On Constructing AG Codes Without Basis Functions for Riemann-Roch Spaces

Drue Coles

Department of Mathematics, Computer Science, and Statistics,
Bloomsburg University
dcoles@bloomu.edu

Abstract. The standard construction of linear error-correcting codes on algebraic curves requires determining a basis for the Riemann-Roch space $\mathcal{L}(G)$ associated to a given divisor G, often a hard problem. Here we consider the problem of constructing the code without any knowledge of such a basis. We interpret the columns of a generator matrix as points on an embedded copy of the curve, and show that in certain cases these points can be realized in principle as the images of a set of vector bundles under a standard map to a class of repartitions.

1 Introduction

Let C denote a smooth projective algebraic curve of genus γ defined over a finite field k. Fix a divisor $D = P_1 + \cdots + P_n$ on C, where each point P_i is rational (over k), and let G be another divisor of degree α with rational support disjoint from that of D. The algebraic-geometric (AG) code given by these two divisors is defined to be

$$C(D, G) = \{(f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G)\}.$$

The code is linear over k, and if $\alpha \geq 2\gamma - 1$ then it has dimension $\alpha - \gamma + 1$ by the Riemann-Roch theorem. The minimum distance is at least $n - \alpha$, since a non-zero function in $\mathcal{L}(G)$ has at most α zeros. AG codes were discovered by Goppa [5] in the early 1980s, and since that time many important practical and theoretical advances have been made, including efficient decoding algorithms (surveyed, for example, in [8]) and polynomial-time constructable codes that beat the Gilbert-Varshamov bound [15, 6, 13].

Usually the divisor G is taken as a multiple of a single point, and here as well we let $G = \alpha Q$ for a rational point $Q \in C$. We assume $\alpha > 2\gamma$ so that the rational map $\varphi : C \to \mathbb{P}^m$ ($m = \alpha - \gamma$) given by the complete linear system $|\alpha Q|$ is an embedding [12–Ch. III, Sect. 6.6].

In practice, a linear code is constructed by computing a generator matrix for it. If $\{f_i\}$ is a basis for $\mathcal{L}(G)$, then we get the rows of a generator matrix for $C(D, G)$ by computing the linearly independent codewords $(f_i(P_1), \ldots, f_i(P_n))$. Equivalently, we can view the points $\varphi(P_i)$ as columns of this matrix.

M. Fossorier et al. (Eds.): AAECC 2006, LNCS 3857, pp. 108–117, 2006.

Computing a basis for a Riemann-Roch space, however, is often a difficult problem. This note describes the theoretical framework for an alternative method of one-point AG code construction. It applies only for certain choices of the point Q, but from a coding standpoint the choice of Q is immaterial since the dimension and distance of an AG code depend only on the *degree* of the divisors used.

The basic idea is to map extensions of lines bundles determined by Q and the points P_i into a class of repartitions via standard sheaf cohomology; elements of the class can be uniquely expressed as a linear combination of certain fixed repartitions of a very simple form, and the coefficients in that combination are precisely the coordinates of $\varphi(P_i)$.

The next section reviews some background material and establishes notation. After proving the main result in the third section, we point out that it can be used to determine the Weierstrass non-gaps at Q, and we demonstrate this fact with an example on the Klein curve. The last section looks at computational aspects of the cohomology maps used in the main result and the algorithmic details that would need to be worked out for an explicit implementation.

2 Background and Notation

Fix a smooth projective curve C of genus γ over a finite field k for the rest of the paper. Let $\bar{k}$ denote the algebraic closure of k. We refer to k-rational points simply as rational points for brevity.

Fix a rational point $Q \in C$ and an integer $\alpha > 2\gamma$, and let φ denote the embedding of the curve determined by the complete linear system $|\alpha Q|$. The goal is to compute $\varphi(P)$ for rational points $P \neq Q$ on the curve without knowing a basis for $\mathcal{L}(\alpha Q)$. In that way, we get the columns of a generator matrix for $C(D, \alpha Q)$, where as usual D is the formal sum of all rational points other than Q. The code has length $n = |Supp(D)|$, and we assume $n > \alpha$.

For $f \in \bar{k}(C)$ and $P \in C$, $\nu_P(f)$ denotes the order of f at P, and $\mathcal{O}_P$ denotes the local ring at P.

We enumerate the Weierstrass non-gaps at Q by $\mu_0, \mu_1, \mu_2, \ldots$

2.1 Extension Spaces

For any rank-2 vector bundle $E \to C$ of degree at least γ, there is line bundle L such that the sequence $0 \to \mathcal{O}_C \to E \to L \to 0$ is exact. Here E is called an extension of L by $\mathcal{O}_C$. Another such extension E' is isomorphic to E if there is an isomorphism of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}_C & \longrightarrow & E & \longrightarrow & L & \longrightarrow & 0 \\ & & \| & & \cong\downarrow & & \| & & \\ 0 & \longrightarrow & \mathcal{O}_C & \longrightarrow & E' & \longrightarrow & L & \longrightarrow & 0. \end{array}$$

We denote by $Ext(L, \mathcal{O}_C)$ the space of extension classes of L by $\mathcal{O}_C$. This has the structure of a linear space over $\bar{k}$ [3–Sect. 5.7].

An extension $E \in Ext(L, \mathcal{O}_C)$ corresponds to an element of $H^1(L^{-1})$ as follows: twist by L^{-1} to get an exact sequence $0 \to L^{-1} \to E \otimes L^{-1} \to \mathcal{O}_C \to 0$, form the associated long exact sequence and take the image of the identity element in $H^0(\mathcal{O}_C)$. Some authors actually define first cohomology directly in terms of extensions, and there is a geometric way of defining a group operation on them [3–Sect. 5.7].

Now $H^1(L^{-1}) \cong H^0(\omega_C \otimes L)^*$ by Serre duality, so we have identified the space $Ext(L, \mathcal{O}_C)$ (modulo scalers) with projective space $\mathbb{P}(H^0(\omega_C \otimes L)^*)$.

2.2 The Segre Invariant and Secant Varieties

The s-invariant of a non-split rank-2 vector bundle E on a smooth projective curve is defined by

$$s(E) = \deg E - 2 \max\{\deg M : M \hookrightarrow E\},$$

where M runs over all line subbundles of E. Let (e) denote the rank-2 extension E viewed as a point of projective space $\mathbb{P}$. Lange and Narasimhan [10], following Atiyah [1], showed that $s(E)$ is determined by the smallest integer j such that (e) is contained in the j-secant variety of the curve in $\mathbb{P}$. This picture was also described by Bertram [2], and later Trygve Johnsen observed that it leads to an interpretation of decoding AG codes in terms of vector bundles on the underlying curve [9].

It turns out that $(e) = \varphi(P)$ if and only if $\mathcal{O}_C(P)$ is a quotient line bundle of E. This fact is really just a special case of [10–Proposition 1.1], made more explicit by [9–Proposition 2.5]. Summarizing with the notation established at the beginning of this section, we have:

Proposition 1. *Let $L = \mathcal{O}_C(\alpha Q - K)$. For any point $P \in C$, there is a unique extension $E \in Ext(L, \mathcal{O}_C)$ with quotient line bundle $\mathcal{O}_C(P)$, and E corresponds to $\varphi(P)$ as a point of projective space with respect to the embedding φ determined by $|\alpha Q|$.*

2.3 Repartitions

A repartition r associates to each point $P \in C$ a function $r_P \in \bar{k}(C)$, with $r_P \in \mathcal{O}_P$ for all but finitely many points. R denotes the ring of repartitions, and $\bar{k}(C)$ is viewed as a subring by identifying $f \in \bar{k}(C)$ with the repartition that assigns f to each point of the curve. If $f \in \bar{k}(C)$ and $Q \in C$, then we write f/Q for the repartition that assigns f to Q and zero to every other point.

Given a divisor A, $R(A)$ denotes the additive subgroup of repartitions $r \in R$ satisfying $\nu_P(r_P) + \nu_P(A) \geq 0$ for every point $P \in C$. There is a canonical isomorphism

$$H^1(\mathcal{O}_C(A)) \;\cong\; R \,/\, \big(R(A) + \bar{k}(C)\big)\,.$$

Serre proves this fact [14–Proposition II.3] and uses it to prove the duality theorem for curves.

For a divisor G, we therefore have

$$H^0(\mathcal{O}_C(G))^* \;\cong\; H^1(\mathcal{O}_C(K-G)) \;\cong\; R\,/\,\big(R(K-G)+\bar{k}(C)\big)$$

When G is a multiple of a single point, there is a basis for $R/(R(K-G)+\bar{k}(C))$ consisting of repartitions of an especially simple form; using our notation, this result can be stated as:

Proposition 2. *For a local parameter t at Q, define the differential $\omega = dt$ in a neighborhood of Q and let $K = (\omega)$. Then the set $\{t^{\mu_i - 1}/Q : 0 \le i \le m\}$ is a basis for the vector space $R/(R(K-\alpha Q)+\bar{k}(C))$ over $\bar{k}$.*

This was used to compute a transition matrix for the rank-2 extension that corresponds as a point in projective space to the syndrome of a corrupted codeword [4–Proposition 1]. The proof is repeated in the appendix of this paper.

3 Constructing a Generator Matrix

Recall that the columns of a generator matrix for $C(D, \alpha Q)$ are given explicitly by the points $\varphi(D)$, where φ is the embedding of C determined by $|\alpha Q|$.

Theorem 1. *For a local parameter t at Q, define the differential $\omega = dt$ in a neighborhood of Q and let $K = (\omega)$. Suppose there is a basis $S = \{f_1, \ldots, f_\gamma\}$ for $\mathcal{L}(K)$ consisting of functions that have a single non-zero term of degree less than α when expanded in powers of t. Then for any point $P \neq Q$ on the curve, $\varphi(P) = (c_0 : \cdots : c_m)$ if and only if the repartition $(c_0 t^{\mu_0 - 1} + \cdots + c_m t^{\mu_m - 1})/Q$ corresponds to the unique extension $E \in Ext(\mathcal{O}_C(\alpha Q - K), \mathcal{O}_C)$ with quotient line bundle $\mathcal{O}_C(P)$.*

Proof. Since ω is regular and non-zero at Q by definition, any function in $\mathcal{L}(K)$ is regular at Q. Distinct functions $f_i, f_j \in S$ have distinct orders at Q, for otherwise $\nu_Q(f_i - f_j) \ge \alpha$ by the hypothesized property of elements of S, which would not be possible since $f_i - f_j \in \mathcal{L}(K)$ can have at most $2\gamma - 2 < \alpha$ zeros.

Let $n_i = \nu_Q(f_i)$. We will show that $t^{n_i}/Q \in R(K-\alpha Q) + \bar{k}(C)$ for $1 \le i \le \gamma$.

Multiplying each f_i by a constant if necessary, we can write

$$f_i \;=\; t^i + \sum_{j=\alpha}^{\infty} b_{ij} \cdot t^j$$

with uniquely determined coefficients $b_{ij} \in \bar{k}$. Now for each function $f_i \in S$, we define a repartition r_i by

$$(r_i)_P \;=\; \begin{cases} f_i - t^{n_i} \;:\; P = Q \\ -f_i \;:\; P \neq Q. \end{cases}$$

We have $\nu_Q((r_i)_Q) \ge \alpha$, and since $f_i \in \mathcal{L}(K)$ it follows that $r_i \in R(K-\alpha Q)$. Now $r_i + f_i = t^{n_i}/Q$, so $t^{n_i}/Q \in R(K-\alpha Q) + \bar{k}(C)$ as claimed.

Let $A = \{t^i/Q : 0 \leq i \leq \alpha\}$. We have just shown that there are γ elements of A that are zero in the space $R/R(K - \alpha Q) + \bar{k}(C))$, namely each t^{n_i}/Q. On the other hand, Proposition 2 provides a basis for this space consisting of the remaining $m + 1 = \alpha - \gamma + 1$ elements of A. Consequently, any element of $R/R(K - \alpha Q) + \bar{k}(C))$ can be uniquely expressed as a linear combination of the particular $m + 1$ elements of A specified in the proposition.

By Proposition 1, there is a unique extension $E \in Ext(\mathcal{O}_C(\alpha Q - K), \mathcal{O}_C)$ with quotient bundle $\mathcal{O}_C(P)$; the extension corresponds via Serre duality to the point $\varphi(P) \in \mathbb{P}(H^0(\mathcal{O}_C(\alpha Q))^*)$, and the isomorphism

$$H^0(\mathcal{O}_C(\alpha Q))^* \quad \xrightarrow{\sim} \quad R \,/\, \big(R(K - \alpha Q) + \bar{k}(C)\big)$$

is realized by $(c_0, \ldots, c_m) \mapsto \big(c_0 t^{\mu_0 - 1} + \cdots + c_m t^{\mu_m - 1}\big) \,/\, Q$. □

3.1 Computing Weierstrass Non-gaps

Suppose that for some fixed positive integer $i < \alpha$, the repartition corresponding to a given point $\varphi(P)$ is simply t^i/Q. This means that $\varphi(P)$ has a single non-zero coordinate. But we do not know *which* coordinate is non-zero unless we also happen to know where the integer i lies among the exponents $\mu_0 - 1, \ldots, \mu_m - 1$, or in other words, unless we know the Weierstrass non-gaps at Q.

Consider, however, the set of all points $\varphi(P_1), \ldots, \varphi(P_n)$. It is not possible that all of them are zero at the same coordinate, for otherwise there would exist a non-zero function in $\mathcal{L}(\alpha Q)$ that vanishes at $n > \alpha Q$ points. We can therefore think of Theorem 1 as *determining* the non-gaps at Q. This is illustrated below. Of course, this observation does not translate directly into an effective algorithm for computing the non-gaps at certain points since the cohomology maps that we are using have been described in a completely abstract fashion. Section 4 discusses the algorithmic aspects of Theorem 1.

3.2 Illustration

Let C denote the Klein curve of genus 3 defined by $x^3y + y^3z + z^3x = 0$. We will use Theorem 1 with $\alpha = 5$ (the highest possible non-gap) to compute the Weierstrass non-gaps at $Q_1 = (1 : 0 : 0)$. Let $Q_2 = (0 : 1 : 0)$ and $Q_3 = (0 : 0 : 1)$. These latter two points also lie on the curve. Computing the intersection divisors of the three lines $xyz = 0$ with the curve, we have:

$$\begin{aligned} div(x) &= 3Q_3 + Q_2 \\ div(y) &= 3Q_1 + Q_3 \\ div(z) &= 3Q_2 + Q_1 \end{aligned}$$

We can use this information to obtain the order of a monomial at any of the points Q_i. In particular, we see that $t = z/x$ is a local parameter at Q_1.

Define the differential $\omega = dt$ in the open set $U = \{(x : y : z) \in C : x \neq 0\}$, and let $K = (\omega)$.

Lemma 1. $K = 3Q_3 + Q_2$.

Proof. A point $P \in U$ has the form $P = (1 : b : c)$. Note that $t' = (z + cx)/x$ is a local parameter at P, and $dt' = dt$. It follows that ω has no zeros on U, so the support of K must be contained in $C \setminus U = \{Q_2, Q_3\}$. A canonical divisor on a plane quartic is the intersection divisor of a line with the curve, and the only such divisor supported by Q_2 and Q_3 is the intersection divisor of the line $x = 0$ with the curve; that is, $3Q_3 + Q_2$. □

Lemma 2. *The set* $\{1,\ z/x,\ y/x\}$ *is a basis for* $\mathcal{L}(K)$.

Proof. The dimension of $\mathcal{L}(K)$ is 3 (genus), and we see that the given functions are contained in $\mathcal{L}(K)$ by checking the intersection divisors of the lines $xyz = 0$ with the curve. For linear independence, note that the functions have distinct orders at Q_1. □

We want to verify that the basis given by the preceding lemma satisfies the hypothesis of Theorem 1; that is, the basis functions have a single non-zero term of degree less than $\alpha = 5$ when expanded in powers of $t = z/x$. Obviously, we only need to look at y/x, which vanishes at Q_1 with order 3. The first term in the expansion of y/x is t^3, and to determine the next term we compute

$$y/x - t^3 \quad = \quad (x^3y + xz^3)/x^4 \quad = \quad y^3z/x^4.$$

Since $\nu_{Q_1}(y^3z/x^4) = 10$, the expansion of y/x in powers of t has exactly one non-zero term of degree less than α. The basis functions therefore satisfy the hypothesis of Theorem 1. They vanish at Q_1 with orders 0, 1 and 3, and the proof of Theorem 1 show that in this case

$$\{1/Q_1,\ t/Q_1,\ t^3/Q_1\} \quad \subset \quad R/R(K - 5Q_1) + \overline{k}(C)).$$

On the other hand, $\{t^{\mu_i - 1} : 0 \leq i \leq 2\}$ is a basis for $R/(R(K - 5Q) + \overline{k}(C))$ according to Proposition 2, and the values 0, 1 and 3 have been excluded as possible values for $\mu_i - 1$, leaving -1, 2 and 4. The non-gaps μ_i at Q_1 are therefore 0, 3 and 5.

Indeed, the set $\{1,\ x/y,\ xz/y^2\}$ is a basis for $\mathcal{L}(5Q_1)$, and the functions in this basis have pole orders 0, 3, and 5 at Q_1.

4 Algorithmic Questions

Theorem 1 provides the theoretical framework for computing the points $\varphi(P)$ via cohomology maps, but three main computational problems must be solved to apply the theorem in practice:

1. Compute a concrete representation of the unique extension

$$E \in Ext(\mathcal{O}_C(\alpha Q - K), \mathcal{O}_C)$$

with quotient bundle $\mathcal{O}_C(P)$ for each rational point $P \neq Q$.

2. Compute the image of E under the map
$$\psi \ : \ Ext\left(\mathcal{O}_C(K-\alpha Q), \mathcal{O}_C\right) \ \xrightarrow{\sim} \ R \,/\, \left(R(K-\alpha Q) + \bar{k}(C)\right).$$
3. If $\psi(E) \in R/(R(K-\alpha Q) + \bar{k}(C))$ is not of the form $\sum_{i=0}^{\alpha} c_i t^{\mu_i - 1}/Q$, then translate it into the unique representative of its equivalence class having that form.

We look briefly at each of these questions in turn.

4.1 Concrete Representations of Rank-2 Extensions

The problem is to find the extension $E \in Ext(\mathcal{O}_C(\alpha Q - K), \mathcal{O}_C)$ with quotient line bundle $\mathcal{O}_C(P)$, or equivalently with line subbundle $\mathcal{O}_C(\alpha Q - K - P)$. Here we quickly review the idea of a vector bundle as an abstract algebraic variety, and a subbundle as an embedding of varieties. The basic facts can be looked up in Shafarevich [12–Chap. VI]. Then following the definitions, we translate the problem of finding the desired rank-2 bundle into a search for rational functions on the curve satisfying a certain linear relation.

Consider a line bundle $L \to C$, say $L = \mathcal{O}_C(A)$ for a divisor A. Since the base space C is a curve, there is a covering by two open sets with L trivial over each. Fix such a covering (U_1, U_2), and let $U_{12} = U_1 \cap U_2$. Then L is realized as an abstract algebraic variety by glueing the two affine varieties $U_i \times \bar{k}$ along their intersection. In particular, it is represented by a transition function $h \in \mathcal{O}_C(U_{12})^*$ that for each $x \in U_{12}$ identifies the point $(x, a) \in U_1 \times \bar{k}$ with the point $(x, h(a)) \in U_2 \times \bar{k}$. If A has local equations h_i in U_i, then we may take $h = h_2/h_1$. Then an extension $E \in Ext(L, \mathcal{O}_C)$ is represented by a transition matrix
$$M = \begin{pmatrix} 1 & 0 \\ g & h \end{pmatrix},$$
where $g \in \bar{k}(C)$ depends on the class of E. This matrix determines the glueing relation for the affine varieties $U_1 \times \bar{k}^2$ and $U_2 \times \bar{k}^2$.

Considering vector bundles as abstract algebraic varieties, an embedding
$$\varphi \ : \ L \to E$$
is a regular map of varieties that preserves fibers, and on each fiber induces a linear map $\bar{k} \to \bar{k}^2$. This means that there are regular functions r_i and s_i on U_i $(i = 0, 1)$ such that $\varphi|_{U_i \times k} : (x, a) \mapsto (x, r_i(x) \cdot a, s_i(x) \cdot a)$, and these functions preserve the gluing relation of E; in our case, it means
$$f \cdot (r_2, s_2) = \begin{pmatrix} 1 & 0 \\ g & h \end{pmatrix} \begin{pmatrix} r_1 \\ s_1 \end{pmatrix}$$
on the intersection U_{12}, where f is a transition function for $L = \mathcal{O}_C(\alpha Q - K - P)$. We may take $f = hp^{-1}$, where p is a transition function for $\mathcal{O}_C(P)$. Note that for suitable choices of the trivializing cover $\{U_i\}$, it is easy to obtain local equations for the rational points of the curve, or for any divisor with rational support.

In summary, we get a transition matrix for $E \in Ext(\mathcal{O}_C(\alpha Q - K), \mathcal{O}_C)$ with quotient line bundle $\mathcal{O}_C(P)$ by finding $g \in \bar{k}(C)$ and $r_i, s_i \in \mathcal{O}_C(U_i)$ that

$$f \cdot r_2 = r_1$$
$$f \cdot s_2 = g \cdot r_1 + h \cdot s_1$$

on the intersection U_{12}.

4.2 Cohomology Maps

Our map ψ is a composition of three maps

$$\begin{aligned} Ext(\mathcal{O}_C(\alpha Q - K), \mathcal{O}_C) &\longrightarrow Ext(\mathcal{O}_C, \mathcal{O}_C(K - \alpha Q)) && (1)\\ &\longrightarrow H^1(\mathcal{O}_C(K - \alpha Q)) && (2)\\ &\longrightarrow R/(R(K - \alpha Q) + \bar{k}(C)) && (3) \end{aligned}$$

The first map takes an extension of the form $0 \to \mathcal{O}_C \to E \to \mathcal{O}_C(\alpha Q - K) \to 0$ and twists by $\mathcal{O}_C(K - \alpha Q)$ to obtain $0 \to \mathcal{O}_C(K - \alpha Q) \to E' \to \mathcal{O}_C \to 0$. What this means concretely, in terms of transition matrices, is multiplying each entry of a transition matrix for E by a transition function for $\mathcal{O}_C(\alpha Q - K)$ to obtain a transition matrix for E'.

The second map arises by forming the associated long exact sequence and taking the image of the identity element under $H^0(\mathcal{O}_C) \to H^1(\mathcal{O}_C(K - \alpha Q))$. But here the picture seems too abstract for direct computation. It may simplify matters to use the Cech cohomology, but care is needed to choose a suitable open cover so that the Cech cohomology agrees with the derived functor cohomology; see Hartshorne [7–Chap. III] on this point.

The map to repartitions (3) is described by Serre [12–Proposition II.3], and there also one may need to recast the details in terms of Cech cohomology for a more computationally concrete picture.

4.3 Translating Repartitions

Let us define the *support* of a repartition r to be the set of points P at which $r_P \neq 0$. We begin by noting that for any divisor A, a repartition with infinite support is equivalent modulo $R(A)$ to one with finite support: for example, if $r' \in R$ is defined by

$$r'_P = \begin{cases} r_p & : \ P \notin Supp\,(A) \text{ and } \nu_P(r_p) \geq 0 \\ 0 & : \ \text{otherwise} \end{cases}$$

then $r - r' \equiv r$ has finite support. Recall that we identify $f \in \bar{k}(C)$ with the repartition that assigns f to every point. If we take $f = r_Q$, then $r - f$ does not have Q in its support and it is equivalent to r modulo $R(K - \alpha Q) + \bar{k}(C)$. We may therefore assume that a given repartition r, viewed as an element of $R\,/(R(K - \alpha Q) + \bar{k})$, is supported by finitely many points, Q not among them.

Proposition 1 says that any $r \in R$ is equivalent modulo $R(K - \alpha Q) + \bar{k}(C)$ to a linear combination of the repartitions $t^{\mu_i - 1}/Q$ for $0 \leq i \leq m$. This means that there are unique coefficients $c_i \in \bar{k}$ and a function $f \in \bar{k}(C)$ such that

$$r - f + \left(\sum_i c_i t^{\mu_i - 1}/Q \right) \in R(K - \alpha Q).$$

Equivalently, assuming $r_Q = 0$ as discussed above, the coefficients c_i and the function f must satisfy:

1. $\nu_P(r_P - f) \geq -\nu_P(K)$ for all $P \neq Q$;
2. $\nu_Q(\sum_i c_i t^{\mu_i} - f) \geq \alpha$.

The existence of f satisfying (1) is guaranteed by the Strong Approximation Theorem [11–Chap. 12]; moreover, since $\alpha > m$, (2) implies that f is regular at Q and the coefficients c_i can be obtained from the initial part of its expansion in powers of t.

References

1. M. Atiyah. *Complex fibre bundles and ruled surfaces*, Proc. London Math. Soc., vol. 5, pp. 407–434, 1955.
2. A. Bertram. *Moduli of rank-2 vector bundles, theta divisors, and the geometry of curves in projective space*, Journal of Diff. Geometry, vol. 35, pp. 429–469, 1992.
3. F. Bogomolov and T. Petrov. *Algebraic Curves and One-Dimensional Fields*, Providence, RI: Amer. Math. Soc., 2002, Courant Lecture Notes in Mathematics.
4. D. Coles. *Vector Bundles and Codes on the Hermitian Curve*, IEEE Trans. Inf. Theory, vol. 51, no. 6, pp. 2113–2120, 2005.
5. V.D. Goppa. *Codes on algebraic curves*, Soviet Math. Dokl., vol. 24, pp. 170–172, 1981.
6. A. Garcia and H. Stichtenoth. *A Tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound*, Invent. Math., vol. 121, pp. 211–222, 1995.
7. R. Hartshorne. *Algebraic Geometry*, Springer-Verlag, New York, 1977.
8. T. Høholdt and R. Pellikaan. *On the decoding of algebraic-geometric codes*, IEEE Trans. Inf. Theory, vol. 41, no. 6, pp. 1589–1614, 1995.
9. T. Johnsen. *Rank two bundles on Algebraic Curves and decoding of Goppa Codes*, International Journal of Pure and Applied Mathematics, vol. 4, no. 1, pp. 33–45, 2003.
10. H. Lange and M.S. Narasimhan. *Maximal Subbundles of Rank Two Vector Bundles on Curves*, Math. Ann., vol. 266, pp. 55–72, 1983.
11. O. Pretzel. *Codes and Algebraic Curves*, Oxford University Press, 1998.
12. I. R. Shararevich. *Basic Algebraic Geometry 1-2*, 2nd edition, Springer-Verlag, New York, 1994. Translated by M. Reid.
13. K. W. Shum, I. Aleshnikov, P. V. Kumar, H. Stichtenoth, V. Deolalikar. *A Low-Complexity Algorithm for the Construction of Algebraic-Geometric Codes Better Than the Gilbert-Varshamov Bound*, IEEE Trans. Inf. Theory, vol. 47, no. 6, pp. 2225–2241, 2001.

14. J.-P. Serre. *Algebraic Groups and Class Fields*, Springer-Verlag, New York, 1988.
15. M.A. Tsfasman, S.G. Vlăduţ, and T. Zink. *Modular curves, Shimura curves and Goppa codes better than the Varshamov-Gilbert bound*, Mathematische Nachrichten, vol. 109, pp. 21–28, 1982.

A The Proof of Proposition 2

This comes directly from [4], with minor rewording.

Applying Serre's proof of the duality theorem for curves [14–Proposition II.3] to our situation, we note that $\Omega^1(K - \alpha Q) \cong H^0(\alpha Q)$ is put in duality with $R/(R(K - \alpha Q) + \bar{k}(C))$ by the pairing

$$\langle \omega, r \rangle \;=\; \sum_{P \in C} Res_P(r_P \cdot \omega). \tag{4}$$

Fix a basis $\{f_i\}$ for $\mathcal{L}(\alpha Q)$. We may assume $\nu_Q(f_i) = \mu_i$ (the i-th Weierstrass non-gap at Q). Let $a(i,j) \in \bar{k}$ denote the coefficient of t^j in the expansion of f_i in powers of t; that is,

$$f_i \;=\; \sum_{r=-\mu_i}^{\infty} a(i,r) \cdot t^r.$$

Now suppose for a moment that there are distinct indices i and j for which $a(i,-\mu_j) \neq 0$. Thus while f_j has a pole of order μ_j at Q, there is a non-zero coefficient of $t^{-\mu_j}$ in the expansion of some other function f_i with a higher pole order at Q. Since $\nu_Q(f_i - a(i,-\mu_j) \cdot f_j) = -\mu_i$, we may replace f_i with $f_i - a(i,-\mu_j) \cdot f_j$ to obtain another basis for $\mathcal{L}(\alpha Q)$; moreover, the coefficient of $t^{-\mu_j}$ in the expansion of this new function is zero. We may therefore assume that $a(i,-\mu_j) = 0$ if and only if $i \neq j$. Letting $\omega_i = f_i \cdot dt$ in an open neighborhood of Q, we can write $Res_Q(t^{n_j - 1} \cdot \omega_i) \;=\; a(i,-n_j)$; that is,

$$Res_Q(t^{n_j - 1} \cdot \omega_i) = 0 \;\longleftrightarrow\; i \neq j.$$

Combining this with (4), we have

$$\langle \omega_i,\, t^{n_j - 1}/\, Q \rangle = 0 \;\longleftrightarrow\; i \neq j.$$

Referring again to (4), we see that every differential $\omega \in \Omega^1(K - \alpha Q)$ defines a linear functional $\langle \omega, \cdot \rangle$ on $R/(R(K - \alpha Q) + \bar{k}(C))$. Indeed, $\langle \omega, r \rangle = 0$ for all $r \in R(K - \alpha Q)$ since $r_P \cdot \omega$ has no poles for any point $P \in C$, and $\langle \omega, r \rangle = 0$ for all repartitions $r \in \bar{k}(C)$ by the Residue Theorem.

We have contructed a basis $\{t^{\mu_j - 1}/Q\}$ in the standard way for the space $R/(R(K - \alpha Q) + \bar{k}(C))$ in terms of a basis $\{\omega_i\}$ for the dual space. That is, $\langle \omega_i,\, t^{n_j - 1} \rangle = 0$ if and only if $i \neq j$. □