Automorphisms and Encoding of AG and Order Domain Codes

John B. Little
Department of Mathematics and Computer Science
College of the Holy Cross
Worcester, MA 01610 USA
little@mathcs.holycross.edu

June 25, 2007

Abstract

We survey some encoding methods for AG codes, focusing primarily on one approach utilizing code automorphisms. If a linear code C over $\mathbb{F}_q$ has a finite abelian group H as a group of automorphisms, then C has the structure of a module over a polynomial ring $\mathcal{P}$. This structure can be used to develop systematic encoding algorithms using Gröbner bases for modules. We illustrate these observations with several examples including geometric Goppa codes and codes from order domains.

1 Introduction

In order for a code to be useful in practice, it should admit efficient encoding and efficient decoding. Although most of the research effort on algebraic geometric (AG) Goppa codes from curves has focused on the decoding side, several approaches have been considered for encoding as well.

In this article we will briefly survey several approaches to encoding these codes. We will then concentrate on a systematic encoding method based on the fact that codes possessing permutation automorphisms have the structure of modules over polynomial rings. This discussion is based on Heegard, Little,

and Saints, [HLS], which shows how to use module Gröbner bases for such codes to construct encoders. This approach is a direct generalization of the commonly-used polynomial division encoding method for cyclic codes that appears in most textbook treatments of coding theory. The module Gröbner basis furnishes an analog of the generator polynomial of a cyclic code (see Theorem 2). This particular connection between encoding and Gröbner bases was well-established previously in the case of abelian (m-dimensional cyclic) codes. See, for instance, [PH], section 6.1.6, or Chapter 9 of [CLO]. Since it relies only on the presence of suitable groups of code automorphisms, it applies to many classes of codes, including cyclic, quasi-cyclic, abelian, and many Goppa-type evaluation codes from curves, higher-dimensional varieties, and order domains. In the last three cases, interesting code automorphisms often arise from automorphisms of the underlying algebraic variety (see §6). Some results on implementation of this approach in hardware for the case of codes from the Hermitian curves considered in §7 have been reported by Chen and Lu, [CL].

To conclude this introduction, we note that codes with sufficiently large automorphism groups may also be amenable to *permutation decoding*. In this decoding method, a fixed collection of code automorphisms is applied to the received word. If the error weight is sufficiently small, at least one of the automorphisms will move the errors out of the information positions. Then the correct information symbols can be re-encoded to accomplish the decoding. Chabanne, [C], has considered this decoding method from the point of view of Gröbner bases in the case of abelian codes, and [L1] gives an example for a Hermitian code.

2 Other Encoding Methods for AG Goppa Codes

The most basic encoding method for these codes simply treats them as linear codes and uses matrix multiplication of the information word with any generator matrix G to do the encoding.

In the article [MOS], Matsumoto, Oishi, and Sakaniwa propose a faster encoding method for the one-point residue codes $C_\Omega(D, mQ)$ (and also their dual codes). This method is based on the structure of a special basis

$$\{x^i\omega_j : 0 \leq j \leq a-1, v_Q(x^i\omega_j) \geq m\}$$

for the vector space of differentials $\Omega(mQ - D)$. Here x is an element of the Riemann-Roch space $L(aQ)$, where a is the smallest pole order of a nonconstant function with poles only at Q. The ω_j are differentials in $\Omega(-\infty Q - D)$ having the maximum valuation at Q among differentials ω such that $v_Q(\omega) - j$ is divisible by a. The resulting generator matrix G possesses a block factorization that can be exploited to reduce the number of multiplications involved in computing a product of the form xG. This method does not make use of Gröbner bases and yields a nonsystematic encoder.

More recently, Matsui and Mita, [MM], have described a method combining discrete Fourier transforms (DFT) and Gröbner bases that yields a systematic encoder for the $C_\Omega(D, mQ) = C_L(D, mQ)^\perp$ codes from a $C_{a,b}$ curve. Their method works as follows. A pair (i, j) with $0 \leq i, j \leq q-1$ can represent either the monomial $x^i y^j$ or the point (α^i, α^j) where α is a primitive element of the field. For simplicity, assume D is supported at points in $(\mathbb{F}_q{}^*)^2$. Partition the support into two subsets: a set of information positions P' of cardinality k, and a set of parity-checks P of cardinality $n - k = \dim L(mQ)$, where Q is the point at infinity on the $C_{a,b}$ curve. A Gröbner basis G for the ideal $\mathbf{I}(P)$ is pre-computed. For most choices of P, the monomials in the footprint or Gröbner éscalier are identified with the collection of pairs (i, j) as above with $ai + bj \leq m$.

To encode a given information word $a = (a_{(i,j)} : (i, j) \in P')$, the DFT A is computed, where $A_{(i,j)} = f(\alpha^i, \alpha^j)$ for the polynomial

$$f(x, y) = \sum_{(\alpha^k, \alpha^l) \in P'} a_{(k,l)} x^k y^l.$$

The portion of the DFT corresponding to (i, j) with $ai + bj \leq m$ is then extended to an array A' for all (i, j) with $0 \leq i, j \leq q - 1$ by means of the Gröbner basis G. The difference array $A - A'$ represents the DFT of a codeword in $C_\Omega(D, mQ)$ since its syndromes corresponding to $x^i y^j$ with $ai + bj \leq m$ are all zero. Moreover it can be seen that the inverse DFT of $A - A'$ provides a systematic encoding of the information a.

3 Automorphisms and module structures

We now prepare for another encoding method by introducing some general information on automorphisms of codes and module structures. The symmetric group S_n acts on $\mathbb{F}_q^n$ by permuting the entries of vectors. A permutation

automorphism of a linear code $C \subset \mathbb{F}_q^n$ is an element of S_n that maps the set of codewords to itself. We will only consider code automorphisms of this type in the following.

Let C be a code that has a nontrivial abelian group H of automorphisms. For instance, the ordinary cyclic codes and m-dimensional cyclic codes (also known as abelian codes) are well-studied examples. For simplicity of notation, we will usually restrict to the case that $H = \langle \sigma \rangle$ is cyclic. The generalization to the product of several cyclic groups is essentially immediate. With the restriction to cyclic groups H, cyclic codes are the most basic examples. But note that we do not assume that H acts transitively on the set of codeword components. Hence, for instance, the *quasicyclic* codes of length n also have this sort of structure (by definition, C is quasicyclic if its automorphism group contains an m-fold cyclic shift for some m dividing n) .

Let O_i, $i = 1, \ldots, r$ be the *orbits* of the components of the codewords c under the action of H. Pick any component $c_{i,0}$ in the ith orbit and label the components in that orbit as $c_{i,j}$ where $j = 0, \ldots, |\, O_i| - 1$. With the convention that the second index is an integer modulo $|\, O_i|$, the action of σ can be written as $\sigma(c_{i,j}) = c_{i,j+1}$ for all $i = 1, \ldots, r$, and $j = 0, \ldots, |\, O_i| - 1$.

For the remainder of this article, $\mathcal{P}$ will denote the polynomial ring in one variable $\mathbb{F}_q[t]$. As usual, let $\mathbf{e}_i$ be the ith standard basis vector in the free module $\mathcal{P}^r$. Then the orbit structure of the components of the codewords of C determines the submodule $\langle (t^{|O_i|} - 1)\mathbf{e}_i : i = 1, \ldots, r \rangle$ of $\mathcal{P}^r$. We can view the code C as subset of the quotient module

$$N = \mathcal{P}^r / \langle (t^{|O_i|} - 1)\mathbf{e}_i : i = 1, \ldots, r \rangle, \tag{1}$$

via the mapping

$$\begin{aligned} \phi : C &\rightarrow N \\ (c_{i,j}) &\mapsto \sum_{i=1}^{r} \left(\sum_{j=0}^{|O_i|-1} c_{i,j} t^j \right) \mathbf{e}_i \bmod \langle (t^{|O_i|} - 1)\mathbf{e}_i : i = 1, \ldots, r \rangle. \end{aligned}$$

We have the following theorem describing the structure of the image $\phi(C)$.

Theorem 1 *Let C linear block code over $\mathbb{F}_q$ with a cyclic group H of automorphisms and ϕ, N be as above. Then $\phi(C)$ has the structure of a $\mathcal{P}$-submodule of N.*

Proof: First ϕ is linear, so $\phi(C)$ is an $\mathbb{F}_q$-vector subspace of N. By the definition of ϕ, if $c \in C$ is any codeword, multiplication of $\phi(c)$ by t yields

$$\begin{aligned} t \cdot \phi(c) &= \sum_{i=1}^{r} \left(\sum_{j=0}^{|O_i|-1} c_{i,\,j} t^{j+1} \right) \mathbf{e}_i \\ &\equiv \sum_{i=1}^{r} \left(\sum_{j=0}^{|O_i|-1} c_{i,\,j-1} t^{j} \right) \mathbf{e}_i \bmod N \\ &= \phi(\sigma^{-1}(c)). \end{aligned}$$

By hypothesis, this is another element of $\phi(C)$. Hence $\phi(C)$ is closed under multiplication by t, hence under multiplication by all polynomials in $\mathcal{P}$. It follows that $\phi(C)$ is a $\mathcal{P}$-submodule of N. $\square$

Note that if the theorem applies to a code C, it applies to the dual code $C^{\perp}$ as well.

In [HLS], [LSH], and [L1], this essentially straightforward generalization of the usual construction showing that a cyclic code of length n over $\mathbb{F}_q$ is an ideal in $\mathcal{P}/\langle t^n - 1 \rangle$ was applied to some AG Goppa codes. We will present several explicit examples in §7. The article [LF] applies the module structures described here to study quasicyclic codes. Theorem 1 can also be generalized to more general finite abelian automorphism groups. In those cases, we obtain module structures over the polynomial ring in s variables if a minimal generating set for H has s elements.

4 A systematic encoding algorithm

We will now show how the theory of Gröbner bases for modules can be applied to work with these codes. Let $\mathsf{M}(C)$ be the submodule of $\mathcal{P}^r$ corresponding to $\phi(C) \subset N$ under the mapping

$$\pi : \mathcal{P}^r \to N,$$

where N is the quotient module from (1). The key observation here is that the canonical form algorithm with respect to a Gröbner basis G for $\mathsf{M}(C)$ with respect to any term ordering $\prec$ on $\mathcal{P}^r$ can be used to produce a systematic encoder for C.

The encoding algorithm can be described succinctly using the standard and nonstandard terms for $\mathsf{M}(C)$. Following the general notational conventions of this volume, $\mathbf{N}_{\prec}(\mathsf{M}(C))$ will denote the *Gröbner éscalier* or "footprint" of the module $\mathsf{M}(C)$ with respect to a term order $\prec$. Similarly, $\mathbf{T}_{\prec}(\mathsf{M}(C))$ will denote the leading term module of $\mathsf{M}(C)$. The terms $t^j\mathbf{e}_i \in \mathbf{N}_{\prec}(\mathsf{M}(C))$ will be called the *standard terms*. The *nonstandard terms* are the $t^j\mathbf{e}_i$ with $j \leq |\,O_i| - 1$ contained in $\mathbf{T}_{\prec}(\mathsf{M}(C))$.

In this method, the coefficients of the nonstandard terms give the information positions in the codewords, and the coefficients of the standard terms are the parity checks. The precise statement of the encoding method is given in the following theorem.

Theorem 2 *Let G be a Gröbner basis for the module $\mathsf{M}(C)$ with respect to a term ordering $\prec$ on $\mathcal{P}^r$. The algorithm below produces a codeword c in all cases and gives a systematic encoder for the code C.*

Input: G, the nonstandard terms m_i, information symbols c_i
Output: c, a codeword

$f = \sum c_i m_i$;
$c := f - \mathbf{CanonicalForm}(f, G)$;

Proof: Since

$$\mathbf{CanonicalForm}(c) = \mathbf{CanonicalForm}(f - \mathbf{CanonicalForm}(f, G), G) = 0,$$

it follows that $c \in \mathsf{M}(C)$, which means that c represents a codeword of C. The information symbols appear as coefficients of the nonstandard terms in f, but $\mathbf{CanonicalForm}(f, G)$ is a linear combination of standard terms. The sets of nonstandard and standard terms are disjoint, hence this encoder is systematic, in the sense that the information symbols appear unchanged in a subset of the codeword entries. □

Some important examples of the term orderings that can be used here are obtained as follows. First order the $\mathbf{e}_j$ themselves; we will use

$$\mathbf{e}_1 > \mathbf{e}_2 > \cdots > \mathbf{e}_r,$$

but the opposite order is also possible and is used too. The *position over term* (or POT) ordering on $\mathcal{P}^r$ is defined by

$$t^i \mathbf{e}_j \prec_{POT} t^k \mathbf{e}_\ell$$

if $j > \ell$, or $j = \ell$ and $i < k$. Reversing the way the comparison is made, we obtain the *term over position* (or TOP) ordering on $\mathcal{P}^r$:

$$t^i \mathbf{e}_j \prec_{TOP} t^k \mathbf{e}_\ell$$

if $i < k$, or $i = k$ and $j > \ell$.

5 Complexity Comparisons

The basic encoding method described at the start of §2 requires kn products and $(k-1)n$ sums in $\mathbb{F}_q$ to compute the matrix product xG if G is a general, dense generator matrix. By way of comparison, the method of [MOS] described in §2 effectively reduces the storage space and the number of operations needed. However, as noted above, this encoding method is not systematic.

One potential advantage of exploiting the module structures described in Theorem 1 is that, as is true for the generator polynomial of a cyclic code, a Gröbner basis for $\mathsf{M}(C)$ is typically significantly smaller than a full systematic generator matrix. The exact savings in stored information (or the size of the circuit in hardware) required for the encoding depends on the particular code. However, the situation in Example 2 in §7 below is quite typical. The code C there is a $[64, 44, 8]$ code over $\mathbb{F}_8$. A reduced echelon form systematic generator matrix would be a 44×64 matrix $G = (I|X)$ with X a 44×20 block of potentially nonzero entries. The Gröbner basis for the module $\mathsf{M}(C)$ has 10 generators, which contain at most

$$5 \times 2 + 6 \times 4 + 7 \times 6 + 8 \times 7 + 9 = 141$$

nonzero, non-leading terms. The division algorithm used for encoding in Theorem 2 takes roughly the same amount of arithmetic as the matrix product xG (see [HLS]).

The authors of [MM] conjecture that their method requires less field arithmetic than multiplication xG with a systematic generator matrix but do not prove this. The Gröbner basis for the ideal $\mathbf{I}(P)$ would typically be even smaller than the Gröbner basis for the module $\mathsf{M}(C)$ when there is a module structure.

6 Automorphisms of curves and AG Goppa codes

In [HLS], it was pointed out that many examples of AG Goppa codes have the module structures described in Theorem 1, hence systematic encoders as described in Theorem 2, because of the presence of automorphisms of the underlying curves. Indeed, many interesting curves with large numbers of $\mathbb{F}_q$-rational points also tend to have large automorphism groups.

Let $\mathcal{X}$ be a smooth projective algebraic curve defined over $\mathbb{F}_q$. An automorphism of $\mathcal{X}$ is a regular mapping from $\mathcal{X}$ to itself with a regular inverse. An automorphism σ of $\mathcal{X}$ defined over $\mathbb{F}_q$ induces an $\mathbb{F}_q$-automorphism of the function field $K = \mathbb{F}_q(\mathcal{X})$ (an isomorphism of fields from K to itself that is the identity on $\mathbb{F}_q$) via $f \mapsto f \circ \sigma^{-1}$. The set of all automorphisms of $\mathcal{X}$ forms a group $\mathrm{Aut}(\mathcal{X})$ under function composition and $\mathrm{Aut}(\mathcal{X})$ acts on divisors on $\mathcal{X}$ in the obvious way: $\sigma(\sum n_P P) = \sum n_P \sigma(P)$.

In fact, all of the examples of automorphisms we will consider will be induced by invertible linear mappings on the ambient projective space of $\mathcal{X}$. If such a mapping takes the curve $\mathcal{X}$ to itself, then it induces an automorphism of $\mathcal{X}$.

For instance, consider the Hermitian function fields and curves over $\mathbb{F}_{q^2}$. The Hermitian curve may be defined as the variety

$$\mathcal{V}(x_0^{q+1} + x_1^{q+1} + x_2^{q+1}) \subset \mathbb{P}^2,$$

where $(x_0 : x_1 : x_2)$ is the homogeneous coordinate vector of a point in $\mathbb{P}^2$. In section VI.3 of [S], it is shown that (in geometric language) the tangent line to this curve at an $\mathbb{F}_{q^2}$-rational point can be taken to the line at infinity by a linear change of coordinates in $\mathbb{P}^2$. When that is done, the defining equation is taken to the form given in the following

$$\mathcal{HC}_q = \mathcal{V}(x^{q+1} - y^q z - y z^q) = \{(x : y : z) \in \mathbb{P}^2 : x^{q+1} - y^q z - y z^q = 0\}. \quad (2)$$

We will use this form of the equations of the Hermitian curves. Let α be a primitive element of $\mathbb{F}_{q^2}$. The mapping

$$\begin{aligned} \sigma : \mathbb{P}^2 &\rightarrow \mathbb{P}^2 \\ (x : y : z) &\mapsto (\alpha x : \alpha^{q+1} y : z) \end{aligned} \quad (3)$$

induces an automorphism of the curve $\mathcal{HC}_q$ because it is easy to check that if the point $(x : y : z)$ satisfies the equation in (2), the same is true of $\sigma(x : y : z)$.

In the construction of an AG Goppa evaluation code on a curve $\mathcal{X}$, recall that one begins by selecting $\mathbb{F}_q$-rational divisors $D = \sum_{i=1}^{n} P_i$ and E with disjoint supports on $\mathcal{X}$. The codewords are obtained by evaluating the rational functions f in the vector space

$$L(E) = \{f : (f) + E \geq 0\} \cup \{0\}$$

at the points in D:

$$\begin{aligned} ev : L(E) &\rightarrow \mathbb{F}_q^n \\ f &\mapsto (f(P_1), \ldots, f(P_n)). \end{aligned}$$

The image of the evaluation mapping is the AG Goppa evaluation code $C_L(D, E)$.

Theorem 3 *In this situation, let σ be an automorphism of the curve $\mathcal{X}$ and assume the divisors D and E are fixed by σ. Then σ induces an automorphism of the code $C_L(D, E)$.*

Proof: Since σ fixes the divisor E, it follows that $f \mapsto f \circ \sigma^{-1}$ takes $L(E)$ to itself. Hence we can define an action of σ on the codewords of $C_L(D, E)$ by

$$(f(P_1), \ldots, f(P_n)) \mapsto (f(\sigma^{-1}(P_1)), \ldots, f(\sigma^{-1}(P_n))).$$

Since the divisor D is also assumed to be fixed by σ, this means that the points $\{\sigma^{-1}(P_i)\}$ are a permutation of the $\{P_i\}$. Hence σ induces a permutation automorphism of the code $C_L(D, E)$. $\square$

By Proposition VII.3.3 of [S], the subgroup $\langle\sigma\rangle$ of $\mathrm{Aut}(\mathcal{X})$ can be viewed as a subgroup of the permutation automorphism group of $C_L(D, E)$ whenever $n > 2g + 2$, where g is the genus of $\mathcal{X}$. Furthermore, Joyner and Ksir, [JK], have given conditions under which the permutation automorphism group of $C_L(D, E)$ is isomorphic to the subgroup of $\mathrm{Aut}(\mathcal{X})$ fixing D and E.

Because of these observations, Theorems 1 and 2 from §3 apply to any $C_L(D, E)$ code from a curve $\mathcal{X}$ with an automorphism σ fixing D and E, provided $n = \deg D$ is sufficiently large. In the case of maximal length one-point codes ($E = aQ$ for some point Q, $a \geq 0$, and D the sum of the other $\mathbb{F}_q$-rational points), it suffices to find a σ defined over $\mathbb{F}_q$ fixing Q. One usually takes σ with maximal order to make the number of orbits as small as possible.

7 Examples

Example 1. As shown in section VII.4 of [S], the Hermitian curve $\mathcal{HC}_q$ is a smooth plane curve of degree $q+1$, hence has genus $q(q-1)/2$. In addition, $\mathcal{HC}_q$ has q^3+1 $\mathbb{F}_{q^2}$-rational points. There are q^3 affine points. In the coordinates used in (2), there are q points on each line $x=c$ and $Q=(0:1:0)$ at infinity. As is well-known, this is the maximum number possible for a curve of genus $g=q(q-1)/2$ over $\mathbb{F}_{q^2}$ by the Hasse-Weil bound. If $g=g(\mathcal{X})=q(q-1)/2$, then

$$|\mathcal{X}(\mathbb{F}_{q^2})| \leq 1+q^2+2gq = 1+q^2+q(q-1)q = q^3+1.$$

With $q=2$, we get the picture of the $\mathbb{F}_4$-rational points on the Hermitian curve $\mathcal{V}(x^3+y^2z+yz^2)$ given below in Figure 1.

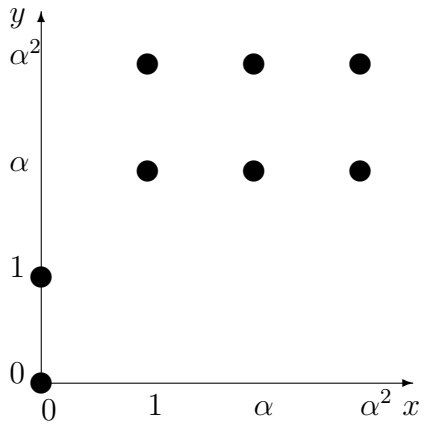

Figure 1. The $\mathbb{F}_4$-rational points of the Hermitian curve with $q=2$.

The mapping σ from (3) is an automorphism of of the Hermitian curve fixing Q and permuting the q^3 affine $\mathbb{F}_{q^2}$-rational points. The subgroup of the full automorphism group generated by σ has order q^2-1. Theorem 3 and the construction from §3 apply if we take the divisor $E=aQ$ for any $a \geq 0$, and let D be the sum of the q^3 affine $\mathbb{F}_{q^2}$-rational points, each with coefficient 1.

In the case $q=2$, the automorphism σ is given by

$$\sigma(x:y:z) = (\alpha x:y:z)$$

(since $\alpha^3 = 1$). This permutes the eight affine $\mathbb{F}_4$-rational points in four orbits, two of length three, and two of length one:

$$\begin{aligned} O_1 &= \{(1:\alpha:1),(\alpha:\alpha:1),(\alpha^2:\alpha:1)\} \\ O_2 &= \{(1:\alpha^2:1),(\alpha:\alpha^2:1),(\alpha^2:\alpha^2:1)\} \\ O_3 &= \{(0:0:1)\} \\ O_4 &= \{(0:1:1)\}. \end{aligned}$$

There are similar patterns for the orbits of $G = \langle\sigma\rangle$ on the $\mathbb{F}_{q^2}$-rational points in D for any q Under σ there are q orbits of length q^2-1 (all coordinates nonzero), one orbit of length $q-1$ (the points with $x = 0$, $y \neq 0$), and one orbit of length 1 (a fixed point – $\{(0:0:1)\}$). See [HLS] and [LSH] for more detail on these Hermitian examples.

We next show the module structure for the code $C = C_L(D, 3Q)$ from the Hermitian curve over $\mathbb{F}_4$ and a Gröbner basis in detail. The affine coordinate functions x/z and y/z are elements of $L(3Q)$, as is $1 = z/z$. Hence, if we order the $\mathbb{F}_4$-rational points on H according to the orbit structure above (listing the points in O_1, then O_2, then O_3, and finally O_4), the code $C_L(D, 3Q)$ has generator matrix

$$\mathcal{M} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & 1 & \alpha & \alpha^2 & 0 & 0 \\ \alpha & \alpha & \alpha & \alpha^2 & \alpha^2 & \alpha^2 & 0 & 1 \end{pmatrix}.$$

and parameters $[n, k, d] = [8, 3, 5]$ over $\mathbb{F}_4$ (incidentally, the best possible d for this n, k over $\mathbb{F}_4$).

Under the mapping ϕ from §3, the first row corresponds, for instance, to the module element

$$(1 + t + t^2, 1 + t + t^2, 1, 1).$$

With respect to the $\prec_{POT}$ term ordering, the reduced Gröbner basis G for the submodule of $\mathcal{P}^4$ corresponding to $\phi(C)$ is:

$$\begin{aligned} g_1 &= (\alpha + t, \alpha + t, \alpha^2, \alpha^2) \\ g_2 &= (0, 1 + t + t^2, \alpha, \alpha^2) \\ g_3 &= (0, 0, 1 + t, 0) \\ g_4 &= (0, 0, 0, 1 + t). \end{aligned}$$

The element g_1, for instance, equals the linear combination

$$\alpha^2(1+t+t^2, 1+t+t^2, 1, 1) + (1+\alpha t+\alpha^2 t^2, 1+\alpha t+\alpha^2 t^2, 0, 0)$$

of the module elements from rows 1 and 2 of $\mathcal{M}$ which would be computed in the course of Buchberger's algorithm. (Recall that $\alpha^2+\alpha+1=0$ in $\mathbb{F}_4$.)

In the systematic encoding presented in Theorem 2, we have

- Information positions: coefficients of t^2e_1, te_1, t^2e_2.
- Parity checks: coefficients of e_1, te_2, e_2, e_3, e_4.

Then, to do encoding in this example, it suffices to compute remainders on division by G. For the $\prec_{POT}$ term ordering, this amounts to ordinary polynomial divisions in each component. For example, if we want to encode

$$f = (t+\alpha t^2, \alpha^2 t^2, 0, 0),$$

it is easy to check that dividing first by g_1, then g_2 yields

$$\mathbf{CanonicalForm}(f, G) = (\alpha^2, \alpha, \alpha, \alpha^2).$$

The corresponding codeword is

$$c = f - \mathbf{CanonicalForm}(f, G) = (\alpha^2+t+\alpha t^2, \alpha+\alpha^2 t^2, \alpha, \alpha^2).$$

As indicated in the proof of Theorem 2, the information from the coefficients of f is visible immediately in the codeword c, so this is a systematic encoding method.

We note that Hermitian curves have many automorphisms besides those in the subgroup generated by σ above. Indeed, for some q, there are σ of order larger than q^2-1 fixing Q and D (see [HLS]). Moreover, by [S], VII.4.6, there is also a nonabelian subgroup $\overline{H}$ of order $|\overline{H}| = (q^2-1)q^3$ in the full automorphism group of the Hermitian curve that fixes both the point at infinity Q, and the divisor D, hence induces automorphisms of $C_L(D, aQ)$ for all a. The elements of this subgroup can be written as the mappings

$$\tau_{\lambda,\,\delta,\,\mu}(x : y : z) = (\lambda x + \delta z : \lambda^{q+1} y + \lambda\delta^q x + \mu z : z),$$

where $\lambda \in \mathbb{F}_{q^2}^*$, and $(\delta : \mu : 1)$ is any affine $\mathbb{F}_{q^2}$-rational point on the curve. Note that

$$\tau_{\lambda,\,\delta,\,\mu}(0 : 0 : 1) = (\delta : \mu : 1).$$

This implies that $\overline{H}$ acts *transitively* on the affine $\mathbb{F}_{q^2}$-rational points, or equivalently, that there is only one orbit of points under $\overline{H}$. Consequently, the codes $C_L(D, aQ)$ can also be studied as *ideals* in the group algebra $\mathbb{F}_{q^2}[\overline{H}]$. Since $\overline{H}$ is not abelian, however, the analogs of Gröbner bases in the group algebra do not seem to be as convenient for encoding. $\Diamond$

AG Goppa codes from several other classes of curves with the maximal number of rational points for their genus over the given field $\mathbb{F}_q$ can be treated in a very similar fashion.

Example 2. Let $q = 2^{2n+1}$, $q_0 = 2^n$ and let $\mathcal{Y}_n$ be the curve over $\mathbb{F}_q$ defined by the affine equation

$$x^q + x = y^{q_0}(y^q + y).$$

These curves were studied by Hansen and Stichtenoth in [HS], and by a number of other authors. With $n = 1$, for example, the curve $\mathcal{Y}_1$ over $\mathbb{F}_8$ in this family has affine equation

$$x^8 + x = y^2(y^8 + y).$$

This defines a curve of degree 10, genus 14, with a single (singular) point Q at infinity. The singularity at Q is a cuspidal (unibranch) singularity – more precisely, there is only one point $\widetilde{Q}$ that lies over Q on the normalization (smooth model) $\widetilde{\mathcal{Y}_n} \to \mathcal{Y}_n$.

From the point of view of coding theory, the curves $\mathcal{Y}_n$ are interesting because they have as many $\mathbb{F}_q$-rational points as possible for a curve of their genus (however, the Hasse-Weil bound is not sharp in these cases). Indeed, $\mathcal{Y}_n$ passes through *every point* of the affine plane over $\mathbb{F}_q$. For constructing AG Goppa evaluation codes from $\mathcal{Y}_n$, one can use $G = a\widetilde{Q}$ and D the sum of the q^2 $\mathbb{F}_q$-rational affine points, each with coefficient 1.

Letting α denote a primitive element of $\mathbb{F}_q$, the mapping

$$\sigma(x, y) = (\alpha^{q_0+1}x, \alpha y) \tag{4}$$

restricts to an automorphism of $\mathcal{Y}_n$. Since σ fixes the divisors D and $G = a\widetilde{Q}$, σ induces an automorphism of each of the codes $C_L(D, a\widetilde{Q})$ constructed from $\mathcal{Y}_n$, by Theorem 3. The automorphism σ has order $q - 1$ in $\mathrm{Aut}(\mathcal{Y}_n)$. The following explicit example of the module structure of one of these codes comes from [L1].

The code $C = C_L(D, 57\widetilde{Q})$ on the Hansen-Stichtenoth curve $\mathcal{Y}_1$ has parameters $n = 64$, $k = 44$, $d = 8$ by [CD]. The automorphism σ from (4) permutes the points of D in 10 orbits, 9 of length 7 and one of length 1. The semigroup of pole orders at $\widetilde{Q}$ of rational functions on the curve $\mathcal{Y}_1$ is generated by the natural numbers $8, 10, 12, 13$. Moreover $y \in L(8\widetilde{Q})$, $x \in L(10\widetilde{Q})$, $f = y^5 + x^4 \in L(12\widetilde{Q})$, and $g = yx^4 + y^{20} + x^{16} \in L(13\widetilde{Q})$ (see [HS]). We use these functions to generate a basis for $L(57\widetilde{Q})$, the normalization $\mathbb{F}_8 = \mathbb{F}_2[\alpha]/\langle \alpha^3 + \alpha + 1 \rangle$, and the orbit representatives $(1, \alpha^6), \ldots, (1, \alpha), (1, 1), (0, 1), (1, 0), (0, 0)$ (in that order). The reduced $\prec_{POT}$ Gröbner basis G of the module $\mathsf{M}(C)$ has the form

$$
\begin{aligned}
g_1 &= (1, 0, 0, 0, 0, *, *, *, *, *) \\
g_2 &= (0, 1, 0, 0, 0, *, *, *, *, *) \\
g_3 &= (0, 0, 1, 0, 0, *, *, *, *, *) \\
g_4 &= (0, 0, 0, 1, 0, *, *, *, *, *) \\
g_5 &= (0, 0, 0, 0, 1, *, *, *, *, *) \\
g_6 &= (0, 0, 0, 0, 0, t^2 + (\alpha^2 + \alpha)t + \alpha + 1, *, *, *, *) \\
g_7 &= (0, 0, 0, 0, 0, 0, t^4 + (\alpha + 1)t^3 + (\alpha^2 + 1)t^2 + \alpha^2 + \alpha + 1, *, *, *) \\
g_8 &= (0, 0, 0, 0, 0, 0, 0, t^6 + t^5 + t^4 + t^3 + t^2 + t + 1, 0, 0) \\
g_9 &= (0, 0, 0, 0, 0, 0, 0, 0, t^7 + 1, 0) \\
g_{10} &= (0, 0, 0, 0, 0, 0, 0, 0, 0, t + 1).
\end{aligned}
$$

(To save space, the coefficients in the non-maximal terms are omitted. Also, it is only the maximal terms that determine the information positions and parity check positions for the code.)

Like the Hermitian curves, the Hansen-Stichtenoth curve $\mathcal{Y}_1$ has many automorphisms besides those in the subgroup generated by the σ from (4) we have used. There is a (non-abelian) subgroup $\overline{H}$ of $Aut(\mathcal{Y}_1)$, of order 448 that fixes both $a\widetilde{Q}$ and D, hence induces automorphisms of each $C_L(D, a\widetilde{Q})$ code. The elements of this subgroup can be written as

$$\tau_{\lambda, \delta, \mu}(x, y) = (\lambda^3 x + \lambda\delta^2 y + \mu, \lambda y + \delta),$$

where $\lambda \in \mathbb{F}_8^*$, and (μ, δ) is any affine $\mathbb{F}_8$-rational point on $\mathcal{Y}_1$. Once again, $\overline{H}$ acts transitively on the points of D, and the codes $C_L(D, a\widetilde{Q})$ are *ideals* in the group algebra $\mathbb{F}_8[\overline{H}]$. $\Diamond$

Codes from both the Hermitian and Hansen-Stichtenoth curves can be studied with the language of order domains introduced in [HLP]. Higher-dimensional varieties can also be used to construct examples of order domains and generalized Goppa-type evaluation codes. See, for instance, [GP] and [L2] for a general discussion of order domains, how they arise, and how the theory of Gröbner bases yields key insights about their structure and their special relevance for coding theory.

Example 3. For instance let

$$\mathcal{HS}_q = \mathcal{V}(x_0^{q+1} + x_1^{q+1} + x_2^{q+1} + x_3^{q+1})$$

be the Hermitian surface in $\mathbb{P}^3$. The variety $\mathcal{HS}_q$ has

$$(q^2+1)(q^3+1)$$

$\mathbb{F}_{q^2}$-rational points. Changing coordinates to put a tangent plane to the surface as the plane at infinity gives the affine surface

$$\mathcal{HS}'_q = \mathcal{V}(x^{q+1} + y^{q+1} - z^q - z)$$

(whose affine coordinate ring has an order domain structure). $\mathcal{HS}'_q$ has q^5 $\mathbb{F}_{q^2}$-rational points. $\mathcal{HS}'_q$ also has many automorphisms, for instance

$$\sigma(x,y,z) = (\alpha x, \alpha y, \alpha^{q+1} z)$$

(of order $= q^2 - 1$). This σ fixes the plane at infinity and permutes the q^5 $\mathbb{F}_{q^2}$-rational points in $q^3 + q$ orbits of size $q^2 - 1$, one of size $q - 1$, and one of size 1. So Theorem 1 applies to all evaluation codes constructed from $\mathcal{H}'$ and subspaces $L \subset \mathbb{F}_{q^2}[x,y,z]$. For instance, the code from the Hermitian surface over $\mathbb{F}_4$ constructed by evaluating $1, x, y, z$ has $[n,k,d] = [32,4,22]$. The minimum weight codewords come by evaluating linear polynomials that define the tangent plane at one of the $\mathbb{F}_4$-rational points on the surface. The minimum distance $d = 22$ equals the best possible for a code with $n = 32$, $k = 4$ over $\mathbb{F}_4$ by Brouwer's online tables. But these codes also have Gröbner basis encoding, and good decoding algorithms because of the extra order domain structure. $\Diamond$

References

[C] Chabanne, H. "Permutation decoding of abelian codes," *IEEE Trans. on Inform Theory* **38** (1992), 1826–1829.

[CD] Chen, C.-Y. and Duursma, I. "Geometric Reed-Solomon codes of length 64 and 65 over F8," *IEEE Trans. on Inform. Theory* **49** (2003), 1351-1353.

[CL] Chen, J.-P. and Lu, C.-C. "A serial-in-serial-out hardware architecture for systematic encoding of Hermitian codes via Groebner bases," *IEEE Trans. on Communications*, **52**, no. 8 (2004), 1322–1332.

[CLO] Cox, D., Little, J., and O'Shea, D. *Using Algebraic Geometry, 2nd ed.*, New York: Springer Verlag, 2005.

[GP] Geil, O. and Pellikaan, R. "On the Structure of Order Domains," *Finite Fields Appl.* **8** (2002), 369-396.

[HS] Hansen, J. and Stichtenoth, H. "Group Codes on Certain Algebraic Curves with Many Rational Points," *Applicable Algebra in Eng. Comm. Comp.* **1** (1990), 67-77.

[HLS] Heegard, C., Little, J., and Saints, K. "Systematic encoding via Gröbner bases for a class of algebraic-geometric Goppa codes," *IEEE Trans. Inform. Theory* **41** (1995), 1752-1761.

[HLP] Høholdt, T., van Lint, J., and Pellikaan, R. "Algebraic Geometry Codes," in *Handbook of Coding Theory* (Huffman, W. and Pless, V. eds.), Amsterdam: Elsevier, 1998, 871-962.

[JK] Joyner, D. and Ksir, A. "Automorphism groups of some AG codes." *IEEE Trans. Inform. Theory* **52** (2006), 3325–3329.

[LF] Lally, K. and Fitzpatrick, P. "Algebraic structure of quasicyclic codes," *Discrete Appl. Math.* **111** (2001), 157–175.

[L1] Little, J. "The Algebraic Structure of Some AG Goppa Codes," Proceedings of 33rd Annual Allerton Conference on Communication, Control, and Computing (1995), University of Illinois, 492-500.

[L2] Little, J. "The Ubiquity of Order Domains for the Construction of Error Control Codes," *Advances in Mathematics of Communications* **1** (2007), 151-171.

[LSH] Little, J., Saints, K., and Heegard, C. "On the structure of Hermitian codes," *J. Pure Appl. Algebra* **121** (1997), 293–314.

[MM] Matsui, H. and Mita, S. "Efficient encoding via Gröbner bases and discrete Fourier transforms for several kinds of algebraic codes," accepted for proceedings of ISIT 2007, *preprint:* ArXiv:cs.IT/0703104.

[MOS] Matsumoto, R., Oishi, M., Sakaniwa, K. "Fast Encoding of Algebraic Geometry Codes," *IEICE Trans. Fundamentals*, **E84-A** (2001), 2514–2517.

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

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