gröbner bases, *Transactions of the 10th Army Conference on Applied Mathematics and Computing*, West Point, NY (1992), pp. 1-11.
8. D. Cox, J. Little, and D. O'Shea: *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer-Verlag, New York (1992).
9. P. Delsarte, J. M. Goethals, and F. J. MacWilliams, On generalized Reed-Muller codes and their relatives, *Information and Control*, Vol. 16 (1970) pp. 403-442.
10. G. L. Feng and T. R. N. Rao, Improved geometric Goppa codes, part I: basic theory, *IEEE Transactions on Information Theory*, Vol. 41, No. 6 (1995) pp. 1678-1693.
11. T. Høholdt, J. H. van Lint, and R. Pellikaan, Algebraic geometry codes, preprint (1996).
12. H. Kredel, *MAS* (computer program), Universität Passau, (1993).
13. J. H. van Lint and G. van der Geer, *Introduction to Coding Theory and Algebraic Geometry*, Birkhäuser Verlag, Basel, (1988).
14. P. Loustaunau and E. V. York, On the decoding of cyclic codes using Gröbner bases, preprint.
15. H. M. Möller and B. Buchberger, The construction of multivariate polynomials with preassigned zeros, *Computer Algebra. EUROCAM '82, European Computer Algebra Conference*, Marseille, France, Lecture Notes in Computer Science, Springer-Verlag, Berlin–New York (1982) pp. 24–31.
16. R. Pellikaan, B.Z. Shen, and G.J.M. van Wee, Which linear codes are algebraic-geometric? *IEEE Transactions on Information Theory*, Vol. 37, No. 3 (1991) pp. 583–602.
17. C. Rong and T. Helleseth, Use characteristic sets to decode cyclic codes up to actual minimum distance, *Finite Fields and Applications*, London Mathematical Society Lecture Notes 233, Cambridge University Press (1996).
18. C. Rong and T. Helleseth, On methods of using Gröbner bases to decode cyclic codes up to actual minimum distance, preprint.
19. A. Seidenberg, Constructions in algebra, *Transactions of the American Mathematical Society*, Vol. 197 (1974) pp. 273-313.
20. K. Saints and C. Heegard, Algebraic-geometric codes and multidimensional cyclic codes: a unified theory and algorithms for decoding using Gröbner bases, *IEEE Transactions on Information Theory*, Vol. 41, No. 6, (1995) pp. 1733–1751.

21. K. Yang and P. V. Kumar, On the true minimum distance of Hermitian codes, *Coding Theory and Algebraic Geometry: Proceedings of AGCT-3, Luminy, France, June 1991* (H. Stichtenoth and M. A. Tsfasman, eds.), Lecture Notes in Mathematics, Springer-Verlag, New York (1992) pp. 99–107.