ELSEVIER

Journal of Pure and Applied Algebra 121 (1997) 293–314

JOURNAL OF PURE AND APPLIED ALGEBRA

On the structure of Hermitian codes[1]

John Little[a,*], Keith Saints[b], Chris Heegard[c]

[a]*Department of Mathematics, College of the Holy Cross, Worcester, MA 01610, USA*
[b]*Center for Applied Mathematics, Cornell University, Ithaca, NY 14853, USA*
[c]*School of Electrical Engineering, Cornell University, Ithaca, NY 14853, USA*

Communicated by M.-F. Roy; received 14 June 1995; revised 7 September 1995

Abstract

Let X_m denote the Hermitian curve $x^{m+1} = y^m + y$ over the field $\mathbf{F}_{m^2}$. Let Q be the single point at infinity, and let D be the sum of the other m^3 points of X_m rational over $\mathbf{F}_{m^2}$, each with multiplicity 1. X_m has a cyclic group of automorphisms of order $m^2 - 1$, which induces automorphisms of each of the the one-point algebraic geometric Goppa codes $C_L(D, aQ)$ and their duals. As a result, these codes have the structure of modules over the ring $\mathbf{F}_q[t]$, and this structure can be used to good effect in both encoding and decoding. In this paper we examine the algebraic structure of these modules by means of the theory of Groebner bases. We introduce a *root diagram* for each of these codes (analogous to the set of roots for a cyclic code of length $q - 1$ over $\mathbf{F}_q$), and show how the root diagram may be determined combinatorially from a. We also give a specialized algorithm for computing Groebner bases, adapted to these particular modules. This algorithm has a much lower complexity than general Groebner basis algorithms, and has been successfully implemented in the Maple computer algebra system. This permits the computation of Groebner bases and the construction of compact systematic encoders for some quite large codes (e.g. codes such as $C_L(D, 4010Q)$ on the curve X_{16}, with parameters $n = 4096$, $k = 3891$). © 1997 Elsevier Science B.V.

1991 Math. Subj. Class.: 94B27, 13P99

1. Introduction

Let X_m denote the Hermitian curve $x^{m+1} = y^m + y$ over the field $\mathbf{F}_{m^2}$. The projective closure of X_m is a smooth curve of degree $m + 1$, hence of genus $g = m(m - 1)/2$

* Corresponding author. E-mail: jlittle@hcacad.holycross.edu.

[1] 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. Contract DAAL03-92-G-0126, and in part by NSF grant NCR-9207331.

PII S0022-4049(96)00067-9

in $\mathbf{P}^2$. X_m is special in many ways. For each $x \in \mathbf{F}_{m^2}$, there are m distinct solutions $y \in \mathbf{F}_{m^2}$ of the equation $y^m + y = x^{m+1}$. Together with the single point at infinity, this gives $m^3 + 1$ points of X_m rational over the field $\mathbf{F}_{m^2}$. By the Weil bound (see, e.g. [4, 8])

$$|X(\mathbf{F}_q)| \leq 1 + q + 2g\sqrt{q}$$

(valid for any curve defined over $\mathbf{F}_q$) we see that X_m has the maximum possible number of points rational over $\mathbf{F}_{m^2}$ for a curve of genus $g = m(m-1)/2$. Furthermore, X_m has a very large group of automorphisms. Indeed, by [6],

$$|\mathrm{Aut}(X_m)| = m^3(m^3 + 1)(m^2 - 1).$$

For us, a key role will be played by the cyclic subgroup of $\mathrm{Aut}(X_m)$ generated by

$$\sigma : \begin{cases} x \mapsto \alpha x \\ y \mapsto \alpha^{m+1} y \end{cases}$$

It is easy to see that σ fixes the point Q at infinity and permutes the other m^3 rational points of X_m in $m + 2$ orbits (see Lemma 3.1 below).

The simple form of X_m, the large number of $\mathbf{F}_{m^2}$-rational points, and the large automorphism group of X_m are all advantageous when we apply the general construction of Goppa to produce codes starting from X_m. Recall that if X is a smooth curve defined over the finite field $\mathbf{F}_q$, and $D = \sum_{i=1}^{n} P_i$ and G are $\mathbf{F}_q$-rational effective divisors on X with disjoint supports, then the Goppa code $C_L(D, G)$ is defined to be

$$C_L(D, G) = \{(f(P_1), \ldots, f(P_n)) \in \mathbf{F}_q^n \mid f \in L(G)\}.$$

(As usual we write $L(G)$ for the vector space of rational functions on X defined over $\mathbf{F}_q$, whose divisor of poles is bounded by G.)

To obtain long codes from the Hermitian curve X_m, we will always take D to be the sum of the m^3 affine $\mathbf{F}_{m^2}$-rational points of X_m, and $G = aQ$, for some $a \geq 1$. The resulting one-point Hermitian codes have been studied extensively, for example in [9, 7, 5]. The parameters of the code $C_L(D, aQ)$ are $n = m^3$, $k = \dim L(aQ) - \dim L(aQ - D)$ (for $a < m^3$, the second term here is zero), and the exact minimum distance d has been determined in all cases (see [8, 12]).

Encoding and decoding algorithms for Hermitian codes have been considered in [5]. For instance, for encoding, it is easy in principle to construct generator matrices for the codes $C_L(D, aQ)$, because the vector space $L(aQ)$ is spanned by the collection of monomial functions

$$\{x^r y^s \mid rm + s(m+1) \leq a\}.$$

If systematic encoders are desired for long Hermitian codes, however, this approach leads to some impractically large matrix computations. In [3], we showed that the extra symmetries of the Hermitian codes induced by the automorphism σ above can be used to reduce the amount of information needed to specify the code and to describe a

systematic encoder. Namely, each code $C_L(D, aQ)$ has the structure of a module over the ring $\mathbf{F}_q[t]$ (in which multiplication by t is the same as applying the automorphism of the code induced by σ). As a result, the theory of Groebner bases for modules (see, e.g. [1], or Section 2 of [3] and Section 2 of the present paper for the portions of that theory that we will need) can be applied. For Hermitian codes, the results of [3] imply that any code $C_L(D, aQ)$ can be completely specified by giving a Groebner basis whose elements are in 1-1 correspondence with the *orbits* of the points of D under the action of the group of automorphisms generated by σ. This means a collection of $m+2$ module elements, each of which is an $(m+2)$-tuple of polynomials of degree no more than $m^2 - 1$. If we use the unique reduced Groebner basis for the module (relative to a fixed term ordering), then each of these module elements contains at most $n - k + 1$ non-zero terms.

A general algorithm, originally due to Buchberger, is known for computing Groebner bases (see, e.g. [2] for the case of ideals, [1] for the case of modules). Moreover, this algorithm can be simplified considerably for the case of modules over the polynomial ring in one variable. However, even the simplified algorithm is still impractical on modules such as the code $C_L(D, 4010Q)$ on the curve X_{16}, with parameters $n = 4096$, $k = 3891$; the size of the input and the amount of calculation needed to compute several thousand GCDs of polynomials of degree $m^2 - 1 = 255$ with coefficients in $\mathbf{F}_{256}$ is prohibitive. Hence we are led to ask whether the special structure of Hermitian codes can be exploited to yield alternative methods adapted to this situation.

The main theme of the present paper is that the symmetries of the Hermitian curves can be harnessed to do precisely this as well. In Section 2, we will show that to any code over $\mathbf{F}_q$ with an automorphism of order $q - 1$, we can associate a *root diagram* describing the shape of the Groebner basis for the *POT* term order (see [3, Eq. (2.2.1)]). In a sense, this root diagram is a direct generalization of the set of roots of the generator of a *cyclic code* of blocklength $q - 1$ over $\mathbf{F}_q$ (see, for example, [10, Chapter 6]). Since our construction applies to any code with such an automorphism, we believe that the developments here may be valuable in studying other codes as well.

In Section 3 we specialize to the case of Hermitian curves and show how the structure of the rational points on X_m allows one to determine this root diagram for the code $C_L(D, aQ)$ in a direct, *purely combinatorial* fashion, given the integer a. In particular, the actual Groebner basis for the code need not be computed to determine the root diagram.

In Section 4 we show how, given the root diagram for a Hermitian code $C_L(D, aQ)$, the *POT* Groebner basis may be determined without applying the general Buchberger algorithm. The idea is that the elements of $L(aQ)$ which evaluate to give the coefficients of the Groebner basis elements may be determined as the solution of a sequence of *interpolation problems* on the $\langle\sigma\rangle$-orbits in the support of D. Using a simple variant of Lagrange Interpolation, we can produce the Groebner basis elements in a very direct way by evaluating suitably constructed elements of $L(aQ)$. Our algorithms have been successfully implemented in the Maple computer algebra system. With them, it is possible, for example, to construct compact systematic encoders for some very large codes.

The following Section 5 is devoted to a study of the relationship between the root diagram of a $C_L(D, aQ)$ code and that of its dual. Once again we obtain a nice generalization of known facts for cyclic codes of length $q-1$.

The final section Section 6 is devoted to a detailed analysis of the code $C_L(D, 19Q)$ from the Hermitian curve over $\mathbf{F}_9$, an example which illustrates all of the results from the previous sections. The reader may wish to refer to this section as the general results are introduced.

After this article was completed, we learned of [11] which treats the Hermitian codes we study from a somewhat different point of view (without using Groebner bases), but which derives a similar sort of algebraic structure for these codes.

2. Preliminaries

Let $C \subseteq \mathbf{F}_q^n$ be a linear code over $\mathbf{F}_q$ which has a non-trivial automorphism σ of order $q-1$. The cyclic codes of block length $q-1$ are perhaps the most familiar examples of this type. Many interesting algebraic geometric Goppa codes, including the one point Hermitian codes $C_L(D, aQ)$ and their dual codes $C_\Omega(D, aQ)$, also have such automorphisms.

2.1. Example. Let X_m be the Hermitian curve over $\mathbf{F}_{m^2}$, defined by the equation

$$x^{m+1} = y^m + y.$$

Let Q be the single point at infinity of this curve, and let D be the sum of the other m^3 $\mathbf{F}_{m^2}$-rational points, each with coefficient 1. Writing α for a generator of $\mathbf{F}_{m^2}^*$, as in [3], we will consider the automorphism

$$\sigma : \begin{cases} x \mapsto \alpha x \\ y \mapsto \alpha^{m+1} y \end{cases} \tag{1}$$

of X_m. Note that σ has order m^2-1. Since σ fixes the divisors D and $G = aQ$, σ induces an automorphism of each of the codes $C_L(D, aQ)$ constructed from X_m.

It is easy to see that if C is a code as above, then the dual code $C^\perp$ also has an automorphism induced by σ.

As is well-known (see, for instance, [10, Chapter 6]), a cyclic code of block length $q-1$ can be viewed as an ideal I in the ring

$$R = \mathbf{F}_q[t]/\langle t^{q-1} - 1 \rangle.$$

(R may be thought of as the group ring of the cyclic group generated by σ.) Moreover the ideal I is principal, generated by a divisor $g(t)$ of the polynomial $t^{q-1}-1$. Hence we may associate to the cyclic code the set of roots of the generator polynomial, a subset of $\mathbf{F}_q^*$. In this section we will introduce a *root diagram* for any linear code with an automorphism of order $q-1$ which will play a similar role.

In general, e.g. if the block length is greater than $q-1$, the entries of the codewords of one of our codes C will be cyclically permuted in several blocks by σ. We will use the following algebraic structure possessed by the codes C (and $C^{\perp}$). Decompose the entries of words (or equivalently, the standard basis vectors $\mathbf{v}_i$ in $\mathbf{F}_q^n$) into disjoint $\langle\sigma\rangle$-orbits

$$O_1 \cup \cdots \cup O_r.$$

Picking any one element $\mathbf{v}_{i,0}$ from each orbit as representative, we may relabel the basis vectors in the following way

$$\mathbf{v}_{i,j} = \sigma^j(\mathbf{v}_{i,0}),$$

and relabel the entries of each word correspondingly. If $c \in C$, we will write $c_{i,j} =$ coefficient of $\mathbf{v}_{i,j}$ in c.

Using this we may write the codewords as r-tuples of polynomials $(h_1(t), \ldots, h_r(t))$, where

$$h_i(t) = \sum_{j=0}^{|O_i|-1} c_{i,j} t^j.$$

We have thus represented our codes as vector subspaces of

$$\bigoplus_{i=1}^{r} \mathbf{F}_q[t]/\langle t^{|O_i|} - 1\rangle$$

As in [3, Proposition (2.1.4)], because C and $C^{\perp}$ are closed under the action of σ, the collections of r-tuples of polynomials are closed under multiplication by t. In other words, this construction gives C and $C^{\perp}$ the structure of *modules* over the ring $\mathbf{F}_q[t]$. (Since $\sigma^{q-1} = 1$, C may also be viewed as a module over the finite-dimensional ring R.) Furthermore, we have an obvious surjection

$$\mathbf{F}_q[t]^r \xrightarrow{\pi} \bigoplus_{i=1}^{r} \mathbf{F}_q[t]/\langle t^{|O_i|} - 1\rangle,$$

so to each code C as above, we can associate the corresponding submodule $\overline{C} = \pi^{-1}(C)$ of the free module $\mathbf{F}_q[t]^r$.

We will use the *POT monomial ordering* in $\mathbf{F}_q[t]^r$ with the standard basis vectors $\mathbf{e}_i$ ordered:

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

That is,

$$t^u \mathbf{e}_i >_{POT} t^v \mathbf{e}_j$$

if $i < j$, or if $i = j$ and $u > v$. There is a unique reduced Groebner basis $\mathscr{G}$ for the module $\overline{C}$ with respect to this ordering. By the properties of the *POT* ordering (see

e.g. [3, Eq. (2.2.4)]), $\mathscr{G} = \{g^{(1)}, \ldots, g^{(r)}\}$ will have the form

$$\begin{aligned} g^{(1)} &= (g_1^{(1)}, g_2^{(1)}, \ldots, g_r^{(1)}), \\ g^{(2)} &= (0, g_2^{(2)}, \ldots, g_r^{(2)}), \\ &\vdots \\ g^{(r)} &= (0, 0, \ldots, 0, g_r^{(r)}), \end{aligned} \tag{2}$$

Most important for us will be the *diagonal components* $g_i^{(i)}(t)$, $i = 1, \ldots, r$. These polynomials have the following properties.

2.2. Proposition. *For each i, let d_i be the degree of the diagonal component $g_i^{(i)}(t)$. Then the equation $g_i^{(i)}(t) = 0$ has d_i distinct roots in $\mathbf{F}_q^*$.*

Proof. This follows since for each i, $q_i = (t^{|O_i|} - 1)\mathbf{e}_i$ is an element of the module $\overline{C}$. Moreover $|O_i|$ is a factor of $q - 1$. On division by $\mathscr{G}$, q_i must reduce to zero. Hence, we have

$$g_i^{(i)}(t) \mid t^{|O_i|} - 1 \mid t^{q-1} - 1.$$

Hence, $g_i^{(i)}(t)$ has distinct roots in $\mathbf{F}_q^*$. □

The collections of roots of the $g_i^{(i)}(t)$, $i = 1, \ldots, r$, may be conveniently represented by a *root diagram*, in which each row corresponds to one element of the Groebner basis (hence to one of the orbits), the boxes on the ith row correspond to the roots of $t^{|O_i|} - 1 = 0$, and we mark the roots of $g_i^{(i)}(t) = 0$ on the ith row with an X. For an example, we refer the reader to (10) in Section 6 of this paper where the root diagram for the code $C_L(D, 19Q)$ from the Hermitian curve over $\mathbf{F}_9$ is examined in detail. We conclude this section with the following important observation.

2.3. Proposition. *The dimension of the code C is equal to the number of empty boxes in the POT root diagram.*

Proof. By a general property of Groebner bases, (see [3, Eq. (2.3.1)]) there is an $\mathbf{F}_q$-basis for C in one-to-one correspondence with the *non-standard* monomials in the module $\overline{C}$, that is, terms $t^e\mathbf{e}_i$ appearing as leading terms of some element of the module, whose exponents satisfy $e \leq |O_i| - 1$. If there are n_i empty boxes on row i of the root diagram, then there are $|O_i| - n_i$ roots, and the leading term of the Groebner basis element g_i is $t^{|O_i|-n_i}\mathbf{e}_i$. We obtain n_i non-standard monomials containing $\mathbf{e}_i$. The result follows by summing over i. □

3. Determining the root diagram for a Hermitian code

In this section, we will show that the root diagram for a Hermitian code can be determined in a direct, combinatorial fashion, *without first computing the POT Groebner basis* for the module $\overline{C}$. Indeed, as we will see later, this fact can be exploited to give a very direct specialized algorithm for calculating the Groebner basis of one of these modules, which has a much lower complexity than the general Buchberger algorithm. The basis for our method is the following collection of facts about the $\langle\sigma\rangle$-orbits in the affine $\mathbf{F}_q$ rational points of X_m, and about rational functions on X_m. We begin with a general statement about the orbits.

3.1. Lemma. *Under the action of the σ in* (1), *the m^3 points of X_m rational over $\mathbf{F}_q$ decompose into $m+2$ orbits, m of length m^2-1, one of length $m-1$, and one of length* 1. (*We will fix notation for the orbits in the following way. The orbits of length m^2-1, in any convenient order, will be denoted by $O_1,\ldots,O_m$, the orbit of length $m-1$ will be O_{m+1}, and the singleton will be O_{m+2}.*) *Each of the orbits of length m^2-1 is the complete intersection of X_m with a reducible algebraic curve of degree $m-1$, defined by an equation of the form*

$$M_i(y) = \prod_{j=0}^{m-2} (y - \alpha^{\ell_i + j(m+1)}) = y^{m-1} - \alpha^{\ell_i(m-1)} = 0 \tag{3}$$

(*a union of "horizontal lines"*). *The same is true for the orbit O_{m+1} of length $m-1$ if we assign a multiplicity of $m+1$ to each point. The singleton orbit O_{m+2} (with assigned multiplicity m^2-1 is the complete intersection of X_m with the zero set of $M_{m+2} = y^{m-1}$ (a non-reduced curve). Moreover, each $M_i(y)$, $i = 1,\ldots,m+2$, is a non-zero constant when restricted to each of the orbits O_k, $k \neq i$.*

Proof. First consider the orbits of the m points on the line $x = 1$. Say $P_{i,0} = (1, \alpha^{\ell_i})$. Then $\sigma^j(P_{i,0}) = (\alpha^j, \alpha^{\ell_i + j(m+1)})$. From the first components, we see that these points are distinct and that there are precisely m^2-1 of them. From the second components, since $(\alpha^{m+1})^{m-1} = 1$, they are distributed evenly over the $m-1$ horizontal lines $y = \alpha^{\ell_i + j(m+1)}$, $j = 0,\ldots,m-2$. Each of those lines meets X_m in precisely $m+1$ points, so the claim follows. The orbit of length $m-1$ consists of the the $m-1$ affine points other than $(0,0)$ on the line $x = 0$. The horizontal line passing through each of those points is the tangent line to the curve there, which intersects X_m only at that point, and with multiplicity $m+1$.

The fact that $M_i(y)$ is constant on the other orbits is clear from the simplified form on the second line of (3). □

We will call $M_i(y)$ in (3) the *orbit masking function* for orbit i, since it vanishes identically at the points of that orbit. A somewhat curious property of these functions

is that the value of M_i on orbit O_j is equal to the negative of the value of M_j on orbit O_i. In other words, the matrix of orbit masking function values is *skew-symmetric* (or symmetric in characteristic 2). This can be seen easily from the simplified form in the second line of (3).

Next, for future reference, we will construct a function which is zero at all but one point of O_i. As we will see later, the function $B_{i,j}(x, y)$ is essentially one of the basis polynomials for Lagrange interpolation on O_i.

3.2. Lemma. *Let $i \leq m$, and let $P_{i,j} = \sigma^j(P_{i,0})$ be the jth point of O_i. If $i \leq j$, the function*

$$B_{i,j}(x, y) = \prod_{k=1}^{m-2} (y - \alpha^{\ell_i + (j+k)(m+1)}) \cdot \prod_{k=1}^{m} (x - \alpha^{j+k(m-1)})$$

vanishes at each point of O_i except $P_{i,j}$. Similarly, $\prod_{k=1}^{m-2} (y - \alpha^{\ell_{m+1} + (k+j)(m+1)})$ vanishes at each point of O_{m+1} except $P_{m+1,j}$.

Proof. Since $B_{i,j}$ contains all of the factors from $M_i(y)$ except $y - \alpha^{\ell_i + j(m+1)}$, $B_{i,j}$ vanishes at all points of O_i, except those on the horizontal line through $P_{i,j}$. At each of those points except $P_{i,j}$, one of the remaining factors vanishes. The idea for the orbit O_{m+1} is the same. □

Since x has pole order m at Q and y has pole order $m+1$ at Q, we see immediately that for $i \leq m$,

$$M_i \in L((m^2 - 1)Q) \quad \text{and} \quad B_{i,j} \in L(((m-2)(m+1) + m^2)Q). \tag{4}$$

The pole order of $B_{m+1,j}$ at Q is $(m-2)(m+1)$.

As a first consequence of these observations, we have the following information about the rows of the root diagram for $C_L(D, aQ)$.

3.3. Theorem. *Consider the root diagram for the Hermitian code $C_L(D, aQ)$.*

(1) *Let $i \leq m$. If $a \geq (i-1)(m^2-1)$, then the ith row of the root diagram for the code is not full, or in other words, there is some $\beta \in \mathbf{F}_q^*$ which is not a root of the ith diagonal component $g_i^{(i)}(t)$ of the reduced POT Groebner basis for $\overline{C}$.*

(2) *Let $i \leq m$ again. If $a \geq (i-1)(m^2-1) + m^2 + (m-2)(m+1)$, then the ith row of the root diagram is empty, or in other words, the ith diagonal component $g_i^{(i)}(t)$ of the reduced POT Groebner basis is* 1.

(3) *Finally, consider the case $i = m+1$. The $(m+1)$st row of the root diagram is not full if $a \geq m(m^2-1)$. It is empty if $a \geq m(m^2-1) + (m-2)(m+1)$.*

Proof. Recall that we have represented the elements of $C_L(D, aQ)$ as $(m+2)$-tuples of polynomials

$$(h_1(t), \ldots, h_{m+2}(t))$$

where

$$h_i(t) = \sum_{j=0}^{|O_i|-1} f(P_{i,j})t^j$$

for some $f \in L(aQ)$.

(1) Suppose that $i \leq m$ and $a \geq (i-1)(m^2-1)$. Then by (5), the following product of orbit masking functions is an element of $L(aQ)$:

$$f = M_1(y)M_2(y)\cdot\cdots\cdot M_{i-1}(y) \in L(aQ).$$

Evaluating f to form the coefficients of a module element, we see that $C_L(D, aQ)$ will contain an element of the form

$$(0,\ldots,0,h_i(t),\ldots,h_{m+2}(t))$$

with $i-1$ zero leading components. By the last statement in Lemma 3.1, the ith component $h_i(t)$ has the form

$$h_i(t) = c(1+t+t^2+\cdots+t^{m^2-2})$$

for some $c \in \mathbf{F}_q^*$. The roots of $h_i(t)$ are all $t \neq 1$ in $\mathbf{F}_q^*$. The ith diagonal component from the *POT* Groebner basis for the module must divide this $h_i(t)$, so we see that in row i of the root diagram at least one root ($t = 1$) has been omitted.

(2) Similarly, by (4), if $i \leq m$ and $a \geq (i-1)(m^2-1)+m^2+(m-2)(m+1)$, then we have that $f = (\prod_{k=1}^{i-1} M_k(y))B_{i,0}(x,y) \in L(aQ)$. f is zero on orbits $1,\ldots,i-1$, and also at every point of O_i except $P_{i,0}$. After multiplying by a suitable non-zero constant, we obtain a module element of the form

$$(0,\ldots,0,1,h_{i+1}(t),\ldots,h_{m+2}(t)).$$

In this case *every* polynomial of degree m^2-2 or less appears as the ith component of some element of the module, and there are *no* common roots.

(3) This follows in the same way. Row $m+1$ of the root diagram is non-full for any $a \geq m(m^2-1)$, since $L(aQ)$ will contain the product of the orbit masking functions for $O_1,\ldots,O_m$. Similarly, if $a \geq m(m^2-1)+(m-2)(m+1)$, then $L(aQ)$ contains the product $M_1(y)\cdot\cdots\cdot M_m(y)B_{m+1,0}$. □

The actual roots present on each row of the *POT* root diagram may also be determined in terms of a in a simple fashion. To understand the pattern, consider the *filtration* (increasing chain of vector subspaces)

$$L(Q) \subseteq L(2Q) \subseteq \cdots \subset L((a-1)Q) \subset L(aQ)$$

for $L(aQ)$. By the Riemann–Roch Theorem, for any $b \geq 2g-1$, we will have strict inclusion $L((b-1)Q) \subset L(bQ)$, and in fact $\dim L(bQ) = \dim L((b-1)Q)+1$. Provided that $a < m^3$, no element of $L(aQ)$ vanishes at every point of D, and the dimension of the code $C_L(D, aQ)$ is just the dimension of $L(aQ)$. By Proposition 2.3, the number

of empty boxes in the root diagram is equal to this dimension. If $a < a'$, then since $L(aQ) \subseteq L(a'Q)$, the boxes marked in the root diagram for $L(a'Q)$ form a subset of the boxes marked in the diagram for $L(aQ)$.

For simplicity, we give the statement for the orbits of length $m^2 - 1$. There is a corresponding statement for the remaining two orbits as well, which we leave to the reader as an exercise. Also see Section 6 for an example.

3.4. Theorem. *Let $1 \leq i \leq m$ and let a be in the range*

$$(i-1)(m^2-1) \leq a < (i-1)(m^2-1) + m^2 + (m-2)(m+1),$$

so that row i of the POT root diagram is neither full, nor empty. The complement of the set of roots marked on row i of the diagram is the set of elements $\alpha^{-k} \in \mathbf{F}_q^*$ such that $k = r + s(m+1)$, where $0 \leq r \leq m$, $0 \leq s \leq m-2$, and $rm + s(m+1) + (i-1)(m^2-1) \leq a$. As a result, for any given a, there are at most two rows of the root diagram which are neither full nor empty.

Proof. By considering pole orders at Q, we see that each of the functions $(\prod_{k=1}^{i-1} M_k(y))$ $x^r y^s$ with $rm + s(m+1) + (i-1)(m^2-1) \leq a$ is an element of $L(aQ)$. We may exclude powers of x greater than m because they may be reduced using the equation of X_m. Furthermore, we will exclude powers of y greater than $m-2$, since

$$y^{m-1} = M_i(y) + \text{ lower degree terms in } y.$$

As a result, any $(\prod_{k=1}^{i-1} M_k(y))x^r y^s$ with $s \geq m-2$ will influence the roots of row $i+1$ rather than those of row i.

Corresponding to each such product $(\prod_{k=1}^{i-1} M_k(y))x^r y^s$ in $L(aQ)$, we have a module element whose first $i-1$ components are zero, and whose ith component is found by evaluating the product at the points of orbit i. By the last statement in Lemma 3.1, the product of the orbit masking functions is a non-zero constant on orbit i, so we may ignore that factor. Since the points of orbit i satisfy an equation of the form $y = \alpha^{\ell_i} x^{m+1}$ for some ℓ_i, the monomial $x^r y^s$ evaluates to $\alpha^{rj+s\ell_i+sj(m+1)}$ at $P_{i,j} = (\alpha^j, \alpha^{\ell_i+j(m+1)})$. Removing common factors in the coefficients, we have zeroes in entries $1, \ldots i-1$, and an ith entry of the form

$$h_i(t) = \sum_{j=0}^{m^2-2} (\alpha^{r+s(m+1)} t)^j.$$

The roots of this polynomial are all $t \neq \alpha^{-(r+s(m+1))} \in \mathbf{F}_q^*$. Since $C_L(D, aQ)$ is a $\mathbf{F}_q[t]$-module, it will contain an element whose first $i-1$ entries are 0, and whose ith entry is the greatest common divisor of the polynomials $\sum_{j=0}^{m^2-2} (\alpha^{r+s(m+1)} t)^j$ where r, s satisfy $0 \leq r \leq m$, $0 \leq s \leq m-2$, and $rm + s(m+1) + (i-1)(m^2-1) \leq a$. The diagonal component $g_i^{(i)}(t)$ of the *POT* Groebner basis element must divide this GCD. This argument shows that the subset of $\mathbf{F}_q^*$ given by the ith row of the root diagram is contained in the set described in the statement of the theorem.

The opposite inclusion follows essentially by counting dimensions. In order to provide a simple proof, we will postpone giving the argument until Section 4, where some additional structure of the collection of polynomial functions on each of the orbits will be introduced. □

4. Determining the Groebner basis by interpolation on the orbits

Our main result in this section will be a specialized algorithm for constructing the full *POT* Groebner basis of a Hermitian $C_L(D, aQ)$ code. The key idea is that once we have the root diagram, the construction of the Groebner basis simply amounts to a sequence of *interpolation problems*: For each i, $i = 1, \ldots, m+2$, we need to find the $f_i(x, y) \in L(aQ)$ that evaluates at the points of D to give the coefficients of the module element g_i in the Groebner basis.

To prepare for this, we will begin by reconsidering the techniques used in the first part of the proof of Theorem 3.4. In particular recall that a key role there was played by the functions of the form $\prod_{k=1}^{i-1} M_k(y) x^r y^s$. Note that there are exactly $m^2 - 1$ of these products with $0 \leq r \leq m$, $0 \leq s \leq m-2$. Moreover, their pole orders at Q are distinct, so they are linearly independent as rational functions on X_m, or on the plane. Let us consider what happens when we restrict to the points of orbit O_i. Here and in the following discussion, $I(O_i)$ denotes the ideal in $\mathbf{F}_q[x, y]$ consisting of polynomials vanishing at each point of the set O_i. The quotient ring $\mathbf{F}_q[x, y]/I(O_i)$ is the ring of polynomial functions on O_i.

4.1. Lemma. *Let $i \leq m$, and let V_i be the linear span of the*

$$\left(\prod_{k=1}^{i-1} M_k(y)\right) x^r y^s$$

for $0 \leq r \leq m$, $0 \leq s \leq m-2$. The restriction mapping from V_i to the ring of polynomial functions on O_i is an isomorphism of $\mathbf{F}_q$ vector spaces.

Proof. Since $i \leq m$, O_i consists of $m^2 - 1$ points with distinct x coordinates and we have the relation $y = \alpha^{\ell_i} x^{m+1}$ on O_i, the ring of polynomial functions $\mathbf{F}_q[x, y]/I(O_i)$ is isomorphic to $\mathbf{F}_q[x]/\langle x^{m^2-1} - 1 \rangle$. The restriction mapping

$$\Phi_i : V_i \to \mathbf{F}_q[x, y]/I(O_i)$$

is clearly linear, and can be given in concrete terms as follows. For each $f(x, y) \in V_i$, $\Phi_i(f(x, y)) = f(x, \alpha^{\ell_i} x^{m+1})$. By Lemma 3.1, each of the orbit masking functions $M_k(y)$ is a non-zero constant on O_i, and those factors may be ignored. In particular we see that

$$\Phi_i\left(\prod_{k=1}^{i-1} M_k(y) x^r y^s\right) = c x^{r+s(m+1)}$$

for some $c \in \mathbf{F}_q^*$. As r, s range over the set of pairs with $0 \le r \le m$, $0 \le s \le m-2$, we obtain non-zero multiples of each of the powers x^u, $u = 0, \ldots, m^2 - 2$. Hence Φ_i is surjective. Since V_i and $\mathbf{F}_q[x,y]/I(O_i)$ have the same dimension over $\mathbf{F}_q$, Φ_i is a vector space isomorphism. □

As an immediate result, we see that any interpolation problem on O_i, including the side condition that the interpolating function vanishes on $O_1, \ldots, O_{i-1}$, has a unique solution in V_i.

4.2. Corollary. *For any collection of values c_j, $j = 0, \ldots, m^2 - 2$, there is a unique function $f(x,y) \in V_i$, which satisfies $f(P_{i,j}) = c_j$ for all j and which vanishes identically on $O_1, \ldots, O_{i-1}$.*

Proof. By standard techniques, e.g. the Lagrange interpolation formula, there is a unique polynomial function $F(x) \in \mathbf{F}_q[x]/\langle x^{m^2-1} - 1\rangle \cong \mathbf{F}_q[x,y]/I(O_i)$ (of degree at most $m^2 - 2$) solving the given interpolation problem on O_i. The function $f(x,y) = \Phi_i^{-1}(F(x)) \in V_i$ also vanishes on orbits $1, \ldots, i-1$. □

Indeed, the functions $B_{i,j}(x,y)$ introduced in Lemma 3.2, multiplied by the product of the orbit masking functions $M_1(y), \ldots, M_{i-1}(y)$, give elements of V_i mapping to constant multiples of the usual Lagrange interpolation basis functions under Φ_i. For example,

$$\begin{aligned}
\Phi_i\left(\prod_{k=1}^{i-1} M_k(y) B_{i,0}(x,y)\right) &= c \cdot B_{i,0}(x, \alpha^{\ell_i} x^{m+1}) \\
&= c \cdot \prod_{k=1}^{m-2} (\alpha^{\ell_i} x^{m+1} - \alpha^{\ell_i + k(m+1)}) \cdot \prod_{k=1}^{m} (x - \alpha^{k(m-1)}) \\
&= c \cdot \alpha^{(m-2)\ell_i} \prod_{k=1}^{m-2} (x^{m+1} - \alpha^{k(m+1)}) \cdot \prod_{k=1}^{m} (x - \alpha^{k(m-1)}) \\
&= c' \cdot \prod_{j=1}^{m^2-2} (x - \alpha^j).
\end{aligned}$$

Dividing by the value at $P_{i,0}$, we would obtain the usual Lagrange interpolation basis function.

At this point we will complete the proof of Theorem 3.4.

Proof of Theorem 3.4 (*Conclusion*). Recall that we have shown that if $i \le m$ and a is in the range $(i-1)(m^2-1) \le a < (i-1)(m^2-1) + m^2 + (m-2)(m+1)$, then $L(aQ)$ contains some $f(x,y)$ which is zero on orbits $1, \ldots, i-1$, and which has as roots the complement of the set of $\alpha^{-k} \in \mathbf{F}_q^*$ such that $k = r + s(m+1)$, where $0 \le r \le m$, $0 \le s \le m-2$, and $rm + s(m+1) + (i-1)(m^2-1) \le a$. It only remains to show that *no smaller set of roots is possible*. Using Corollary 4.2, we can now give a simple proof of this. Suppose that there were some $g(x,y) \in L(aQ)$ that evaluated to give the

coefficients of a module element with zeroes in components $1,\ldots,i-1$, and a smaller set of roots. Finding such a g to produce a set of ℓ roots $\{\alpha^{e_1},\ldots,\alpha^{e_\ell}\}$, for example, amounts to solving an interpolation problem. Let

$$\prod_{k=1}^{\ell}(t-\alpha^{e_k})=\sum_{j=0}^{\ell}c_j t^j \tag{5}$$

be the expansion of the unique monic polynomial with the given roots. We ask for a function whose values on O_i are

$$g(P_{i,j})=\begin{cases}0 & \text{for all } j=\ell+1,\ldots,m^2-2,\\ c_j & \text{from (5) for } j=0,\ldots,\ell.\end{cases}$$

By Corollary 4.2 there is a unique solution for g in V_i. On the other hand, by Theorem 3.4, there exists such a function *for a larger value of* a. Hence, we get a smaller set of roots *only* by going to a code with a larger a. □

4.3. Theorem. *Let* $\{\alpha^{e_1},\ldots,\alpha^{e_\ell}\}$ *be the set of roots appearing on row* i *of the root diagram for a Hermitian code* $C_L(D,aQ)$. *Let*

$$p(t)=\prod_{k=1}^{\ell}(t-\alpha^{e_k})=\sum_{j=0}^{\ell}c_j t^j, \tag{6}$$

be the unique monic polynomial of degree ℓ *with these roots. Then*

$$f(x,y)=\prod_{k=1}^{i-1}M_k(y)\cdot\sum_{j=0}^{|O_i|-1}c_j B_{i,j}(x,y)/B_{i,j}(P_{i,j}) \tag{7}$$

is a function in $L(aQ)$ *which yields a module element* $g^{(i)}$ *with* $i-1$ *leading zero components, and* i*th component equal to* $p(t)$.

Proof. Since $f\in V_i$ is the solution of the interpolation problem on O_i specified by the coefficients of the polynomial $p(t)$ in (6), the only thing we need to prove is that this $f(x,y)$ is in $L(aQ)$ (i.e. that its pole order at Q is actually a or less, and not $(i-1)(m^2-1)+m^2+(m-2)(m+1)$ as one might guess from the formula). But this follows from Theorem 3.4 and Lemma 3.2 as well. By the latter result, the solution of the interpolation problem is unique in V_i. On the other hand by Theorem 3.4, there exists some solution of the interpolation problem in $L(aQ)\cap V_i$. Hence this linear combination of the $(\prod_{k=1}^{i-1}M_k(y))B_{i,j}(x,y)$ must lie in $L(aQ)$. □

In intuitive terms, the coefficients in the linear combination in (7) produce *cancellations* lowering the pole order at Q.

The conclusion of the proof of Theorem 3.4, and the resulting Theorem 4.3 are also the basis for an *algorithm* for producing Groebner bases for the Hermitian codes $C_L(D,aQ)$, which in effect constructs the Groebner basis directly from the root diagram. This algorithm has a much lower complexity than general Groebner basis algorithms

because we are relying so heavily on the particular features of Hermitian codes. We will give a rudimentary version which produces *POT* Groebner bases with the minimal number $m+2$ of elements, but which are *not reduced* (the basis elements may contain terms that can be removed by division with respect to other basis elements). It is easy to see in this situation that the basis has the same triangular form as in (2), and the diagonal components are *the same* as those appearing in the reduced basis.

It is also possible to find solutions of our interpolation problems by solving systems of linear equations for the coefficients in a linear combination of the basis functions $(\prod_{k-1}^{i-1} M_k(y))x^r y^s$. For instance, knowing the degree ℓ of the polynomial in (6), we would need to find the linear combination $f(x,y)$ of the first $m^2-1-\ell$ of the functions

$$\left\{ \left(\prod_{k=1}^{i-1} M_k(y) \right) x^r y^s \mid 0 \le r \le m,\ 0 \le s \le m-2 \right\}$$

(listed in increasing graded lexicographic order), which satisfy

$$f(P_{i,j}) = \begin{cases} 0 & \text{for } j = \ell+1, \ldots, m^2-2, \\ 1 & \text{for } j = \ell. \end{cases}$$

This yields a system of $m^2-1-\ell$ inhomogeneous linear equations for the $m^2-1-\ell$ coefficients, and there is a unique solution. By our previous results, we know that the corresponding module element will have a non-zero ith component of minimal possible degree, so it must have the correct set of roots. Moreover, the two methods are complementary in a sense – the interpolation method is more efficient for rows of the root diagram containing a small number of roots, while solving a system of equations is preferable if the number of roots is large. In our description of the algorithm, for simplicity we will use the interpolation approach exclusively.

In the following, we will denote by *GetRootDiagram* a procedure which given $a \ge 1$, determines the roots of each of the diagonal components of the *POT* Groebner basis elements using Theorems 3.3 and 3.4. We will assume that GetRootDiagram returns a list of $m+2$ lists of roots (corresponding to the marked boxes in the root diagram). We will denote by *GetValueList* a procedure which takes as input a list of elements in $\mathbf{F}_q^*$ and returns the list of coefficients in the unique monic polynomial of minimal degree over $\mathbf{F}_q$ with those roots, as in (5), including zeroes for powers of t higher than the number of roots. Finally, we will by denote by *EvaluateCombination* a function which takes a list of coefficients: values $= \{c_j\}$ as in (7), and evaluates the linear combination of the functions $(\prod_{k=1}^{i-1} M_k(y))B_{i,j}(x,y)$ given in (7), at a point $P = (x,y) \in \mathbf{F}_q^2$.

4.4. Proposition. *The following algorithm correctly computes a (non-reduced) POT Groebner basis for the module* $C_L(D, aQ)$.

Input: a, $\{P_{i,j}\}$ (the m^3 points of X_m rational over $\mathbf{F}_q$)
Output: A non-reduced *POT* Groebner basis $\mathcal{G}$
$= \{g^{(1)}, \ldots, g^{(m+2)}\}$ for $C_L(D, aQ)$ on X_m

Uses: GetRootDiagram, GetValueList, EvaluateCombination

$\mathcal{G} := \{\}$
rootdiagram := GetRootDiagram(a)
for i from 1 to $m+2$ do
  if |rootdiagram[i]| < $|O_i|$ then # the number of roots on row i
    values := GetValueList(rootdiagram[i])
    for k from 1 to $i-1$ do
      $g_k^{(i)} := 0$
    for k from i to $m+2$ do
      $g_k^{(i)} := 0$
      for j from 0 to $|O_i| - 1$ do
        $g_k^{(i)} := g_k^{(i)} + \text{EvaluateCombination}(\text{values}, P_{k,j}))t^j\mathbf{e}_k$
  else
    $g^{(i)} := (t^{|O_i|} - 1)\mathbf{e}_i$
  $\mathcal{G} := \mathcal{G} \cup \{g^{(i)}\}$

Proof. The correctness of the algorithm follows directly from Theorem 4.3. □

Note that if $a \geq (i-1)(m^2-1) + m^2 + (m-2)(m+1)$ for some i, the ith element of $\mathcal{G}$ computed by this algorithm is just the module element formed by evaluating the function $(\prod_{k=1}^{i-1} M_k(y))B_{i,0}(x,y)/B_{i,0}(P_{i,0})$ at all the points of X_m. As a result, it is actually *independent of* a (in this range), and if we wanted Groebner bases for several codes $C_L(D, aQ)$ with a as above, we could "reuse" this element.

If a reduced Groebner basis is required, then two approaches are possible. First, we could simply apply the algorithm of 5.4 to produce a non-reduced basis, and then reduce it. This would mean subtracting suitable multiples of $g^{(i+1)}, \ldots, g^{(m+2)}$ from each $g^{(i)}$, $i = m+1, m, \ldots, 1$ in that order, to eliminate terms behind the leading term. Since that computation itself can be somewhat large for large m, it is also possible to replace the linear combinations of basis functions in (7) by linear combinations of $\prod_{k=1}^{i-1} M_k(y)B_{i,j}(x,y)$ for *more than one* i. The idea is the same as in the proof of Theorem 4.3, so we will not give a full development here.

5. The dual code

In this section, we wish to address the question:

5.1. Question. What is the precise relation between the root diagrams for the Hermitian code $C_L(D, aQ)$ and for the dual code $C_\Omega(D, aQ)$? (By [8, Section VII.4.2], the dual code is equal to $C_L(D, a'Q)$ for an a' determined by a in this case, so our results will also indicate a certain duality between the root diagrams for pairs of $C_L(D, aQ)$ codes.)

As in Section 2, the answer only depends on the existence of an automorphism of order $q-1$. So we will give a general argument that applies to any linear code over $\mathbf{F}_q$ with this extra structure. Of course, a nice answer is well-known in the case of cyclic codes of block length $q-1$. (See the comments after the statement of Theorem 5.2 below.) Our results will show that there is an extension of this to the more general codes under consideration.

We need two additional pieces of terminology. First, we will call the *POT* monomial ordering on $\mathbf{F}_q[t]^r$ based on the *reversed* ordering of the standard basis:

$$\mathbf{e}_r > \mathbf{e}_{r-1} > \cdots > \mathbf{e}_1$$

the *rPOT* ordering. If we list the elements of an *rPOT* Groebner basis with their leading terms in *increasing* order, we will have something of the form:

$$\begin{aligned} h^{(1)} &= (h_1^{(1)}, 0, \ldots, 0), \\ h^{(2)} &= (h_1^{(2)}, h_2^{(2)}, 0, \ldots, 0), \\ &\vdots \\ h^{(r)} &= (h_1^{(r)}, h_2^{(r)}, \ldots, h_r^{(r)}). \end{aligned} \tag{8}$$

(We are assuming here that the module C is finite-dimensional as a vector space over $\mathbf{F}_q$, so that there are Groebner basis elements whose leading terms contain each of the standard basis vectors.) Since we have merely reordered the components of the r-tuples, everything we said before for *POT* Groebner bases carries over *mutatis mutandis* to *rPOT* Groebner bases. In particular, we can also construct a *root diagram* from the *rPOT* diagonal components $h_i^{(i)}$.

Second, given any root diagram, we can construct another similar diagram by, in each row, placing an X in the position corresponding to β^{-1} for each root β in the original diagram. We will call this the *inverted root diagram*. See Section 6 below for an example.

5.2. Theorem. *Let C be a linear code over $\mathbf{F}_q$ with an automorphism of order $q-1$. Then the inverted root diagram for the POT Groebner basis of $\overline{C}$ and the root diagram for the rPOT Groebner basis of $\overline{C^\perp}$ are complements of each other.*

Note that in the case of a cyclic code of blocklength $n = q-1$, Theorem 5.2 reduces to a well-known fact. In the case $r = 1$, the Groebner basis for C will consist of the single generator polynomial $g(t) \mid t^{q-1} - 1$, and the corresponding one-row root diagram just gives the roots of g. Similarly, we get a single generator polynomial $h(t)$ for $C^\perp$, and its set of roots. The *rPOT* and *POT* orderings are the same in the case $r = 1$, so we have the familiar result that the set of roots of $h(t)$ is the complement of the set of inverses of the roots of $g(t)$.

Proof of Theorem 5.2. Our proof will be in several steps, which we break out as separate lemmas. First we give another characterization of the dual code $C^\perp$.

5.3. Definition. Let

$$S = \bigoplus_{i=1}^{r} \mathbf{F}_q[t]/\langle t^{|O_i|} - 1\rangle.$$

Define a mapping $[\,,\,] : S \times S \to \mathbf{F}_q$ as follows. For $g = (g_1, \ldots, g_r)$ and $h = (h_1, \ldots, h_r)$ in S, let

$$[g, h] = \sum_{i=1}^{r} \text{constant term in } g_i(t)h_i(t^{-1})$$

where

$$h_i(t^{-1}) \equiv h_i(t^{|O_i|-1})$$

in $\mathbf{F}_q[t]/\langle t^{|O_i|} - 1\rangle$, the products $g_i(t)h_i(t^{-1})$ are computed in $\mathbf{F}_q[t]/\langle t^{|O_i|} - 1\rangle$, and the "constant terms" refer to the constant terms in the unique standard representatives of the products in $\mathbf{F}_q[t]/\langle t^{|O_i|} - 1\rangle$, obtained by division with respect to $t^{|O_i|} - 1$.

It is clear that $[\,,\,]$ defines a bilinear form on S.

5.4. Lemma. *Let C be a linear code over $\mathbf{F}_q$ with an automorphism of order $q - 1$, and denote also by C the corresponding subspace of S constructed as above. Then under the same construction the dual code $C^{\perp}$ corresponds to*

$$\{h = (h_1(t), \ldots, h_r(t)) \in S : [g, h] = 0 \text{ for all } g \in C\}.$$

Proof. The proof is essentially the same as the proof for the corresponding fact for cyclic codes of blocklength $q - 1$. □

The idea of our proof of Theorem 5.2 is to start from the unique *POT* reduced Groebner basis for $\overline{C}$, and construct a set of elements $\mathscr{H} = \{h^{(1)}, \ldots, h^{(r)}\}$ in $C^{\perp}$, whose *rPOT* root diagram is the complement of the inverted root diagram for the *POT* Groebner basis $\mathscr{G}$ of C. Then we will argue that $\mathscr{H}$ must be an *rPOT* Groebner basis of $\overline{C^{\perp}}$. So assume $\mathscr{G}$ as in (2) above is the reduced *POT* Groebner basis for $\overline{C}$.

We let B_i be the set of elements $\beta \in \mathbf{F}_q^*$ satisfying $\beta^{|O_i|} = 1$, but which are *not* roots of the diagonal component $g_i^{(i)}$. Let

$$h_i(t) = \prod_{\beta \in B_i} (t - \beta^{-1}). \tag{9}$$

(That is, the set of roots of $h_i(t^{-1})$ is the complement of the set of roots of $g_i^{(i)}(t)$ in the set of $\beta \in \mathbf{F}_q^*$ satisfying $\beta^{|O_j|} = 1$).

5.5. Lemma. *There exists a collection* $\mathscr{H}$ *of elements* $h^{(i)} \in \overline{C^{\perp}}$ *of the form:*

$$\begin{aligned} h^{(1)} &= (h_1, 0, \ldots, 0), \\ h^{(2)} &= (h_1^{(2)}, h_2, 0, \ldots, 0), \\ &\vdots \\ h^{(r)} &= (h_1^{(r)}, h_2^{(r)}, \ldots, h_r), \end{aligned}$$

where the h_i *are as in* (9) *above.*

Proof. The proof is by induction on r. For $r = 1$, our assertion follows directly from the usual description of the dual of a cyclic code of length $n = q - 1$. The induction step consists of determining the subdiagonal entries in $h^{(r)}$ to make $[h^{(r)}, h^{(i)}] = 0$ for each $i = 1, \ldots, r-1$. We will leave the details to the reader. □

To complete the proof of Theorem 5.2, we need to show that $\mathscr{H}$ is actually an *rPOT* Groebner basis for the module $\overline{C^{\perp}}$. That $\mathscr{H}$ is an *rPOT* Groebner basis for the submodule of $\mathbf{F}_q[t]^r$ that it generates is actually obvious. (The *rPOT* leading terms are the leading terms in the diagonal components h_i. These involve distinct standard basis vectors, so Buchberger's criterion implies that $\mathscr{H}$ is a Groebner basis.) Hence, we only need show:

5.6. Lemma. $\mathscr{H}$ *generates* $\overline{C^{\perp}}$.

Proof. To show this, it suffices to consider the image of the submodule spanned by $\mathscr{H}$ under the mapping $\pi : \mathbf{F}_q[t]^r \to S$. By the above, $\pi(\langle \mathscr{H} \rangle) \subseteq C^{\perp}$. On the other hand from the form of the leading terms, it is clear that the dimension of $\pi(\langle \mathscr{H} \rangle)$ as $\mathbf{F}_q$ vector space is equal to

$$\dim_{\mathbf{F}_q}(\pi(\langle \mathscr{H} \rangle)) = \sum_{i=1}^{r} (|O_i| - \deg h_i(t)) = \sum_{i=1}^{r} \deg g_i^{(i)}$$

On the other hand, the dimension of $C^{\perp}$ is

$$\begin{aligned} \dim_{\mathbf{F}_q}(C^{\perp}) &= \sum_{i=1}^{r} |O_i| - \dim_{\mathbf{F}_q}(C) \\ &= \sum_{i=1}^{r} |O_i| - \sum_{i=1}^{r} (|O_i| - \deg g_i^{(i)}). \end{aligned}$$

Hence $\dim_{\mathbf{F}_q}(\pi(\langle \mathscr{H} \rangle)) = \dim_{\mathbf{F}_q}(C^{\perp})$ and the proof of Lemma 5.6 and Theorem 5.2 are complete. □

6. An extended example

Because of the combinatorial intricacy of some of the results in the previous sections, we wish to illustrate our conclusions by working out a representative example in full detail.

Consider the code $C = C_L(D, 19Q)$ on the Hermitian curve over $\mathbf{F}_9$ and the automorphism σ of order 8 as in (1). The automorphism σ permutes the 27 affine $\mathbf{F}_9$-rational points in 5 orbits: three of length 8, one of length 2 and one of length 1.

First we determine the *POT* root diagram for this code directly from the Groebner basis. Using the normalization $\mathbf{F}_9 = \mathbf{F}_3[\alpha]/\langle \alpha^2 + \alpha - 1 \rangle$ and choosing as orbit representatives the three affine points with $x = 1$, the point $(0, \alpha^2)$, and $(0,0)$ as in [3, Eq. (3.2)], the *POT* Groebner basis $\mathscr{G}$ has the form:

$$g^{(1)} = (1, \alpha^6, \alpha t^5 + \alpha t^4 + \alpha^6 t^3 + \alpha^2 t^2 + \alpha t + \alpha^2, \alpha^2 t + \alpha, 1),$$
$$g^{(2)} = (0, t + \alpha^5, t^5 + \alpha^5 t^4 + \alpha^7 t^3 + \alpha^7 t + \alpha^7, \alpha^2 t + \alpha^4, 1),$$
$$g^{(3)} = (0, 0, t^6 + \alpha^6 t^5 + \alpha^2 t^4 + \alpha^7 t^3 + \alpha t^2 + \alpha^4 t + \alpha^5, \alpha^3 t + \alpha^3, \alpha^7),$$
$$g^{(4)} = (0, 0, 0, t^2 - 1, 0),$$
$$g^{(5)} = (0, 0, 0, 0, t - 1).$$

The diagonal components are $g_1^{(1)}(t) = 1$, $g_2^{(2)}(t) = t + \alpha^5$,

$$g_3^{(3)}(t) = t^6 + \alpha^6 t^5 + \alpha^2 t^4 + \alpha^7 t^3 + \alpha t^2 + \alpha^4 t + \alpha^5,$$

$g_4^{(4)}(t) = t^2 - 1$, and $g_5^{(5)}(t) = t - 1$. Hence the first row of the root diagram will be empty, the second will contain a single X corresponding to the root of $g_2^{(2)}(t) = t + \alpha^5 = 0$ $(t = \alpha)$, the third row will contain an X for each of the six roots of $g_3^{(3)}(t) = 0$, and so forth.

1	α	α^2	α^3	α^4	α^5	α^6	α^7
	X						
	X	X	X	X	X	X	
X				X			
X							

(10)

Next, we will show that this diagram conforms to the general description given in Theorems 3.3 and 3.4. We have $a = 19 \geq (3-1)(3^2-1) = 16$, so by (1) of the theorem, none of the first 3 rows is *full*. On the other hand, by part (2) of the theorem, $19 \geq (1-1)(3^2-1) + 9 + 4 = 13$, so row 1 is *empty*. (For codes with larger a, we note that row 2 of the root diagram would also be empty for any $a \geq 8 + 13 = 21$, and row 4 would not be full for any $a \geq 24$.)

Consider the second row of the root diagram (10), which contains the single entry $t = \alpha$. The question we will address next is: Why must every module element whose first component is 0 have a second component whose set of roots contains α? (This is a restatement of the fact that the diagonal component $g_2^{(2)}(t)$ in the *POT* Groebner basis is $t - \alpha$.) This may be seen in the following way. Note that since x has pole order 3 at Q and y has pole order 4 at Q, $L(19Q)$ contains the functions:

$$M_1(y), M_1(y)x, M_1(y)y, M_1(y)x^2, M_1(y)xy, M_1(y)x^3, M_1(y)x^2y. \tag{11}$$

(It *also* contains $M_1(y)y^2$, for example. But by part 1) of Theorem 3.3, $M_1(y)M_2(y) \in L(16Q) \subset L(19Q)$ as well. That function is a linear combination of $M_1(y)y^2$, $M_1(y)y$, and $M_1(y)$. Hence, in the filtration of $L(19Q)$, the step from $L(15Q)$ to $L(16Q)$, where $M_1(y)y^2$ is added, is responsible, so to speak, for removing one of the roots on row 3 rather than one on row 2. A similar comment applies to $M_1(y)xy^2 \in L(19Q)\backslash L(18Q)$.)

From suitable constant multiples of the seven functions in (11) we get module elements of the form

$$
\begin{aligned}
&(0,\ 1 + t + t^2 + \cdots + t^7, *, *, *)\\
&(0,\ 1 + \alpha t + \alpha^2 t^2 + \cdots + \alpha^7 t^7, *, *, *)\\
&(0,\ \alpha^5 + \alpha t + \alpha^5 t^2 + \cdots + \alpha t^7, *, *, *)\\
&\quad\vdots\\
&(0,\ \alpha^5 + \alpha^3 t + \alpha t^2 + \cdots + t^7, *, *, *)
\end{aligned}
$$

(where the $*$ components are irrelevant for this discussion). We note that at the points of orbit 2 (orbit representative $(1, \alpha^5)$), we have $y = \alpha^5 x^4$. Hence the module element constructed from $M_1(y)y$ can also be written in the form

$$(0, \alpha^5(1 + \alpha^4 t + (\alpha^4 t)^2 + \cdots + (\alpha^4 t)^7), *, *, *)$$

by factoring. Similarly, we see that all of the module elements above have the form

$$(0, c(1 + (\alpha^j t) + (\alpha^j t)^2 + \cdots + (\alpha^j t)^7), *, *, *)$$

for non-zero constants c and $j = 0, 1, 4, 2, 5, 3, 6$ respectively. The roots of the equation

$$1 + (\alpha^j t) + (\alpha^j t)^2 + \cdots + (\alpha^j t)^7 = 0$$

are all the non-zero elements of $\mathbf{F}_9$, with the exception of α^{-j}. Hence we see that $C_L(D, 19Q)$ contains 7 elements whose first components are zero, and whose second components are polynomials of degree 7 having roots

- all $t \neq 1$ in $\mathbf{F}_9^*$ $(j = 0)$,
- all $t \neq \alpha^7$ in $\mathbf{F}_9^*$ $(j = 1)$,
- all $t \neq \alpha^4$ in $\mathbf{F}_9^*$ $(j = 4)$,

$\vdots$

- all $t \neq \alpha^2$ in $\mathbf{F}_9^*$ $(j = 6)$.

Since $C_L(D, aQ)$ is a module over $\mathbf{F}_9[t]$, there is some element with zero first component, whose second component is the *greatest common divisor* of these polynomials. The leading component of that element is $t - \alpha = t + \alpha^5$. As we noted before, since 19 is not sufficiently large there is no element of $L(19Q)$ vanishing at all points of

orbit 1 and at all points of orbit 2 except $P_{2,0}$. Hence the *POT* Groebner basis will contain $g^{(2)}$ with diagonal component $t + \alpha^5$.

Finally, we will indicate how the results of Section 5 work in this case. The inverted root diagram constructed from (10) is

1	α	α^2	α^3	α^4	α^5	α^6	α^7
							X
		X	X	X	X	X	X
X				X			
X							

(12)

(For instance, on the second row, we place an X in the position corresponding to $\alpha^{-1} = \alpha^7$.)

We claim the root diagram for the *rPOT* Groebner basis of $C_{\Omega}(D, 19Q)$ on the Hermitian curve over $\mathbf{F}_9$ is found by complementing the inverted root diagram from (12):

1	α	α^2	α^3	α^4	α^5	α^6	α^7
X	X	X	X	X	X	X	X
X	X	X	X	X	X	X	
X	X						

(13)

(By [8, Section VII.4.2], the dual code is the same as $C_L(D, 12Q)$ in this case. That (13) is the correct *rPOT* root diagram can be derived directly by a Groebner basis calculation. We leave the details to the reader.)

References

[1] W. Adams and P. Loustaunau, An Introduction to Gröbner Bases (American Mathematical Society, Providence RI, 1994).

[2] D. Cox, J. Little and D. O'Shea, Ideals, Varieties, and Algorithms (Springer, New York, 1992).

[3] C. Heegard, J. Little and K. Saints, Systematic encoding via Gröbner bases for a class of algebraic geometric Goppa codes, IEEE Trans. Inform. Theory, to appear.

[4] C. Moreno, Algebraic Curves over Finite Fields (Cambridge University Press, Cambridge, 1991).

[5] B.-Z. Shen, On encoding and decoding of the codes from Hermitian curves, in: N.J. Ganley, Ed., Cryptography and Coding III (Oxford University Press, Oxford, 1993).

[6] H. Stichtenoth, Ueber die Automorphismengruppe eines algebraischen Funktionenkoerpers von Primzahlcharakteristik, Arch. der Math. XXIV (1973) 527–544.

[7] H. Stichtenoth, A note on Hermitian codes over GF(q^2), IEEE Trans. Inform. Theory 34 (1988) 1345–1348.
[8] H. Stichtenoth, Algebraic Function Fields and Codes (Springer, Berlin, 1993).
[9] H. Tiersma, Remarks on codes from Hermitian curves, IEEE Trans. Inform. Theory 33 (1987) 605–609.
[10] J.H. van Lint, Introduction to Coding Theory (Springer, New York, 1982).
[11] T. Yaghoobian and I.F. Blake, Hermitian codes as generalized Reed–Solomon codes, Designs, Codes, and Cryptography 2 (1992) 5–17.
[12] K. Yang and P.V. Kumar, On the true minimum distance of Hermitian codes, in: H. Stichtenoth and M.A. Tsfasman, Eds., Coding Theory and Algebraic Geometry: Proc. AGCT-3, Luminy, France, June 1991 (Springer, Berlin, 1992).