1999

Algebraic geometric codes over rings

Judy L. Walker
University of Nebraska - Lincoln, judy.walker@unl.edu

Published in Journal of Pure and Applied Algebra 144 (1999), pp 91-110
doi 10.1016/S0022-4049(98)00047-4

ALGEBRAIC GEOMETRIC CODES OVER RINGS

JUDY L. WALKER

Abstract. The techniques of algebraic geometry have been widely and successfully applied to the study of linear codes over finite fields since the early 1980's. Recently, there has been an increased interest in the study of linear codes over finite rings. In this paper, we combine these two approaches to coding theory by introducing the study of algebraic geometric codes over rings. In addition to defining these new codes, we prove several results about their properties.

1. Introduction

Whenever data is transmitted across a channel, errors are likely to occur. The data is usually encoded as a string of zeros and ones of fixed length, that is, as a vector over $\mathbb{F}_2$. The set of all possible data vectors is then a subset of $\mathbb{F}_2^n$. More generally, a code of length n over $\mathbb{F}_q$ is a subset C of $\mathbb{F}_q^n$, and elements of C are called codewords. It is the goal of coding theory to construct codes which have many codewords, which are easy to encode and decode, and which correct errors.

Traditionally, the main tools used in coding theory have been those of combinatorics and group theory. In 1977, V. D. Goppa defined algebraic geometric codes [4], thus allowing a wide range of techniques from algebraic geometry to be applied. This idea of Goppa's has had a great impact on the field. Not long after Goppa's original paper, Tsfasman, Vlăduţ and Zink [14] used modular curves to construct a sequence of codes with asymptotically better parameters than any previously known codes. Further, old conjectures in coding theory are now being approached in a new way via the new techniques, and new results in algebraic geometry have been proven as a result of the connection with coding theory.

Another recent twist in the study of codes is the attention now paid to linear codes over finite rings. The main reason for the recent increased interest in these codes is the 1994 paper of Hammons, Kumar, Calderbank, Sloane, and Solé [6] which shows that certain nonlinear binary codes are in fact nonlinear projections of linear codes over $\mathbb{Z}/4$. These nonlinear codes include such famous codes as the Nordstrom-Robinson code and the Kerdock and Preparata codes. Following the ideas of that paper, other authors (see, for example, [2]) have constructed new linear $\mathbb{Z}/4$ codes in such a way that their nonlinear binary projections have more codewords than any previously known codes of the same length and minimum distance.

1991 *Mathematics Subject Classification.* Primary 94B; Secondary 14, 11.
Key words and phrases. Codes, Algebraic geometry.
The material in this article is a portion of the author's Ph.D. thesis, which was completed at the University of Illinois. The author thanks her thesis advisor, Professor Nigel Boston, for his advice, support, and encouragement.

The object of this paper is to combine these areas of coding theory by introducing and studying algebraic geometric codes over rings. In section 2, we give a review of the basic definitions, notations, and results on linear codes over finite fields, including algebraic geometric codes. In Section 3, we study linear codes over rings. In particular, we explore the relationship with associated linear codes over finite fields and obtain new results in this regard. Section 4 gives the background we need from the algebraic geometry of curves over rings. It is our belief that many of the results of this section are known, so we only list them here. Complete proofs can be found in [17]. Section 5 is the heart of the paper. It contains the definition of algebraic geometric codes over rings, as well as the proofs of the theorems about them mentioned above. In Section 6, we discuss some applications of this new theory.

We use the standard terminology and notation of commutative algebra and algebraic geometry, as in [5], [10], and [8].

2. Linear Codes over Finite Fields

The purpose of this short section is to catalog some basic definitions and results about linear codes over finite fields, including algebraic geometric codes over finite fields. The references for this section are [9], [11], [13], and [15]. We begin with some definitions.

A *code* C of *length* n over the finite field $\mathbb{F}_q$ is a subset of the vector space $\mathbb{F}_q^n$. If C is actually a subspace, it is called a *linear code* and its *dimension* k is its dimension as a $\mathbb{F}_q$-vector space. Elements of C are called *codewords*.

The *Hamming distance* $d(\mathbf{x}, \mathbf{y})$ on $\mathbb{F}_q^n$ is given by

$$d(\mathbf{x}, \mathbf{y}) = \#\{i : x_i \neq y_i\}.$$

The *Hamming weight* of a vector $\mathbf{x}$ in $\mathbb{F}_q^n$ is defined as $d(\mathbf{x}, \mathbf{0})$. The *minimum (Hamming) distance* d of C is

$$d = d(C) = \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x} \neq \mathbf{y} \in C\}.$$

For linear codes, this is equivalent to the minimum Hamming weight of the nonzero codewords of C.

We can also define a symmetric bilinear form on $\mathbb{F}_q^n$ by

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i.$$

The *dual code* $C^\perp$ of C is then defined as

$$C^\perp = \{\mathbf{y} \in \mathbb{F}_q^n : \mathbf{x} \cdot \mathbf{y} = 0 \text{ for every } \mathbf{x} \in C\}.$$

It can be proven that if C is a linear code of dimension k, then $C^\perp$ is a linear code of dimension $n - k$. Also, it is easy to see that $(C^\perp)^\perp = C$. Note that it is possible to have a vector $\mathbf{x} \in \mathbb{F}_q^n$ such that $\mathbf{x} \cdot \mathbf{x} = 0$, so that $C \cap C^\perp \neq \mathbf{0}$ in general.

There are two standard definitions of algebraic geometric codes. Both start with a smooth, absolutely irreducible, projective curve X over $\mathbb{F}_q$, a set $\mathcal{P} \subset X(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on X, and a divisor D on X. Assume that $\operatorname{supp} D \cap \mathcal{P} = \emptyset$, and also use the symbol $\mathcal{P}$ to denote the divisor $P_1 + \cdots + P_n$. The first algebraic geometric code associated to X, $\mathcal{P}$, and D is given by

$$C_L = C_L(X, \mathcal{P}, D) = \{(f(P_1), \ldots, f(P_n)) : f \in L(D)\}.$$

The second algebraic geometric code associated to X, $\mathcal{P}$, and D is given by

$$C_\Omega = C_\Omega(X, \mathcal{P}, D) = \{(res_{P_1}(\nu), \ldots, res_{P_n}(\nu)) : \nu \in \Omega(\mathcal{P} - D)\}.$$

We summarize the properties of C_L and C_Ω in a theorem, due to Goppa. See [11], [13], or [15] for the proof.

Theorem 2.1. *Let X, $\mathcal{P}$ and D be as above, and suppose that $0 \leq \deg D < n = |\mathcal{P}|$. Then*

1. *C_L is a linear code of length n. The dimension k_L and minimum distance d_L of C_L satisfy*
$$k_L \geq \deg D + 1 - g,$$
$$d_L \geq n - \deg D.$$
2. *C_Ω is a linear code of length n. Its dimension k_Ω and minimum distance d_Ω satisfy*
$$k_\Omega \geq n - \deg D + 1 - g,$$
$$d_\Omega \geq \deg D - 2g + 2.$$

If, in addition, we have $2g - 2 < \deg D$, then

1. *$k_L = \deg D + 1 - g$, and*
2. *$k_\Omega = n - \deg D + 1 - g$.*

Further, regardless of $\deg D$,

$$C_L{}^\perp = C_\Omega,$$

and there is a canonical divisor K such that

$$C_L(X, \mathcal{P}, K + \mathcal{P} - D) = C_\Omega(X, \mathcal{P}, D).$$

Hence, for a fixed X and $\mathcal{P}$, the class of algebraic geometric codes $C_L(X, \mathcal{P}, D)$ is closed under duals as D varies.

3. Linear Codes over Rings

Definition 3.1. Let A be a ring. A *linear code* C of *length* n over A is a submodule of the free module A^n. If C itself is isomorphic to a free A-module, then we say C is a *free code* and we define the *dimension* of C to be $\dim C = \text{rank}_A(C)$. We define a symmetric bilinear form on A^n by

$$(a_1, \ldots, a_n) \cdot (a'_1, \ldots, a'_n) = \sum_{i=1}^{n} a_i a'_i$$

and then the *dual code* $C^\perp$ of a linear code C over A is defined in the usual way.

In the rest of this paper, we will assume that A denotes a local Artinian ring, $\mathfrak{m}$ its maximal ideal, and $\pi : A \to A/\mathfrak{m}$ the natural surjection. Later, we will assume that $A/\mathfrak{m}$ is finite. We denote by $\mathfrak{m}^s$ the s^{th} power of $\mathfrak{m}$, and by $\mathfrak{m}^{\times n}$ the Cartesian product of n copies of $\mathfrak{m}$. Elements of A^n will be called *vectors*. A vector which is an element of a code $C \subset A^n$ will also be called a *codeword*.

We will use the following lemmas often.

Lemma 3.2. *Let $k < n$ be integers, and let $f : A^k \hookrightarrow A^n$ be any inclusion. Then f splits. Hence, if C is a free linear code of length n and dimension k over A and $\pi : A^n \to (A/\mathfrak{m})^n$ denotes coordinatewise projection, then $\pi(C) = C/\mathfrak{m}C$.*

Proof. We can represent f as an $n \times k$ matrix of rank k over A. Suppose $\mathfrak{m}^s = 0$ but $\mathfrak{m}^{s-1} \neq 0$. Not all entries of the matrix lie in $\mathfrak{m}$, since then any vector which has all of its coordinates in $\mathfrak{m}^{s-1}$ would lie in the kernel of f. Therefore, some entry of the matrix is a unit. By performing row and column operations, we may assume that the top left entry is the identity of A and the rest of the first row and column are zeros. The matrix obtained by deleting the first row and column of this matrix will represent an injection $A^{k-1} \hookrightarrow A^{n-1}$, so we repeat the above argument. Eventually, we will have a matrix which is a $k \times k$ identity matrix above a $(n-k) \times k$ zero matrix, so that the corresponding map is the standard injection of A^k into A^n. This map splits, so our original f must also.

The last sentence of the Lemma follows by replacing the arbitrary A^k with our code C. The above argument shows that injection $C \hookrightarrow A^n$ splits. Since the functor $- \otimes A/\mathfrak{m}$ preserves split injections, both horizontal arrows in the commutative diagram

$$\begin{array}{ccc} C & \longrightarrow & A^n \\ \downarrow & & \downarrow \\ C \otimes A/\mathfrak{m} & \longrightarrow & (A/\mathfrak{m})^n \end{array}$$

are injections. Hence $\mathfrak{m}^{\times n} \cap C = \mathfrak{m}C$, and so $\pi(C) = C/\mathfrak{m}C$. □

Lemma 3.3. *Let $\mathbf{u}_1, \ldots, \mathbf{u}_d \in A^n$ be vectors over A. If there are elements $a_1, \ldots, a_d \in A$ with at least one $a_i \neq 0$ satisfying $a_1\mathbf{u}_1 + \cdots + a_d\mathbf{u}_d = 0$, then the vectors $\pi(\mathbf{u}_1), \ldots, \pi(\mathbf{u}_d)$ are linearly dependent over $A/\mathfrak{m}$.*

Proof. We prove the contrapositive of this statement, which we phrase as follows: If a map $\varphi : A^d \to A^n$ induces a map $\bar{\varphi} : (A/\mathfrak{m})^d \to (A/\mathfrak{m})^n$ of rank d, then φ is injective. To prove this statement, notice that some $d \times d$ minor of the matrix of $\bar{\varphi}$ is nonzero, i.e., a unit of $A/\mathfrak{m}$. Hence the corresponding $d \times d$ minor of the matrix of φ is a unit of A. Thus this minor has an inverse which gives a splitting $A^n \to A^d$, and the map φ is injective. □

The next result gives a somewhat surprising relationship between the minimum Hamming distance of a code over a ring and that of its coordinatewise projection.

Theorem 3.4. *Let C be a linear code over A and $\bar{C} = \pi(C)$ its coordinatewise projection. Let d and $\bar{d}$ denote the minimum Hamming distances of C and $\bar{C}$, respectively. Assume that $\bar{C} \neq \{\mathbf{0}\}$, so that $\bar{d} > 0$. Then*

1. *$d \leq \bar{d}$, and*
2. *if C is free, then $d = \bar{d}$.*

Proof. (1) Suppose that $\mathbf{y} \in \bar{C}$ has weight $\bar{d} > 0$. Choose $\mathbf{x} \in C$ with $\pi(\mathbf{x}) = \mathbf{y}$. Then $\mathrm{wt}(\mathbf{x}) \geq \bar{d}$. Further, exactly $\bar{d}$ coordinates of $\mathbf{x}$ lie in $A^\times$ and the other $n - \bar{d}$ coordinates belong to $\mathfrak{m}$. Since A is Artinian, there is some s so that $\mathfrak{m}^{s-1} \neq 0$ and $\mathfrak{m}^s = 0$. Choosing $a \in \mathfrak{m}^{s-1} \setminus \{0\}$, we have $a\mathbf{x} \in C$, $a\mathbf{x} \neq 0$, and $\mathrm{wt}(a\mathbf{x}) = \bar{d}$. Hence $d \leq \bar{d}$.

(2) Assume C is free, and suppose $d < \bar{d}$. Let H be a parity check matrix for C, so that $\bar{H}$ is a parity check matrix for $\bar{C}$. By a generalized version of a well-known result for codes over fields (see Theorem 1.10 of [9] for the result for codes over finite fields and Proposition 3.5 of [17] for the generalized result to codes over rings), every d columns of $\bar{H}$ are linearly independent over $A/\mathfrak{m}$ but some d columns

of H are linearly dependent over A. Applying Lemma 3.3 to these d columns of H gives a contradiction. □

Remark 3.5. If C is not free, it may be true that $d = \bar{d}$ or $d < \bar{d}$. For example, if C is the code

$$C = \{(00), (10), (20), (30), (02), (12), (22), (32)\}$$

over $\mathbb{Z}/4$, then

$$\bar{C} = \{(00), (10)\}$$

over $\mathbb{F}_2$ and $d = \bar{d} = 1$. On the other hand, if C is the code

$$C = \{(000), (011), (022), (033), (200), (211), (222), (233)\}$$

over $\mathbb{Z}/4$, then

$$\bar{C} = \{(000), (011)\}$$

over $\mathbb{F}_2$ and $d = 1$ but $\bar{d} = 2$.

4. Curves over Rings

In this section, we collect some definitions and results on curves over rings which we will need in order to define algebraic geometric codes over rings. Most proofs are omitted. We suspect that many of these results are part of the "folklore", but complete proofs can be found in [17].

As before, A denotes a local Artinian ring with maximal ideal $\mathfrak{m}$. In this section, we will use k to denote the residue field $A/\mathfrak{m}$ of A. Let $Y = \operatorname{Spec} A$. Following [7], we will use the phrase "X is a curve over A" to mean that X is a connected irreducible projective scheme over Y which is smooth of relative dimension one. We write X' for the fiber of X over the unique maximal ideal of A. In other words, $X' = X \times_{\operatorname{Spec} A} \operatorname{Spec} k$. We will assume that X' is absolutely irreducible. Denote by ϕ the natural map $X' \to X$. For a line bundle $\mathcal{L}$ on X, write $\mathcal{L}' = \phi^*\mathcal{L}$. We denote by $\mathcal{K}$ the sheaf of total quotient rings on X, by $\mathcal{K}^*$ the sheaf of invertible elements in $\mathcal{K}$, and by $\mathcal{O}^*$ the sheaf of invertible elements of $\mathcal{O}_X$.

Lemma 4.1. *If X is a curve over A, then $\mathcal{K}$ is a constant sheaf.*

Proof. Since X has a unique generic point, it is enough to show that $\mathcal{K}$ is locally constant. We may assume $X = \operatorname{Spec} R$ with R having a unique minimal prime ideal. A basis for the topology on X consists of all sets $\operatorname{Spec} R_f$, where f is a non-nilpotent element of R. Since the map $A \to R$ is smooth, $f \in R$ is nilpotent if and only if it is a zero divisor. Thus $\mathcal{K}(X) = \mathcal{K}(\operatorname{Spec} R_f)$ for each basic open set $\operatorname{Spec} R_f$. □

Using this Lemma, the proof of ([8], Proposition II.6.15) is easily modified to give the following result.

Proposition 4.2. *Let X be a curve over A. Then* $\operatorname{CaCl}(X) \simeq \operatorname{Pic}(X)$.

Definition 4.3. Let X be a curve over A and Z a zero-dimensional closed subscheme of X. Let $i : Z \to X$ be inclusion and $f : X \to Y$ the structure morphism. We call Z an *A-point* of X if the composition $f \circ i$ is an isomorphism of schemes.

In the study of algebraic geometric codes over fields, one makes frequent use of the fact that closed points give Weil divisors. In order to study algebraic geometric codes over rings, we will need some sort of analog of this fact.

Lemma 4.4. *Let X be a curve over A and Z an A-point on X. Then there is a unique, well-defined Cartier divisor (which we will also denote by Z) associated to Z.*

Proof. By ([1],Exposé VII, Proposition 1.10), the inclusion $i : Z \to X$ is a regular closed immersion. Hence, the ideal for Z is locally principal. Let $\{U_i\}$ be an open cover of X on which the ideal for Z is locally principal; say f_i is the generator on U_i. Since f_i and f_j are non-zero-divisors which must generate the same ideal on $U_i \cap U_j$, we certainly have $f_i/f_j \in \Gamma(U_i \cap U_j, \mathcal{O}^*)$ Therefore, $\{(U_i, f_i)\}$ is a Cartier divisor. □

We can express the Cartier divisor for Z much more explicitly, using the fact that every A-point Z of X has a local parameter in a neighborhood of the unique closed point x contained in Z; see [7] or [17]. Let $U = \operatorname{Spec} B$ be an open affine neighborhood of x on which the ideal for Z is principal, and let $V = X \setminus \{x\}$. Let t be a local parameter for Z on U. We have that $B/t \simeq A$ and so t is a unit on $U \setminus \{x\} = U \cap V$. Hence, the Cartier divisor for Z can be expressed as $\{(U, t), (V, 1)\}$.

Remark 4.5. A smooth map is formally smooth ([5]), and so the map

$$\operatorname{Hom}_{\operatorname{Spec} A}(\operatorname{Spec} A, X) \to \operatorname{Hom}_{\operatorname{Spec} A}(\operatorname{Spec} k, X)$$

is surjective. But $\operatorname{Hom}_{\operatorname{Spec} A}(\operatorname{Spec} A, X)$ is in one-to-one correspondence with the A-points of X and $\operatorname{Hom}_{\operatorname{Spec} A}(\operatorname{Spec} k, X)$ is in one-to-one correspondence with the closed points of X which are k-rational points of X'. Hence, every closed point $x \in X$ which is a k-rational point of X' is contained in an A-point of X and thus has a local parameter on X.

We will need versions of both the Riemann-Roch Theorem and the Residue Theorem for curves over a local Artinian ring. We treat the Riemann-Roch Theorem first. The idea for the proof we give is due to Thomason ([12]).

Lemma 4.6. *For any open affine $U \subset X$, write $U' = U \cap X' = U \times_{\operatorname{Spec} A} \operatorname{Spec} k$. Then U' is an affine open subset of X' and we have*

$$\Gamma(U, \mathcal{L}) \otimes_A k = \Gamma(U', \mathcal{L}').$$

Proof. Write $U = \operatorname{Spec} B$. Then $U' = \operatorname{Spec}(B/\mathfrak{m}B)$. Further, since U is affine, $\mathcal{L}|_U = \tilde{M}$ for some B-module M, and $\Gamma(U, \mathcal{L}) \otimes_A k = M \otimes_A k = M/\mathfrak{m}M$. On the other hand, $\mathcal{L}'|_{U'} = (\mathcal{L}|_U)' = (M/(\mathfrak{m}B)M)\tilde{}$ and so $\Gamma(U', \mathcal{L}') = M/(\mathfrak{m}B)M$. Since $\mathfrak{m}M = (\mathfrak{m}B)M$, we have the result. □

Applying the functor $- \otimes k$ to the complex

$$\Gamma(U, \mathcal{L}) \oplus \Gamma(V, \mathcal{L}) \to \Gamma(U \cap V, \mathcal{L}), \tag{4.1}$$

we get the complex

$$\Gamma(U', \mathcal{L}') \oplus \Gamma(V', \mathcal{L}') \to \Gamma(U' \cap V', \mathcal{L}') \tag{4.2}$$

By the above Lemma, we can use this complex to compute the cohomology groups of $\mathcal{L}'$ on X'.

From our original complex 4.1, we get an exact sequence

$$0 \to \Gamma(X, \mathcal{L}) \to \Gamma(U, \mathcal{L}) \oplus \Gamma(V, \mathcal{L}) \to \Gamma(U \cap V, \mathcal{L}) \to H^1(X, \mathcal{L}) \to 0,$$

and applying the right-exact functor $- \otimes k$ gives

$$\Gamma(U', \mathcal{L}') \oplus \Gamma(V', \mathcal{L}') \to \Gamma(U' \cap V', \mathcal{L}') \to H^1(X, \mathcal{L}) \otimes k \to 0.$$

At the same time, the complex 4.2 yields an exact sequence

$$0 \to \Gamma(X', \mathcal{L}') \to \Gamma(U', \mathcal{L}') \oplus \Gamma(V', \mathcal{L}') \to \Gamma(U' \cap V', \mathcal{L}') \to H^1(X', \mathcal{L}') \to 0.$$

This means that $H^1(X, \mathcal{L}) \otimes k = H^1(X', \mathcal{L}')$. In particular, if $H^1(X', \mathcal{L}') = 0$, then since cohomology groups of coherent sheaves on projective schemes over Noetherian rings are always finitely generated ([8], Theorem III.5.2), we can apply Nakayama's lemma ([10]) to obtain $H^1(X, \mathcal{L}) = 0$.

From now on, assume $H^1(X', \mathcal{L}') = 0$. Then we have exact sequences

$$0 \to \Gamma(X, \mathcal{L}) \to \Gamma(U, \mathcal{L}) \oplus \Gamma(V, \mathcal{L}) \to \Gamma(U \cap V, \mathcal{L}) \to 0$$

and

$$0 \to \Gamma(X', \mathcal{L}') \to \Gamma(U', \mathcal{L}') \oplus \Gamma(V', \mathcal{L}') \to \Gamma(U' \cap V', \mathcal{L}') \to 0.$$

Applying $- \otimes k$ to the first of these two sequences gives

$$\operatorname{Tor}_1^A(\Gamma(U \cap V, \mathcal{L}), k) \to \Gamma(X, \mathcal{L}) \to \Gamma(U, \mathcal{L}) \oplus \Gamma(V, \mathcal{L}) \to \Gamma(U \cap V, \mathcal{L}) \to 0$$

since $- \otimes k$ is only right-exact. However, the fact that $\Gamma(U \cap V, \mathcal{L})$ is flat as an A-module means that $\operatorname{Tor}_1^A(\Gamma(U \cap V, \mathcal{L}), k) = 0$. Hence, we conclude that $\Gamma(X, \mathcal{L}) \otimes k = \Gamma(X', \mathcal{L}')$. Further, since $\Gamma(X, \mathcal{L})$ is the kernel of a surjective map of flat A-modules, it is itself flat as an A-module. Since a finitely generated flat module is projective and a projective module over the local ring A is free, $\Gamma(X, \mathcal{L})$ is a free A-module. Applying the standard Riemann-Roch Theorem [8], we have

Theorem 4.7. *Let X be a curve over A and $\mathcal{L}$ a line bundle on X. Let $X' = X \times_{\operatorname{Spec} A} \operatorname{Spec} k$ and $\mathcal{L}' = \phi^* \mathcal{L}$, where $\phi : X' \to X$ is the natural map. Define the degree of $\mathcal{L}$ to be $\deg \mathcal{L} = \deg \mathcal{L}'$ and the genus g of X to be the genus of X'. Assume that $\deg \mathcal{L} > 2g - 2$. Then $\Gamma(X, \mathcal{L})$ is a free A-module of rank $\deg \mathcal{L} + 1 - g$.*

Proof. The Riemann-Roch Theorem states that for any curve C of genus g over a field k and any line bundle $\mathcal{E}$ on C,

$$\dim H^0(C, \mathcal{E}) - \dim H^1(C, \mathcal{E}) = \deg \mathcal{E} + 1 - g.$$

In our case, $X' = C$ and $\mathcal{L}' = \mathcal{E}$. Since $\deg \mathcal{L}' = \deg \mathcal{L} > 2g - 2$ means that $\mathcal{L}'$ is a very ample sheaf, we have $H^1(X', \mathcal{L}') = 0$. Therefore,

$$\dim H^0(X', \mathcal{L}') = \deg \mathcal{L}' + 1 - g.$$

But $H^0(X', \mathcal{L}') = \Gamma(X', \mathcal{L}') = \Gamma(X, \mathcal{L}) \otimes_A k$, so the arguments above give the result. □

Our next task is the Residue Theorem. The version that we need is a special case of a very general theorem stated in [7]. Because it is far from obvious, we show how the version in [7] reduces to what we need. Consequently, the reference for the remainder of this section is [7].

As above, X is a curve over the local Artinian ring A, $Y = \operatorname{Spec} A$, $f : X \to Y$ is the structure morphism, and X' is the fiber of X over the unique maximal ideal of A. Notice that X' is a curve over $k = A/\mathfrak{m}$ and that the unique closed point contained in an A-point of X is a k-rational point of X'. In what follows, we will make the additional assumption that A is a Gorenstein ring; since A is local and Artinian, this is equivalent to saying that A is injective as a module over itself.

In fact, we need a consequence of the Gorenstein property. Recall that for A-modules $M \subseteq L$, L is an *essential extension* of M if $N \cap M \neq 0$ for every nonzero submodule N of L. Also, L is the *injective hull* of M if L is an essential extension of M and L is an injective module; in this case we write $L = E_A(M)$.

Lemma 4.8. ([3]) *Let A be any local Artinian Gorenstein ring, $\mathfrak{m}$ its maximal ideal, and k its residue field. Then $E_A(k) = A$.*

Proof. Since A is an Artinian ring, there is an integer s so that $\mathfrak{m}^{s-1} \neq 0$ and $\mathfrak{m}^s = 0$, where $\mathfrak{m}$ is the maximal ideal of A. Choose $a \in \mathfrak{m}^{s-1} \setminus \{0\}$, and consider the map $A \to A$ given by multiplication by a. Since the kernel of this map is $\mathfrak{m}$, we get an injection of A-modules $k \hookrightarrow A$. Since A is a Gorenstein ring, it is injective as an A-module and we need only show that this extension is essential. We will show the following, slightly stronger, statement: Let I and J be any two ideals of A. If $I \cap J = 0$, then either $I = 0$ or $J = 0$.

To do this, let I and J be as above, and consider the natural map

$$A \hookrightarrow A/I \oplus A/J.$$

Since A is injective, this map splits and the splitting maps either A/I or A/J onto A. Without loss of generality, A/I maps onto A. If $\bar{1} \in A/I$ is mapped to $u \in A$ under this map, then u is a unit and the composite map $A \to A$ is given by multiplication by u, and has I in its kernel. Since multiplication by a unit is an isomorphism, we must have $I = 0$. □

We now return to our treatment of the Residue Theorem.

Definition 4.9. (see [7], p.304) Let Y be a scheme, and for any $y \in Y$, let $J(y)$ be the quasi-coherent injective $\mathcal{O}_Y$-module which is the constant sheaf $I = E_{\mathcal{O}_{Y,y}}(k(y))$ on $\overline{\{y\}}$ and 0 elsewhere. A *residual complex* $K^{\cdot}$ on Y is a complex of quasi-coherent injective $\mathcal{O}_Y$-modules bounded below with coherent cohomology sheaves such that there is an isomorphism

$$\sum_{p \in \mathbb{Z}} K^p \simeq \sum_{y \in Y} J(y).$$

In our case, since $Y = \operatorname{Spec} A$, there is only one point $y \in Y$: the unique closed point corresponding to the maximal ideal of A. Further, since A is Gorenstein, $E_A(k) = A$, where k is the residue field of A. Hence the sheaf $\tilde{A} = \mathcal{O}_Y$, thought of as a complex concentrated in degree zero, is a residual complex on Y.

There is a functor $f^{\triangle}$ ([7], p.318) which maps the category of residual complexes on Y to the category of residual complexes on X. In order to write down $f^{\triangle}(\tilde{A})$, we need to set up some notation. Denote the generic point of X by η. Let $\omega = \omega_X$ be the canonical sheaf on X. For any sheaf $\mathcal{E}$ on X and any $x \in X$, we write $\mathcal{E}_x$ for the stalk of $\mathcal{E}$ at x. For example, if A is a field, then $\omega_\eta = \Omega(X)$, the vector space of rational differential forms on X. For $x \in X$, let $\psi_x : \operatorname{Spec} \mathcal{O}_{X,x} \to X$ be the inclusion and M an $\mathcal{O}_{X,x}$-module. Define $i_x(M)$ to be the sheaf $\psi_{x*}(\tilde{M})$. Finally, let $H^1_x(\omega_x)$ be the local cohomology group defined in ([7], section IV.1). Then by Proposition VII.1.1(d) of [7], $f^{\triangle}(\tilde{A})$ is the complex

$$i_\eta(\omega_\eta) \to \coprod_{\substack{x \in X \\ x \text{ closed}}} i_x(H^1_x(\omega_x)) \tag{4.3}$$

concentrated in degrees -1 and 0.

The following technical lemma allows us to better understand the above complex.

Lemma 4.10. *We have:*

1. $\Big(\coprod_{\substack{x \in X \\ x \text{ closed}}} i_x(H^1_x(\omega_x))\Big)_x = H^1_x(\omega_x)$
2. $H^1_x(\omega_x) = \omega_\eta/\omega_x$

Proof. Statement 1 is clear since by definition of local cohomology, $H^1_x(\omega_x)$ is supported only at x. By ([7], Prop VII.1.1(d)), complex 4.3 is an injective resolution of $f^*(\tilde{A}) \otimes \omega[1]$, so the two term complex fits in an exact sequence of sheaves

$$0 \to \omega \to i_\eta(\omega_\eta) \to \coprod_{\substack{x \in X \\ x \text{ closed}}} i_x(H^1_x(\omega_x)) \to 0.$$

Taking stalks at x gives an exact sequence

$$0 \to \omega_x \to \omega_\eta \to H^1_x(\omega_x) \to 0,$$

proving 2. □

Remark 4.11. In [7], statement (1) is implicitly assumed and (2) is proven only in the special case where $x \in X$ is a k-rational point of the closed fiber X' of X.

The Residue Theorem is stated in terms of the trace map ([7], VI.4), which in general is a map of graded sheaves (but not necessarily of complexes)

$$Tr_f : f_* f^{\triangle} K^{\cdot} \to K^{\cdot},$$

for a morphism $f : X \to Y$ and a residual complex $K^{\cdot}$ on Y.

In our case, noting that both terms of 4.3 are injective so that we can apply f_* degree-wise, the trace map yields a (not necessarily commutative) diagram of sheaves

$$\begin{array}{ccc} f_* i_\eta(\omega_\eta) & \longrightarrow & f_* \coprod_{\substack{x \in X \\ x \text{ closed}}} i_x(\omega_\eta/\omega_x) \\ \downarrow & & \downarrow \\ 0 & \longrightarrow & \tilde{A} \end{array} \tag{4.4}$$

with the vertical maps being Tr_f.

Notice that the sheaf

$$\coprod_{\substack{x \in X \\ x \text{ closed}}} i_x(\omega_\eta/\omega_x)$$

is given by

$$\Gamma(U, \coprod_{\substack{x \in X \\ x \text{ closed}}} i_x(\omega_\eta/\omega_x)) = \coprod_{\substack{x \in X \\ x \text{ closed}}} \Gamma(U, i_x(\omega_\eta/\omega_x))$$

for an open set U of X. In particular,

$$\Gamma(X, \coprod_{\substack{x \in X \\ x \text{ closed}}} i_x(\omega_\eta/\omega_x)) = \coprod_{\substack{x \in X \\ x \text{ closed}}} \Gamma(X, i_x(\omega_\eta/\omega_x))$$

and so

$$f_* \coprod_{\substack{x \in X \\ x \text{ closed}}} i_x(\omega_\eta/\omega_x) = \coprod_{\substack{x \in X \\ x \text{ closed}}} f_* i_x(\omega_\eta/\omega_x).$$

Further, since $f_* i_\eta(\omega_\eta) = \widetilde{\omega_\eta}$ and $f_* i_x(\omega_\eta/\omega_x) = \widetilde{\omega_\eta/\omega_x}$, for each closed $x \in X$, the diagram 4.4 induces maps of A-modules

$$\begin{array}{ccc} \omega_\eta & \longrightarrow & \omega_\eta/\omega_x \\ & & \downarrow \\ & & A \end{array}$$

We denote by Res_x the composition of these two maps, so that $Res_x : \omega_\eta \to A$ factors through ω_η/ω_x, and, for a rational differential form $\nu \in \omega_\eta$, we call $Res_x(\nu)$ the residue of ν at x. In particular, notice that if $x \in X$ is a closed point and $\nu \in \omega_\eta$ is a rational differential form which is regular at x, then the residue of ν at x is zero. For a point $x \in X$ which is a k-rational point of X', we can describe Res_x more precisely as follows (see [7], Proposition VII.1.3, for the rest of this paragraph). By Remark 4.5, there is a local parameter t for x. The ideal generated by the local parameter defines an A-point Z containing x. The map Res_x is described in terms of a local parameter, so we may think of it as defining the residue of ν at Z and we will sometimes write res_Z for the map Res_x when we wish to emphasize this. Choose $\nu \in \omega_\eta$, and consider the image $\bar{\nu} \in \omega_\eta/\omega_x$. In a neighborhood of Z, we can write down an expansion for $\bar{\nu}$

$$\bar{\nu} = \sum_{j<0} a_j t^j dt$$

with $a_j \in A$. Then $res_Z(\nu) = Res_x(\nu)$ is simply described as

$$res_Z(\nu) = a_{-1}.$$

Remark 4.12. In fact, Res_x is well-defined, independent of the choice of local parameter t. In particular, if Z' is some other A-point containing x, then for every $\nu \in \omega_\eta$,

$$res_Z(\nu) = res_{Z'}(\nu).$$

We are now ready to state the Residue Theorem.

Theorem 4.13. ([7], Theorem VII.2.1) *Let $f : X \to Y$ be a proper morphism of Noetherian schemes, and let $K^\cdot$ be a residual complex on Y. Then the trace map*

$$Tr_f : f_* f^\triangle K^\cdot \to K^\cdot$$

is a morphism of complexes.

Corollary 4.14. *Let A be a local, Artinian, Gorenstein ring, and let X be a curve over A. Then for any rational differential form ν on X,*

$$\sum_{\substack{x \in X \\ x \text{ closed}}} Res_x(\nu) = 0.$$

Proof. Theorem 4.13 simply states that the diagram 4.4 commutes. □

5. Algebraic Geometric Codes over Rings

Let A be a local Artinian ring with maximal ideal $\mathfrak{m}$. We assume that the field $A/\mathfrak{m}$ is finite; say $A/\mathfrak{m} = \mathbb{F}_q$. Let X be a curve over A, that is, a connected irreducible scheme over $\operatorname{Spec} A$ which is smooth of relative dimension one, as in Section 4. Let $X' = X \times_{\operatorname{Spec} A} \operatorname{Spec} \mathbb{F}_q$ be the fiber of X over $\mathfrak{m}$, so that we have a Cartesian square

$$\begin{array}{ccc} X' & \xrightarrow{\phi} & X \\ \downarrow & & \downarrow \\ \operatorname{Spec} \mathbb{F}_q & \longrightarrow & \operatorname{Spec} A \end{array}$$

We will always assume X' is absolutely irreducible, so that it is the type of curve on which algebraic geometric codes over $\mathbb{F}_q$ are defined. Let $\mathcal{L}$ be a line bundle on X and $\mathcal{Z} = \{Z_1, \ldots, Z_n\}$ a set of disjoint A-points on X. Then for each i, $\Gamma(Z_i, \mathcal{L}|_{Z_i}) \simeq A$, but noncanonically. Let $\gamma = \{\gamma_i\}$ be a system of these isomorphisms.

Definition 5.1. Let A, X, $\mathcal{Z}$, $\mathcal{L}$, and γ be as above. Define $C_A(X, \mathcal{Z}, \mathcal{L}, \gamma)$ to be the image of the composition α

$$\Gamma(X, \mathcal{L}) \longrightarrow \oplus \Gamma(Z_i, \mathcal{L}|_{Z_i}) \xrightarrow{\gamma} A^n.$$
$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}_{\alpha}$$

Then $C_A(X, \mathcal{Z}, \mathcal{L}, \gamma)$ is called an *algebraic geometric code over* A.

Remark 5.2. Tsfasman and Vlăduţ's "H"-construction ([13]) gives a generalization of algebraic geometric codes to allow higher dimensional algebraic varieties rather than just curves, but assumes that one is working over a field. Our definition is motivated by theirs, and in the case that our ring A is a field, both definitions are the same.

As the definition of algebraic geometric codes over rings is abstract, our first task is to relate it to classical algebraic geometric codes over finite fields. Recall that one way to construct such codes was to evaluate functions at rational points on the curve. Under certain conditions, we may think of these codes in the same way.

Definition 5.3. Let D be a Cartier divisor on X and $P \in X$ a closed point which is a rational point of X'. Then we say P is not in the support of D if there is a neighborhood U of P such that the local equation f for D on U is an element of $\mathcal{O}_X(U)^\times$.

Recall from Proposition 4.2 that $\operatorname{Pic}(X) \simeq \operatorname{CaCl}(X)$, so we can write $\mathcal{L} \simeq \mathcal{O}_X(D)$ for some Cartier divisor D. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be the set of closed points of X contained in the A-points $Z_1, \ldots, Z_n$ of $\mathcal{Z}$. Suppose we can choose D so that each $P_i \in \mathcal{P}$ is not in the support of D. Then evaluation provides a natural choice for γ, and hence for α.

To see this, assume $n = 1$ and write $\mathcal{Z} = \{Z\}$, $\mathcal{P} = \{P\}$. Choose $s \in \Gamma(X, \mathcal{L}) \subset \mathcal{K}(X)$ and some neighborhood U of P for which D is locally a unit f of $\mathcal{O}_X(U)$ on U. We may assume that U is affine, say $U = \operatorname{Spec} B$. Notice that Z is contained in every open set which contains P, so in particular, $Z \subset U$ and $Z = \operatorname{Spec}(B/J)$ for some ideal J of B such that $B/J \simeq A$. This means that the natural map

$\Gamma(X,\mathcal{L}) \to \Gamma(Z,\mathcal{L}|_Z)$ factors through $\Gamma(U,\mathcal{L})$. But $\Gamma(U,\mathcal{L}) = \frac{1}{f}\mathcal{O}_X(U) = \frac{1}{f}B$, so that $s|_U$ is of the form $\frac{h}{f}$ for some $h \in B \subset \mathcal{K}(X)$. Suppose $X \subset \mathbb{P}^r$ and Z is given in projective coordinates by $Z = (z_0 : \cdots : z_r)$. Since $z_0, \ldots, z_r$ generate the unit ideal of A and A is local, some z_i is a unit. Without loss of generality, we may assume that $z_0 = 1$ and that U is contained in the standard open affine subscheme of $\mathbb{P}^r$ defined by $z_0 = 1$. Then J is the ideal generated by $z_1 - x_1, \ldots, z_r - x_r$, where $x_1, \ldots, x_r$ are affine coordinates of U. The map $\Gamma(X,\mathcal{L}) \to \Gamma(Z,\mathcal{L}|_Z) \simeq A$ is given by

$$s \mapsto \frac{h}{f} \mapsto \frac{h(1, z_1, \ldots, z_r)}{f(1, z_1, \ldots, z_r)} \in A.$$

In other words, the map is the evaluation map.

We now proceed to explore the properties of algebraic geometric codes over rings. We begin by computing the parameters.

Theorem 5.4. *Let X, $\mathcal{L}$, $\mathcal{Z} = \{Z_1, \ldots, Z_n\}$ and γ be as above. Let g denote the genus of X, and suppose $2g - 2 < \deg \mathcal{L} < n$. Then $C = C_A(X, \mathcal{Z}, \mathcal{L}, \gamma)$ is a free code of length n and dimension $k = \deg \mathcal{L} + 1 - g$.*

Proof. By Theorem 4.7, it is enough to show that the map $\alpha : \Gamma(X,\mathcal{L}) \to A^n$ is an injection.

Suppose $s \in \Gamma(X,\mathcal{L})$ with $\alpha(s) = \mathbf{0}$. By Lemma 4.4, each Z_i may be considered as a Cartier divisor. Let D be any Cartier divisor such that $\mathcal{O}_X(D) \simeq \mathcal{L}$. By taking refinements if necessary, we may write $D = \{(U_j, g_j)\}$ and $Z_i = \{(U_j, g_{ij})\}$. Then the divisor $D - Z_1 - \cdots - Z_n$ may be written $\{(U_j, \frac{g_i}{g_{1j}\ldots g_{nj}})\}$. Our first step is to show that $s \in \Gamma(X, \mathcal{O}_X(D - Z_1 - \cdots - Z_n))$, i.e., that $s \in \frac{g_{1j}\ldots g_{nj}}{g_j}\mathcal{O}_X(U_j)$ for each j.

The fact that $s \in \Gamma(X,\mathcal{L})$ means that $s \in \frac{1}{g_j}\mathcal{O}_X(U_j)$ for each j, and so $g_j s \in \mathcal{O}_X(U_j)$ for each j. Further, since the ith coordinate of $\alpha(s)$ is 0 for $i = 1, \ldots, n$, we have that $g_j s$ is an element of the ideal $(g_{ij})\mathcal{O}_X(U_j) \subset \mathcal{O}_X(U_j)$ for each i and j. Since the Z_i are disjoint, we have for each j

$$\bigcap_i g_{ij}\mathcal{O}_X(U_j) = g_{1j}\ldots g_{nj}\mathcal{O}_X(U_j).$$

Hence $\ker(\alpha) = \Gamma(X, \mathcal{O}_X(D - Z_1 - \cdots - Z_n))$, and our next step is to show that this is zero.

Consider the line bundle $\phi^*\mathcal{O}_X(D - Z_1 - \cdots - Z_n)$ on X', where $\phi : X' \to X$ is as in Definition 5.1. We have $\deg \phi^*\mathcal{O}_X(D - Z_1 - \cdots - Z_n) = \deg(D - Z_1 - \cdots - Z_n) < 0$, so $\Gamma(X', \phi^*\mathcal{O}_X(D - Z_1 - \cdots - Z_n)) = 0$. By ([8], Theorem III.12.11), if $\mathcal{E}$ is any line bundle, the map

$$\Gamma(X,\mathcal{E}) \otimes \mathbb{F}_q \to \Gamma(X', \phi^*\mathcal{E})$$

is an isomorphism if it is onto. Hence $\Gamma(X, \mathcal{O}_X(D - Z_1 - \cdots - Z_n)) \otimes \mathbb{F}_q = 0$. Applying Nakayama's lemma gives the result.

□

Before computing the minimum distance, we explore the behavior of our codes under linear projection. The minimum distance estimate will be a direct corollary of the following theorem.

Theorem 5.5. *Let X, $\mathcal{L}$ and $\mathcal{Z}$ be as above. Let $\mathcal{P} = \{P_1, \ldots, P_n\} \subset X'(\mathbb{F}_q)$ be the set of closed points contained in $Z_1, \ldots Z_n$. Let $\gamma = \{\gamma_i\}$ be a system of isomorphisms*

$$\gamma_i : \Gamma(Z_i, \mathcal{L}|_{Z_i}) \to A.$$

Let $\gamma' = \{\gamma_i'\}$ be the induced system of isomorphisms

$$\gamma_i' : \Gamma(P_i, \mathcal{L}'|_{P_i}) = \Gamma(Z_i, \mathcal{L}|_{Z_i}) \otimes_A \mathbb{F}_q \to \mathbb{F}_q.$$

Consider the codes $C = C_A(X, \mathcal{Z}, \mathcal{L}, \gamma)$, $C' = C_{\mathbb{F}_q}(X', \mathcal{P}, \mathcal{L}', \gamma')$ and $\bar{C} = \pi(C)$, where $\pi : A^n \to \mathbb{F}_q^n$ denotes coordinatewise projection. Then

$$\bar{C} = C'.$$

Proof. From Theorem 4.7 and its proof, we know that $\Gamma(X, \mathcal{L}) \otimes_A \mathbb{F}_q \simeq \Gamma(X', \mathcal{L}')$ and that this isomorphism is simply the "mod $\mathfrak{m}$" map. Hence, the following diagram commutes:

$$\begin{array}{ccccc}
\Gamma(X, \mathcal{L}) & \longrightarrow & \Gamma(X, \mathcal{L}) \otimes_A \mathbb{F}_q & \xrightarrow{\sim} & \Gamma(X', \mathcal{L}') \\
\downarrow & & & & \downarrow \\
\oplus\Gamma(Z_i, \mathcal{L}|_{Z_i}) & & & & \oplus\Gamma(P_i, \mathcal{L}'|_{P_i}) \\
\downarrow{\scriptstyle \gamma} & & & & \downarrow{\scriptstyle \gamma'} \\
A^n & & \xrightarrow{\quad\pi\quad} & & \mathbb{F}_q^n
\end{array}$$

The image of the clockwise composition $\Gamma(X, \mathcal{L}) \to \mathbb{F}_q^n$ is C', and the image of the counterclockwise composition is $\bar{C}$. □

Remark 5.6. Essentially, we have shown that $C' = C \otimes_A \mathbb{F}_q$ and applied Lemma 3.2.

Corollary 5.7. *Let $X, \mathcal{Z}, \mathcal{L}, \gamma$ be as in Theorem 5.5. Then the minimum Hamming distance d of the algebraic geometric code $C = C_A(X, \mathcal{Z}, \mathcal{L}, \gamma)$ satisfies*

$$d \geq n - \deg \mathcal{L}.$$

Proof. By Theorem 5.4, C is a free code. Theorem 5.5 and Proposition 3.4 give the result.

□

Our next goal is to show that the class of algebraic geometric codes is closed under duals. In particular, for a given A, X, $\mathcal{Z}$, $\mathcal{L}$, and γ, there is some other line bundle $\mathcal{F}$ on X and a system of isomorphisms $\xi = \{\xi_i : \Gamma(Z_i, \mathcal{F}|_{Z_i}) \to A\}$ such that

$$C_A(X, \mathcal{L}, \mathcal{Z}, \gamma)^\perp = C_A(X, \mathcal{F}, \mathcal{Z}, \xi).$$

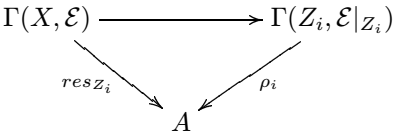
Because we will be using the Residue Theorem to do this, from now on we will make the additional assumption that A is a Gorenstein ring. Our proof is inspired by the proof of Theorem 3.1.44 in [13].

Lemma 5.8. *Let $\mathcal{L}$ be any line bundle on X. As usual, let $\omega = \omega_{X/A}$ denote the canonical line bundle on X, ω_η its stalk at the generic point, and $i_\eta(\omega_\eta) = \psi_{\eta *}(\tilde{\omega}_\eta)$, where $\psi_\eta : \operatorname{Spec} \mathcal{O}_{X,\eta} \to X$ is inclusion. Then $\omega \otimes_{\mathcal{O}_X} \mathcal{L}$ is isomorphic to a subsheaf of $i_\eta(\omega_\eta)$.*

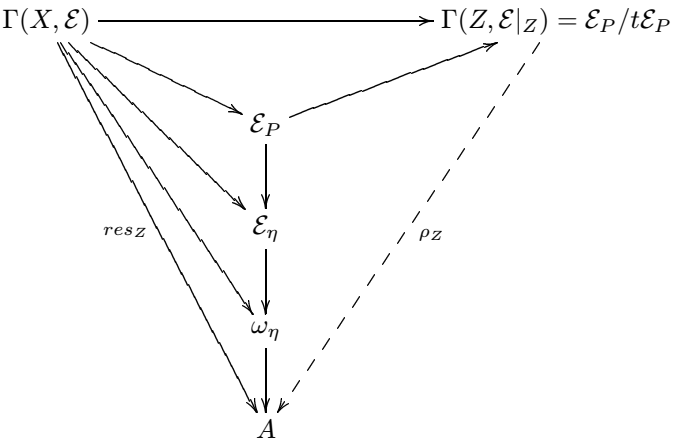
Proof. We know that ω is a subsheaf of $i_\eta(\omega_\eta)$. Since $\mathcal{L}$ is a line bundle, it is locally free and hence a flat $\mathcal{O}_X$-module, so that $-\otimes_{\mathcal{O}_X}\mathcal{L}$ is exact. Hence $\omega\otimes_{\mathcal{O}_X}\mathcal{L}$ is a subsheaf of $i_\eta(\omega_\eta)\otimes_{\mathcal{O}_X}\mathcal{L}$. Further, let U be any open subset of X such that $\mathcal{L}\simeq\mathcal{O}_X$ on U. Then $\Gamma(U, i_\eta(\omega_\eta)\otimes\mathcal{L})\simeq\Gamma(U, i_\eta(\omega_\eta))=\omega_\eta$. Since a locally constant sheaf is constant, we have $i_\eta(\omega_\eta)\otimes_{\mathcal{O}_X}\mathcal{L}\simeq i_\eta(\omega_\eta)$. □

Consider the line bundle $\mathcal{E}=\omega\otimes\mathcal{O}_X(\mathcal{Z})$, where $\mathcal{Z}$ denotes the Cartier divisor obtained by adding up the Cartier divisors $Z_1,\ldots,Z_n$. Since $\mathcal{E}$ is a subsheaf of $i_\eta(\omega_\eta)$ by the above Lemma, $\Gamma(X,\mathcal{E})\subset\omega_\eta$, and for each i, the residue map of Section 2 defines a map $res_{Z_i}:\Gamma(X,\mathcal{E})\to A$.

Lemma 5.9. *For each i, the map res_{Z_i} factors through $\Gamma(Z_i,\mathcal{E}|_{Z_i})$. In particular, there is an isomorphism $\rho_i:\Gamma(Z_i,\mathcal{E}|_{Z_i})\to A$ which makes the following diagram commute:*



Proof. Notice that $\mathcal{O}_X(\mathcal{Z})_{P_i}=\mathcal{O}_X(Z_i)_{P_i}$, so we may assume $n=1$ and write $\mathcal{Z}=\{Z\}$, $\mathcal{P}=\{P\}$. Let t be a local parameter for Z, that is, a local parameter for P which defines Z. The following diagram is given for reference in reading the rest of the proof.



Since any open set U containing P also contains Z, the map $\Gamma(X,\mathcal{E})\to\Gamma(Z,\mathcal{E}|_Z)$ factors through $\Gamma(\mathrm{Spec}(\mathcal{O}_{X,P}),\mathcal{E}|_{\mathrm{Spec}(\mathcal{O}_{X,P})})=\mathcal{E}_P$. Further, the map $\Gamma(X,\mathcal{E})\to\mathcal{E}_\eta$ also factors through $\mathcal{E}_P$ since $\eta\in\mathrm{Spec}(\mathcal{O}_{X,P})$. Since $\omega_\eta=\Gamma(X,i_\eta(\omega_\eta))=(i_\eta(\omega_\eta))_\eta$, the injection $\Gamma(X,\mathcal{E})\hookrightarrow\omega_\eta$ factors through $\mathcal{E}_\eta$. Thus, the residue map $res_Z:\Gamma(X,\mathcal{E})\to A$ factors through $\mathcal{E}_P$.

By definition of t, $\Gamma(Z,\mathcal{E}|_Z)=\mathcal{E}_P\otimes_{\mathcal{O}_{X,P}}\mathcal{O}_{X,P}/t=\mathcal{E}_P/t\mathcal{E}_P$. If we can show that $t\mathcal{E}_P$ is in the kernel of the residue map res_Z, we know that the residue map factors through $\Gamma(Z,\mathcal{E}|_Z)$.

We have that $\mathcal{E}_P=(\omega\otimes\mathcal{O}_X(Z))_P=\omega_P\otimes\mathcal{O}_X(Z)_P$. This means that $\mathcal{E}_P$ is generated by elements of the form $\nu\otimes f$ for some $\nu\in\omega_P$ and $f\in\mathcal{O}(Z)_P$. But f is of the form s/t, where $s\in\mathcal{O}_{X,P}$, so $t\mathcal{E}_P$ is generated by elements of the form

$\nu \otimes s$ with $\nu \in \omega_P$ and $s \in \mathcal{O}_{X,P}$. Hence, $t\mathcal{E}_P \subset \omega_P$, and by the explicit description of residues at rational points given in Section 4, the residue at Z of any element of $t\mathcal{E}_P$ is zero.

Finally, we must show that the residue map $res_Z : \mathcal{E}_P \to A$ is onto. To do this, it is certainly enough to show that the form $\frac{1}{t}\,dt$ is in $\mathcal{E}_P$, since by the explicit description, the residue at Z of this form is 1. Clearly $\frac{1}{t} \in \mathcal{O}_X(Z)_P$ and $dt \in \omega_P$. Since $\mathcal{E}_P = \omega_P \otimes \mathcal{O}_X(Z)_P$, the result follows. □

We now prove our Duality Theorem.

Theorem 5.10. *Let A be a local Artinian Gorenstein ring with finite residue field and let X be a curve over A. Let $\mathcal{Z} = \{Z_1, \ldots, Z_n\}$ be a set of disjoint A-points on X. Let $\mathcal{L}$ be any line bundle on X and let $\gamma = \{\gamma_i : \Gamma(Z_i, \mathcal{L}|_{Z_i}) \to A\}$ be any system of isomorphisms. Notice that for any $s_i \in \Gamma(Z_i, \mathcal{L}|_{Z_i})$ and any $\nu_i \in \Gamma(Z_i, (\omega \otimes \mathcal{O}_X(\mathcal{Z}) \otimes \mathcal{L}^{-1})|_{Z_i})$, we have $s_i\nu_i \in \Gamma(Z_i, (\omega \otimes \mathcal{O}_X(\mathcal{Z}))|_{Z_i})$. Define an isomorphism*

$$\xi_i : \Gamma(Z_i, \omega \otimes \mathcal{O}_X(\mathcal{Z}) \otimes \mathcal{L}^{-1}) \to A$$

by the rule

$$\xi_i(\nu_i) = \rho_i(\gamma_i^{-1}(1)\nu_i),$$

where ρ is the system of isomorphisms from Lemma 5.9. Then

$$C_A(X, \mathcal{Z}, \mathcal{L}, \gamma)^{\perp} = C_A(X, \mathcal{Z}, \omega \otimes \mathcal{O}_X(\mathcal{Z}) \otimes \mathcal{L}^{-1}, \xi).$$

Proof. Let $s \in \Gamma(X, \mathcal{L})$ have image $s_i \in \Gamma(Z_i, \mathcal{L}|_{Z_i})$ and $\nu \in \Gamma(X, \omega \otimes \mathcal{O}_X(\mathcal{Z}) \otimes \mathcal{L}^{-1})$ have image $\nu_i \in \Gamma(X, (\omega \otimes \mathcal{O}_X(\mathcal{Z}) \otimes \mathcal{L}^{-1})|_{Z_i})$. Then we must show

$$\sum_{i=1}^{n} \gamma_i(s_i)\xi_i(\nu_i) = 0.$$

By the definition of ξ_i and the fact that ρ_i, γ_i, and γ_i^{-1} are isomorphisms of A-modules, we have

$$\begin{aligned}
\sum_{i=1}^{n} \gamma_i(s_i)\xi_i(\nu_i) &= \sum_{i=1}^{n} \gamma_i(s_i)\rho_i(\gamma_i^{-1}(1)\nu_i) \\
&= \sum_{i=1}^{n} \rho_i(\gamma_i(s_i)\gamma_i^{-1}(1)\nu_i) \\
&= \sum_{i=1}^{n} \rho_i(\gamma_i^{-1}(\gamma_i(s_i) \times 1)\nu_i) \\
&= \sum_{i=1}^{n} \rho_i(s_i\nu_i) \\
&= \sum_{i=1}^{n} res_{Z_i}(s\nu) \\
&= \sum_{i=1}^{n} Res_{P_i}(s\nu).
\end{aligned}$$

We now claim that the only closed points $P \in X$ for which $Res_P(s\nu) \neq 0$ are $P_1, \ldots, P_n$. To see this, let $U = X \backslash \mathcal{P}$ and for each i, let V_i be an open neighborhood of P_i not containing P_j for $i \neq j$. We may use the open cover $X = U \cup V_1 \cup \cdots \cup V_n$

to express the Cartier divisor for each Z_i. The local equation for Z_i on U is always 1, and the local equation on V_j is 1 if $i \neq j$ and the local parameter t_i if $i = j$. The Cartier divisor $\mathcal{Z}$ can then be represented as $\{(U, 1), (V_1, t_1), \ldots, (V_n, t_n)\}$. Choose any closed $P \in X$ which is not in $\mathcal{P}$. Then $P \in U$, so $s\nu|_U \in \Gamma(U, \omega)$ and thus has nonzero residue at P, proving our claim.

Hence,

$$\begin{aligned}\sum_{i=1}^{n} \gamma_i(s_i)\xi_i(\nu_i) &= \sum_{i=1}^{n} Res_{P_i}(s\nu) \\ &= \sum_{\substack{x \in X \\ x \text{ closed}}} Res_x(s\nu) \\ &= 0\end{aligned}$$

by the Residue Theorem. □

6. Concluding Remarks

In the Introduction, we mention that one motivation for this work was the paper [6], which showed that certain famous nonlinear binary codes were in fact nonlinear projections of linear $\mathbb{Z}/4$-codes. It is now natural to ask whether these linear $\mathbb{Z}/4$-codes can be constructed as algebraic geometric codes. In [18], we prove

Theorem 6.1. *The Nordstrom-Robinson code is the image under the Gray map of an algebraic geometric code over* $\mathbb{Z}/4$.

The proof of this theorem is very explicit. In fact, we are able to give equations for a curve X over $\mathbb{Z}/4$, coordinates for a set of $\mathbb{Z}/4$-points $\mathcal{Z}$ on X, and a minimal generating set for the free module of global sections of a line bundle $\mathcal{L}$ on X, so that the Nordstrom-Robinson code is the image of the code $C_{\mathbb{Z}/4}(X, \mathcal{Z}, \mathcal{L}, \gamma)$, where γ is the evaluation map as described in section 5 above.

We also prove that none of the other Kerdock and Preparata codes can be constructed as images of algebraic geometric codes over $\mathbb{Z}/4$. It remains possible, however, that these codes could be constructed as images of trace codes of algebraic geometric codes over Galois rings. To answer this question, one needs to study the "Lee weight" of linear codes over $\mathbb{Z}/4$ which are trace codes of algebraic geometric codes over Galois rings. This amounts to finding a bound on the absolute value of a certain exponential sum; see [17] for details. In [16], we find a bound on this sum in the case where X' is an ordinary elliptic curve and X is its Serre-Tate canonical lift.

References

[1] P. Berthelot, A. Grothendieck, and L. Illusie. *Séminaire de Géométrie Algébrique du Bois Marie 1966/67 (SGA6)*. Springer-Verlag, Berlin, 1971.

[2] A. R. Calderbank, G. McGuire, P. V. Kumar, and T. Helleseth. Cyclic codes over $\mathbb{Z}_4$, locator polynomials and Newton's identities. *IEEE Transactions on Information Theory*, 42:217–226, 1996.

[3] S. Dutta. Local cohomology: Lecture notes from a course given at the University of Illinois, Urbana-Champaign, 1996.

[4] V. D. Goppa. Codes associated with divisors. *Probl. Peredachi Inf.*, 13:33–39, 1977. English translation in *Probl. Inf. Transm.,* 13:22-27, 1977.

[5] A. Grothendieck. *Éléments de Géométrie Algébrique IV: Étude Locale des Schémas et des Morphismes de Schémas*, volume 20, 24, 28 and 32 of *Publications Mathématiques*. I. H. E. S., 1967.
[6] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Transactions on Information Theory*, 40:301–319, 1994.
[7] R. Hartshorne. *Residues and Duality*. Springer-Verlag, Berlin, 1966.
[8] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, New York, 1977.
[9] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1993.
[10] H. Matsumura. *Commutative Ring Theory*. Cambridge University Press, Cambridge, 1990.
[11] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer-Verlag, Berlin, 1993.
[12] R. W. Thomason. Private communication, 1994.
[13] M. A. Tsfasman and S. G. Vlăduţ. *Algebraic-Geometric Codes*. Kluwer Academic Publishers, Dordrecht, 1991.
[14] M. A. Tsfasman, S. G. Vlăduţ, and Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than the Varshamov-Gilbert bound. *Math. Nachrichten*, 109:21–28, 1982.
[15] J. H. van Lint and G. van der Geer. *Introduction to Coding Theory and Algebraic Geometry*. Birkhäuser, Basel, 1988.
[16] J.-F. Voloch and J. L. Walker. Euclidean weights of codes from elliptic curves over rings. Preprint, 1997.
[17] J. L. Walker. *Algebraic Geometric Codes over Rings*. PhD thesis, University of Illinois, 1996.
[18] J. L. Walker. The Nordstrom Robinson code is algebraic geometric. *IEEE Transactions on Information Theory*, 43:1588–1593, 1997.

Department of Mathematics and Statistics, University of Nebraska, Lincoln, NE 68588-0323

E-mail address: jwalker@math.unl.edu