ERROR-CORRECTING CODES AND ALGEBRAIC FUNCTION FIELDS

JACOB PARISH

Abstract. Error-correcting codes enable one to reliably send data across unreliable communication channels. In this paper, we first give a general introduction to the theory of such codes. We then introduce alebraic function fields, a language which allows us to do algebraic geometry over nonclosed fields; we define places, divisors, and differentials, and we state the Riemann-Roch theorem. Algebraic function fields are applied to construct a large class of codes, the so-called algebraic geometry codes. Finally, as an example of algebraic geometry codes, we look at codes arising from Hermitian function fields and investigate their parameters.

Contents

1. Introduction

Suppose one wants to transmit a message to someone else over an unreliable communication channel. Due to the channel's unreliability, the other party may not receive the correct message. In the best case, the receiver might realize there is an error when the message does not make sense, and ask for it to be retransmitted. This is clearly inefficient, especially in situations where there is high latency. In the worst case, the receiver might misunderstand the transmitter, and take some unintended action.

Error correcting codes are motivated by precisely this problem. By adding some redundancy to the transmitted message, the transmitter can enable the receiver to

Date: August 28, 2021.

recover the original message, even in the presence of errors. To demonstrate how we might do this, we consider the following example. The receiver and transmitter must first agree on some alphabet; we will use the binary alphabet $\{0,1\}$, which is often the alphabet one wants to use in practice. A trivial first example of error-correcting codes are the repetition codes. If the receiver wants to transmit a binary string in $\{0,1\}^k$, they may repeat it m times, for some agreed-upon number m. They thus transmit to the receiver a string in $\{0,1\}^{km}$. To recover the ith symbol of the original message, the receiver may inspect the i-th position in each of the m received copies, and decode according to the majority. Of course ties are possible; in that case, the receiver might ask for a retransmission, or we could require that m be odd. The receiver will successfully recover the original message whenever, for each symbol in the original message, the number of errors in each transmitted copy is at most $\lfloor \frac{m-1}{2} \rfloor$. A protocol of this sort, where the transmitter encodes messages of length k into messages of length n for some $n \geq k$ is known as a *block code*. In practice, a transmitter breaks up a large message they wish to send into *blocks* of length k, encodes each block into a *codeword* of length n, and transmits these codewords in sequence.

We should also clarify that we restrict our attention to channels where the only possible errors are those where some symbol is confused with another; that is, we do not consider the possibility that a symbol is deleted, or that extra symbols are somehow inserted.

2. The Theory of Codes

2.1. **Linear Codes and their Parameters.** While a receiver and transmitter could use any alphabet, allowing arbitrary alphabets generally provides too little structure for us to work with. As such, we choose our alphabet to be the finite field of order q where q is some prime power, which we denote by $\mathbb{F}_q$. Moreover, we will deal exclusively with linear codes, which are defined as follows.

Definition 2.1. A *linear* $[n,k]_q$ *code* is a linear subspace $C \subseteq \mathbb{F}_q^n$ of dimension k. The number n is called the *length* of the code, and k is called its *dimension*.

Since we are restricting our attention to linear codes, we often omit the word "linear". To a code C, we can associate a (non-unique) $k \times n$ matrix whose rows are a basis in C. This matrix is often denoted by G, and is called a *generator matrix* for the code C. Note that this matrix is the matrix corresponding to an injective linear map from $\mathbb{F}_q^k$ to $\mathbb{F}_q^n$, whose image is C. This makes the encoding process particularly easy for linear codes. To encode a vector $x \in \mathbb{F}_q^k$, a transmitter need only compute the product xG.

Definition 2.2. Given an $[n,k]_q$ code C, the *dual code* $C^\perp$ is the $[n, n-k]_q$ code given by the orthogonal complement of C, with respect to the standard inner product $\langle x, y \rangle := \sum_{i=1}^n x_i y_i$.

If H is a generator matrix for the dual code $C^\perp$, then one can see that $Hy^T = 0$ if and only if $y \in C$. For this reason, H is called a *parity-check matrix* for the code C, and this matrix plays an important role in the decoding of linear codes. We will not say any more about duals here, but we will revisit them in our constructions of algebraic geometry codes in Section 4.

Now, we would like to be able to quantify the error-correcting capacity of a linear code. To that end, we introduce the following definitions.

Definition 2.3. The *Hamming distance* between two vectors $x, y \in \mathbb{F}_q^n$, denoted by $d(x, y)$, is the number of coordinate positions where x and y differ. That is, $d(x, y) = \big|\{i : x_i \neq y_i\}\big|$.

Definition 2.4. Let C be an $[n, k]_q$ code. The *minimum distance* of C, denoted by d, is

$$d := \min_{x,y \in C, x \neq y} d(x, y)$$

If C is an $[n, k]_q$ code of minimum distance d, we sometimes refer to C as an $[n, k, d]_q$ code when we wish to specify d. Notice that in a practical sense, d tells us how many errors the code C can correct. In particular, suppose that $d \geq 2t + 1$. If a receiver receives a message $y \in \mathbb{F}_q^n$, then they are able to recover the original message whenever the number of errors is at most t, as there is a unique vector $x \in C$ for which $d(x, y) \leq t$. Thus, an $[n, k, d]_q$ code can correct any $\lfloor \frac{d-1}{2} \rfloor$ errors.

Since C is a linear subspace, there is a simpler way of understanding the minimum distance. We first introduce the following definition.

Definition 2.5. The *Hamming weight* of a vector $x \in \mathbb{F}_q^n$, denoted by $\|x\|$, is the number of nonzero coordinates of x, that is, $\|x\| = \big|\{i : x_i \neq 0\}\big|$.

One can then observe that the minimum distance of C is equivalently given by the following formula.

$$d = \min_{x \in C, x \neq 0} \|x\|$$

We would like for d to be as large as we can make it, as a fraction of the length n. Of course, to increase our error-correcting capacity, we must add more redundancy to our data; that is, we must make k smaller (again, as a fraction of n). This tradeoff between k and d is made more precise by the following bound.

Proposition 2.6 (Singleton bound)**.** *For any $[n, k, d]_q$ code, we have the inequality*

$$k \leq n - d + 1$$

Proof. Let $C' = \{(x_1, \ldots, x_{n-d+1}) : (x_1, \ldots, x_n) \in C\} \subset \mathbb{F}_q^{n-d+1}$ be the subspace formed by removing the last $d-1$ coordinates of each vector in C. By the definition of the minimum distance, it is impossible for two distinct codewords in C to have the same image in C', or else they would be at a distance at most $d - 1$ from each other. Therefore we must have $|C| = \big|C'\big|$, and it follows that C' is a k-dimensional subspace of $\mathbb{F}_q^{n-d+1}$. This implies $k \leq n - d + 1$, as desired. □

Note that this bound is independent of q. When q is taken into account, one can often obtain better bounds, and so the Singleton bound is rather crude. Nonetheless, it is an important bound, and codes which attain the Singleton bound (i.e. for which $k = n - d + 1$) are of particular importance. They are called maximum distance separable (or MDS) codes, as they have the maximum possible minimum distance for a fixed length and dimension. We now turn to our first example of a non-trivial code, which turns out to be maximum distance separable.

Example 2.7 (Reed-Solomon Codes)**.** Let $\mathcal{P} = \{P_1, \ldots, P_n\} \subset \mathbb{F}_q$. For some $a < n$, let $L(a)$ be the space of polynomials in one variable over $\mathbb{F}_q$ of degree at most a. Consider the map $\mathrm{Ev}_{\mathcal{P}} : L(a) \to \mathbb{F}_q^n$ given by

$$\mathrm{Ev}_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n))$$

Then the image of $\mathrm{Ev}_{\mathcal{P}}$ defines some code of length n. Since we have chosen $a < n$, any nonzero polynomial $f \in L(a)$ may vanish at most at a points of $\mathcal{P}$, and thus $\mathrm{Ev}_{\mathcal{P}}(f)$ must have at least $n-a$ nonzero coordinates. It follows that $d = n-a$, and that the map is injective, so that $k = \dim L(a) = a+1$. Thus we have constructed an $[n, a+1, n-a]_q$ code. A generator matrix for this code is given by

$$G = \begin{pmatrix} 1 & \dots & 1 \\ P_1 & \dots & P_n \\ P_1^2 & \dots & P_n^2 \\ \vdots & \ddots & \vdots \\ P_1^a & \dots & P_n^a \end{pmatrix}$$

Codes of this form are known as *Reed-Solomon codes*. Observe that the parameters $[n, a+1, n-a]$ meet the Singleton bound, and hence Reed-Solomon codes are MDS codes.

2.2. **Projective Systems.** Here, we present another way to understand linear codes, which has the benefit of being much less coordinate-centric. These are the so-called *projective systems*, which are covered in more detail in [1, section 1.1]. We first introduce two more important concepts regarding codes.

We say two $[n, k]_q$ codes C and C' are *equivalent* if we can obtain one from the other by re-ordering coordinates, or multiplying single coordinates by nonzero scalars. More specifically, let $\mathcal{A}_n$ be the group of automorphisms of $\mathbb{F}_q^n$ generated by (1) automorphisms which permutate the coordinates and (2) automorphisms which multiply the coordinate x_i by a nonzero scalar $a_i \in \mathbb{F}_q^*$. Then C and C' are equivalent if $A(C) = C'$ for some $A \in \mathcal{A}_n$. One can observe that equivalence of linear codes preserves the minimum distance d. It is common to only want to work with codes up to equivalence.

We say that an $[n, k]_q$ code C is *nondegenerate* if for each $i = 1, \dots, n$, there exists some $x \in C$ such that $x_i \neq 0$. That is, C is not entirely contained in some coordinate hyperplane. In practice, of course, one would always want to use a nondegenerate code, as a degenerate code "wastes" one or more coordinate positions, since they are always set to 0.

Now we are ready to introduce projective systems, and to show their relationship with linear codes. Throughout, we will denote the projective space of dimension k over $\mathbb{F}_q$ by $\mathbb{P}^k(\mathbb{F}_q) = \mathbb{P}^k$.

Definition 2.8. A *projective* $[n, k]_q$ *system* is a multiset $\mathcal{P} \subset \mathbb{P}^{k-1}$ of size n which is not contained in any projective hyperplane. The parameter d for a projective system is defined as follows.

$$d := n - \max\{|\mathcal{P} \cap H| : H \text{ is a projective hyperplane in } \mathbb{P}^{k-1}\}$$

As with codes, we refer to $\mathcal{P}$ as a projective $[n, k, d]_q$ system when we wish to specify d. Two projective systems $\mathcal{P}$ and $\mathcal{Q}$ are said to be *equivalent* if there is an automorphism of $\mathbb{P}^{k-1}$ which maps $\mathcal{P}$ to $\mathcal{Q}$, and this equivalence certainly preserves the value of d.

Theorem 2.9. *Equivalence classes of nondegenerate $[n, k, d]_q$ codes are in one-to-one correspondence with equivalence classes of $[n, k, d]_q$ projective systems.*

Proof. Let C be an $[n,k,d]_q$ code. Let $x_1,\dots,x_n$ be the coordinate functions on $\mathbb{F}_q^n$. Since C is nondegenerate, the restrictions $x_i\mid_C$ are all nonzero elements of the dual space C^*. We thus obtain n corresponding points $\mathcal{P}=\{P_1,\dots,P_n\}$ in the projective space $\mathbb{P}(C^*)\cong\mathbb{P}^{k-1}$. Notice that a nonzero codeword $x\in C$ determines a hyperplane $H(x)\subset\mathbb{P}(C^*)$ consisting of the functionals which vanish on x. The weight of a codeword is given by the number of coordinate functions which do not vanish on x, that is, the number of elements P_i which are not in the hyperplane $H(x)$, so we have

$$\|x\| = \big|\{P_i : P_i\notin H(x)\}\big| = n-\big|\{\mathcal{P}\cap H(x)\}\big| \tag{2.10}$$

If the points P_i were all in the same hyperplane, then the nonzero codeword determined by this hyperplane would have weight 0, which is impossible. Thus $\mathcal{P}$ is a projective $[n,k]_q$ system. Moreover, (2.10) implies the correspondence between the minimum distances, i.e. $\mathcal{P}$ is a projective $[n,k,d]_q$ system.

Now let C' be an $[n,k,d]_q$ code which is equivalent to C, and let $\mathcal{Q}=\{Q_1,\dots,Q_n\}$ be the projective $[n,k,d]_q$ system obtained from C' in the same way as for C. Let $A\in\mathcal{A}_n$ be an automorphism of $\mathbb{F}_q^n$ such that $C=A(C')$, and consider the dual map A^*. There is some permutation $\sigma\in S_n$ and nonzero scalars $a_i\in\mathbb{F}_q$ such that for coordinate functions x_i, we have $A^*(x_i)=a_ix_{\sigma(i)}$. The restriction $A^*:C^*\to C'^*$ induces a map $\widetilde{A^*}:\mathbb{P}^{k-1}(C^*)\to\mathbb{P}^{k-1}(C'^*)$ with $\widetilde{A^*}(P_i)=Q_{\sigma(i)}$. Thus we have $\widetilde{A^*}(\mathcal{P})=\mathcal{Q}$, meaning $\mathcal{P}$ and $\mathcal{Q}$ are equivalent systems.

Conversely, let $\mathcal{P}=(P_1,\dots,P_n)\subset\mathbb{P}^{k-1}$ be a projective $[n,k,d]_q$ system. For each P_i, choose an arbitrary representative $p_i\in\mathbb{F}_q^k$, and consider the linear map $\mathrm{Ev}_{\mathcal{P}}:(\mathbb{F}_q^k)^*\to\mathbb{F}_q^n$ given by

$$\mathrm{Ev}_{\mathcal{P}}(\varphi)=(\varphi(p_1),\dots,\varphi(p_n))$$

Since $\mathcal{P}$ is not contained in any hyperplane, the vectors $p_1,\dots,p_n$ span $\mathbb{F}_q^k$, and hence $\mathrm{Ev}_{\mathcal{P}}$ is injective. Therefore its image is an $[n,k]_q$ code C. Furthermore, since each p_i is nonzero, there is some element of $(\mathbb{F}_q^k)^*$ which is nonzero at p_i, and hence C is nondegenerate. A nonzero element $\varphi\in(\mathbb{F}_q^k)^*$ determines a projective hyperplane $H(\varphi)\subset\mathbb{P}^{k-1}$ consisting of those points on which φ vanishes. The weight of $\mathrm{Ev}_{\mathcal{P}}(\varphi)$ is given by

$$\big\|\mathrm{Ev}_{\mathcal{P}}(\varphi)\big\| = \big|\{p_i:\varphi(p_i)\neq 0\}\big| = n-\big|\mathcal{P}\cap H(\varphi)\big|$$

This implies that C is an $[n,k,d]_q$ code.

Now let $\mathcal{Q}=\{Q_1,\dots,Q_n\}$ be a projective system which is equivalent to $\mathcal{P}$, and let C' be the code obtained from this system in the same way, with $q_i\in\mathbb{F}_q^k$ the chosen representative of Q_i. We wish to show C and C' are equivalent. Let $T:\mathbb{P}^{k-1}\to\mathbb{P}^{k-1}$ be a projective automorphism such that $T(\mathcal{P})=\mathcal{Q}$, so that $T(P_i)=Q_{\sigma(i)}$ for some permutation $\sigma\in S_n$. We can extend T in an arbitrary way to some linear automorphism $\hat{T}:\mathbb{F}_q^k\to\mathbb{F}_q^k$, with $\hat{T}(p_i)=a_iq_{\sigma(i)}$ for some nonzero scalars $a_i\in\mathbb{F}_q$. Let $A\in\mathcal{A}_n$ be the map given by permuting coordinates by σ and scaling the ith coordinate by a_i. One can then verify that $\mathrm{Ev}_{\mathcal{P}}\circ\hat{T}^*=A\circ\mathrm{Ev}_{\mathcal{Q}}$. Thus $C'=A(C')$, and hence C and C' are equivalent codes.

□

Remark 2.11. If we reinterpret the Singleton bound in terms of projective systems, we find it is the statement that

$$k-1 \leq \max\{|\mathcal{P} \cap H| : H \text{ is a projective hyperplane in } \mathbb{P}^{k-1}\}$$

That is, there exists some projective hyperplane containing at least $k-1$ points of $\mathcal{P}$. But any $k-1$ points in $\mathbb{P}^{k-1}$ lie in a hyperplane.

3. Algebraic Function Fields

3.1. **Function Fields and Places.** In this section, we introduce the concept of an algebraic function field. This enables us to do algebraic geometry over a field which is not algebraically closed, and will be vital to our constructions of algebraic geometry codes in the following section. Throughout this section, let $\Bbbk$ denote an arbitrary field.

Definition 3.1. An *algebraic function field* (or just a *function field*) $\mathbb{K}/\Bbbk$ of one variable over $\Bbbk$ is a field $\mathbb{K} \supset \Bbbk$ such that $\mathbb{K}$ is a finite algebraic extension of $\Bbbk(x)$, where $x \in \mathbb{K}$ is transcendental over $\Bbbk$.

Example 3.2. The most basic example of a function field is when we take $\mathbb{K} = \Bbbk(x)$. This is called the *rational function field*, and it corresponds to rational functions on the projective line $\mathbb{P}^1(\Bbbk)$.

It is also common to represent a function field as a simple algebraic extension of $\Bbbk(x)$. That is, we have $\mathbb{K} = \Bbbk(x, y)$, where $\varphi(y) = 0$ for some irreducible polynomial $\varphi(t) \in \Bbbk(x)[t]$. We will see this in Section 5 when we look at the example of the Hermitian function field, which is given by $\mathbb{F}_{r^2}(x, y)/\mathbb{F}_r$, along with the relation $x^{r+1} = y^r + y$.

Definition 3.3. A *valuation ring* of a function field $\mathbb{K}/\Bbbk$ is a proper subring $\mathcal{O} \subset \mathbb{K}$ such that $\mathcal{O} \supset \Bbbk$, and such that for all $f \in \mathbb{K}$, at least one of f or f^{-1} lies in $\mathcal{O}$.

The set $\mathcal{O}^*$ of elements f such that both f and f^{-1} lie in $\mathcal{O}$ is a group under multiplication, and is called the *group of units* of $\mathcal{O}$. Clearly, we have $\Bbbk^* \subset \mathcal{O}^*$.

Proposition 3.4. *Let $\mathcal{O}$ be a valuation ring of $\mathbb{K}/\Bbbk$. Then the set $P = \mathcal{O} \setminus \mathcal{O}^*$ is a maximal ideal of $\mathcal{O}$; moreover, it is the unique maximal ideal of $\mathcal{O}$.*

Proof. Let $f \in P$ and $u \in \mathcal{O}$. Then fu cannot lie in $\mathcal{O}^*$ or else f would be a unit; hence $fu \in P$. Now, if $f, g \in P$, then either f/g or g/f belongs to P. Without loss of generality, assume it is f/g. Then $f + g = g(f/g + 1) \in P$. Thus P is an ideal.

Any ideal which contains a unit $u \in \mathcal{O}^*$ must contain the entire ring, and thus P is maximal, as well as unique. □

Proposition 3.5. *The maximal ideal P of a valuation ring $\mathcal{O}$ is principal. Moreover, if t is a generator of P, then every element $f \in \mathbb{K}^*$ may be represented uniquely as $t^n u$ for some $n \in \mathbb{Z}$ and some unit $u \in \mathcal{O}^*$.*

Proof. See [1, proposition 2.5.1]. □

In algebraic geometry over algebraically closed fields, we speak of points on varieties. For algebraic function fields, we replace the notion of a point with the notion of a *place*.

Definition 3.6. A *place* of a function field $\mathbb{K}/\Bbbk$ is the maximal ideal P of some valuation ring $\mathcal{O} \subset \mathbb{K}$. The set of all places of $\mathbb{K}$ is denoted by $\mathbb{P}_{\mathbb{K}}$.

A place P uniquely determines a corresponding valuation ring; namely, the ring which consists of the elements $f \in \mathbb{K}$ whose inverses do not lie in P. We denote the valuation ring corresponding to a place P by $\mathcal{O}_P$.

Definition 3.7. A *discrete valuation* of a function field $\mathbb{K}/\Bbbk$ is a function $\nu : \mathbb{K} \to \mathbb{Z} \cup \{\infty\}$ satisfying the following conditions.

(1) $\nu(fg) = \nu(f) + \nu(g)$ for all $f, g \in \mathbb{K}$.
(2) $\nu(f + g) \geq \min(\nu(f), \nu(g))$ for all $f, g \in \mathbb{K}$.
(3) There is some element $f \in \mathbb{K}$ such that $\nu(f) = 1$.
(4) $\nu(\lambda) = 0$ for all $\lambda \in \Bbbk^*$.
(5) $\nu(f) = \infty$ if and only if $f = 0$.

By Proposition 3.5, every place $P \in \mathbb{P}_\mathbb{K}$ has a generator t. Such a generator is called a *local parameter* at P. This proposition immediately suggests the following candidate for a discrete valuation on $\mathbb{K}$.

Definition 3.8. Let $P \in \mathbb{P}_\mathbb{K}$ be a place, and define a function ν_P as follows. Let t be a local parameter at P. For $f \in \mathbb{K}*$, write $f = t^n u$ for an integer $n \in \mathbb{Z}$ and a unit $u \in \mathcal{O}_P^*$, and set $\nu_P(f) = n$. Of course we must define $\nu_P(0) = \infty$.

Observe that this function is independent of the choice of local parameter. Indeed, if s is another local paremeter, then we may write $t = su$ where $u \in \mathcal{O}_P^*$ is a unit. For any $f \in \mathbb{K}^*$, we have $f = t^n v$ for some unit v. But $t^n v = s^n(u^n v)$, and $u^n v$ is also a unit.

Proposition 3.9. *The function ν_P is a discrete valuation on $\mathbb{K}$.*

Proof. We first prove properties (1) and (2). Let $f, g \in \mathbb{K}$. If either of f or g is 0, then (1) and (2) are both obvious, so assume both are nonzero. Then $\nu_P(f) = n$ and $\nu_P(g) = m$ for some $n, m \in \mathbb{Z}$. Write $f = t^n u$ and $g = t^m v$ for a local parameter $t \in P$ and units $u, v \in \mathcal{O}_P^*$. Then $fg = t^{n+m}uv$, where $uv \in \mathcal{O}^*$, so (1) is satisfied. Assume without loss of generality that $n \leq m$. Then we have $f + g = t^n(u + t^{m-n}v) = t^n h$, where h lies in $\mathcal{O}_P$. If $h = 0$, then $\nu_P(f + g) = \infty$, and we are done. Otherwise, we can write $h = t^k w$ where $w \in \mathcal{O}_P^*$ is another unit and $k \geq 0$. Then $\nu_P(f + g) = n + k \geq n$, so (2) is satisfied.

Property (3) follows since $\nu_P(t) = 1$ whenever t is a local parameter; property (4) is obvious since $\Bbbk^* \subset \mathcal{O}_P^*$; and property (5) is by definition. □

One can now observe that we have the following relationships between ν_P and the sets $\mathcal{O}_P$, $\mathcal{O}_P^*$, and P.

$$\mathcal{O}_P = \{f \in \mathbb{K} : \nu_P(f) \geq 0\},$$
$$\mathcal{O}_P^* = \{f \in \mathbb{K} : \nu_P(f) = 0\},$$
$$P = \{f \in \mathbb{K} : \nu_P(f) > 0\}$$

In the following definitions, we will make it more clear why $\mathbb{K}/\Bbbk$ is called a function field.

Definition 3.10. Since a ring quotiented by a maximal ideal is a field, we may define the *residue class field* of a place P to be the quotient field $\mathcal{O}_P/P$. We denote this field by $\Bbbk_P$.

Definition 3.11. Let $P \in \mathbb{P}_\mathbb{K}$ be a place, and let $f \in \mathbb{K}$. The *value of f at P*, denoted by $f(P)$, is defined by setting $f(P)$ equal to the image of f in $\Bbbk_P$ whenever

f lies in $\mathcal{O}_P$, and setting $f(P) = \infty$ otherwise. Thus P determines a map from $\mathbb{K}$ to $\Bbbk_P \cup \{\infty\}$.

It now makes sense to define the following.

Definition 3.12. Let $P \in \mathbb{P}_\mathbb{K}$ be a place and $f \in \mathbb{K}$. Then P is a *zero* of f if $\nu_P(f) > 0$ (equivalently, $f \in P$). The value $\nu_P(f)$ is called the order of the zero at P. Similarly, P is a *pole* of f if $\nu_P(f) < 0$ (equivalently, $f^{-1} \in P$); and $-\nu_P(f)$ is called the order of the pole at P.

Recall that the nonzero elements of $\Bbbk$ all lie in $\mathcal{O}_P^* = \mathcal{O}_P \setminus P$. Thus each of them has a different equivalence class in $\Bbbk_P$, implying there is a natural embedding of $\Bbbk$ into $\Bbbk_P$. Thus the following definition makes sense.

Definition 3.13. The *degree* of a place P, denoted by $\deg P$, is the degree of the extension $\Bbbk_P/\Bbbk$.

If a place P is a place of degree 1, then $\Bbbk_P = \Bbbk$, and so for any $f \in \mathbb{K}$, the value of f at P is an element of $\Bbbk \cup \{\infty\}$. That is, f may be thought of as a $\Bbbk$-valued function on the places of degree 1 (where f is allowed to have poles).

Proposition 3.14. *The degree of a place $P \in \mathbb{P}_\mathbb{K}$ is finite. In fact, if x is a nonzero element of P, then* $\deg P \leq [\mathbb{K} : \Bbbk(x)]$.

Proof. See [1, proposition 2.5.7]. □

3.2. **Divisors.** In this section, we begin to build towards the Riemann-Roch theorem by introducing the notion of a *divisor* on a function field.

Definition 3.15. The *divisor group* $\operatorname{Div} \mathbb{K}$ of the function field $\mathbb{K}/\Bbbk$ is the free abelian group generated by the places $P \in \mathbb{P}_\mathbb{K}$. A *divisor* D of $\mathbb{K}/\Bbbk$ is an element of this group. In other words, D is a formal sum $\sum_{P \in \mathbb{P}_\mathbb{K}} a_P P$ for coefficients $a_P \in \mathbb{Z}$, only finitely many of which are nonzero.

The coefficient of the place P in a divisor D is denoted by $\nu_P(D)$. The *degree* of a divisor D, denoted by $\deg D$, is the sum of the coefficients weighted by the degree of the corresponding place, that is

$$\deg D = \sum_{P \in \mathbb{P}_\mathbb{K}} \nu_P(D) \deg P$$

As only finitely many coefficients are nonzero, this is well-defined. The *support* of a divisor is the set of places whose corresponding coefficients are nonzero, and is denoted by $\operatorname{Supp} D$.

We can define a partial ordering on $\operatorname{Div} \mathbb{K}$ by setting $D \leq D'$ whenever $\nu_P(D) \leq \nu_P(D')$ for all $P \in \mathbb{P}_\mathbb{K}$. A divisor D is called an *effective* divisor if $D \geq 0$ with respect to this ordering.

The notation $\nu_P(D)$ for the coefficient of the place P suggests the following definition.

Definition 3.16. Let $f \in \mathbb{K}^*$. The *principal divisor* of f, denoted by (f), is $\sum_{P \in \mathbb{P}_\mathbb{K}} \nu_P(f) P$. If Z is the set of zeroes of f, and N is the set of poles of f, then (f) is the difference between the *divisor of zeroes*,

$$(f)_0 := \sum_{P \in Z} \nu_P(f) P$$

and the *divisor of poles*,

$$(f)_\infty := \sum_{P \in N} -\nu_P(f)P$$

The next theorem shows that not only is this well-defined (i.e. that a function has only a finite number of zeroes and poles), but that a function has the *same* number of zeroes and poles, when multiplicities are properly counted.

Theorem 3.17. *The degree of a principal divisor is 0.*

Proof. See [4, theorem 1.4.11]. □

We define an equivalence relation on divisors by saying that two divisors D and D' are equivalent if $D' = D + (f)$ for some function $f \in \mathbb{K}^*$. In this case, we write $D \sim D'$. The fact that this is an equivalence relation follows from the fact that the principal divisors form a subgroup of $\operatorname{Div} \mathbb{K}$. Indeed, for any $f, g \in \mathbb{K}^*$, we have $(f) + (g) = (fg)$, and $-(f) = (f^{-1})$. Theorem 3.17 implies that equivalent divisors have the same degree, though it is not always true that two divisors of the same degree are equivalent.

One may think of a divisor as specifying, for each place $P \in \mathbb{P}_\mathbb{K}$, how poorly behaved a function $f \in \mathbb{K}$ is allowed to be at P; given a divisor D, we want to look at functions with a pole at P of order at most $-\nu_P(D)$ whenever $\nu_P(D) < 0$, and with a zero of order at least $\nu_P(D)$ whenever $\nu_P(D) > 0$. The following definition formalizes this idea.

Definition 3.18. Let D be a divisor of $\mathbb{K}/\Bbbk$. We define $L(D)$ to be the space given by

$$L(D) := \{f \in \mathbb{K}^* : (f) + D \geq 0\} \cup \{0\}$$

Observe that $L(D)$ is a vector space over $\Bbbk$. Indeed, scaling f by a nonzero constant $\lambda \in \Bbbk$ does not change the principal divisor of f; moreover, if we have $f, g \in L(D)$, then at any place P we have $\nu_P(f + g) \geq \min(\nu_P(f), \nu_P(g)) \geq \nu_P(D)$ by property (2) of a discrete valuation, and thus we also have $f + g \in L(D)$.

Proposition 3.19. *If $D \sim D'$, then $L(D) \cong L(D')$.*

Proof. Let $D' = D + (f)$. We claim the map $g \mapsto fg$ is an isomorphism from $L(D)$ to $L(D')$. If $g \in L(D)$, then for any place P, we have $\nu_P(g) \geq \nu_P(D)$. Thus $\nu_P(fg) = \nu_P(f) + \nu_P(g) \geq \nu_P(f) + \nu_P(D) = \nu_P(D')$. Hence, we indeed have $gf \in L(D')$. Moreover, this map is certainly linear, and its inverse is given by $g \mapsto f^{-1}g$. □

Lemma 3.20. $L(D) = \{0\}$ *whenever* $D < 0$

Proof. If there were a nonzero $f \in L(D)$, then we would have $(f) + D \geq 0$, and hence $\deg(f) > 0$. But this is impossible by Theorem 3.17. □

Lemma 3.21. $L(0) = \Bbbk$.

Proof. See [4, lemma 1.4.7]. □

Lemma 3.22. *Let $D, D' \in \operatorname{Div} \mathbb{K}$ be divisors with $D \leq D'$. Then we have*

$$\dim_\Bbbk(L(D')/L(D)) \leq \deg D' - \deg D$$

Proof. Note first that $D \leq D'$ implies $L(D) \subset L(D')$; if we have $f \in L(D)$, then $(f) + D' \geq (f) + D \geq 0$, so $f \in L(D')$ as well. Thus the quotient $L(D')/L(D)$ makes sense.

Now, since $D \leq D'$, we can write $D' = D + P_1 + \cdots + P_m$ for some not necessarily distinct places P_i. We can therefore assume that $D' = D + P$, and induction proves the general case. Let $t \in \mathbb{K}$ be an element such that $\nu_P(t) = \nu_P(D') = \nu_P(D) + 1$. Consider the linear map $\varphi_P : L(D') \to \Bbbk_P$ given by $\varphi_P(f) = (ft)(P)$. Note that for $f \in L(D')$, we have $\nu_P(ft) = \nu_P(f) + \nu_P(t) \geq -\nu_P(D') + \nu_P(D') = 0$, so this is a well-defined map (i.e. $(ft)(P) \neq \infty$). Moreover, the kernel of φ_P is exactly $L(D)$; f lies in the kernel exactly when $\nu_P(ft) > 0$, which occurs only when $\nu_P(f) > -\nu_P(D')$, i.e. $\nu_P(f) \geq -\nu_P(D)$. Hence, it follows that

$$\dim_{\Bbbk}(L(D')/L(D)) \leq \dim_{\Bbbk}(\Bbbk_P) = \deg P = \deg D' - \deg D$$

□

Corollary 3.23. *$L(D)$ is finite-dimensional as a $\Bbbk$-vector space.*

Proof. If $L(D) = \{0\}$ we are done. Otherwise there is some $f \in L(D)$ such that $(f)+(D) \geq 0$. Let $D' = D+(f)$. Since $L(D') \cong L(D)$, it suffices to show D' is finite-dimensional. By Lemma 3.22, since $D' \geq 0$, we have $\dim_{\Bbbk}(L(D')/L(0)) \leq \deg D'$. Since $\dim_{\Bbbk}(L(0)) = \dim_{\Bbbk}(\Bbbk) = 1$, we conclude that $\dim_{\Bbbk} L(D') \leq \deg D' + 1$. □

We denote the dimension of $L(D)$ by $\ell(D)$. Observe that, as a consequence of Proposition 3.19, this depends only on the equivalence class of D. This corollary gives us an upper bound on $\ell(D)$ in terms of the degree of the divisor, namely, $\ell(D) \leq \deg D + 1$. We also have the following lower bound.

Proposition 3.24. *There exists a constant γ (dependent on the function field) such that $\deg D - \ell(D) \leq \gamma$ for all $D \in \operatorname{Div} \mathbb{K}$.*

Proof. See [4, proposition 1.4.14]. □

As a consequence of this result, we can introduce the following definition, which is an important numerical invariant of a function field.

Definition 3.25. The *genus* of a function field, denoted by g, is defined by

$$g := \max_{D \in \operatorname{Div} \mathbb{K}} \deg D - \ell(D) + 1$$

We can see that g is an integer, and taking $D = 0$, we find that g is a nonnegative integer.

3.3. **Differentials and Riemann-Roch.** Calculating the dimension $\ell(D)$ is, in general, a difficult problem, to which the theorem of Riemann-Roch gives a partial answer. In order to formulate the statement of the theorem, we first must introduce the notion of a differential on a function field. The complete definition is rather technical, and we shall omit some elements of it; a full treatment is given in chapter 4 of [4]. The important idea is that these differentials should behave similarly to the differentials of calculus. Until now, we have allowed $\Bbbk$ to be an arbitrary field, but here we shall require that $\Bbbk$ be perfect.

Definition 3.26. Let M be a $\mathbb{K}$-module. A *derivation* of $\mathbb{K}$ into M is a $\Bbbk$-linear map $\delta : \mathbb{K} \to M$ such that for all $x, y \in \mathbb{K}$, the "product rule" holds:

$$\delta(xy) = x\delta(y) + y\delta(x)$$

Definition 3.27. For each $x \in \mathbb{K}$, let $[x]$ be a symbol. Let F be the free $\mathbb{K}$-module generated by the elements $\{[x] : x \in \mathbb{K}\}$. Consider the submodule N generated by

(1) $\{[x+y] - [x] - [y] : x, y \in \mathbb{K}\}$
(2) $\{[\lambda x] - \lambda[x] : x \in \mathbb{K}, \lambda \in \Bbbk\}$
(3) $\{[xy] - x[y] - y[x] : x, y \in \mathbb{K}\}$

Let $\Omega_{\mathbb{K}}$ be the quotient module F/N, called the *module of differentials* of $\mathbb{K}$.

For $[x] \in F$, we denote by dx the equivalence class of $[x]$ in $\Omega_{\mathbb{K}}$. Let $d : \mathbb{K} \to \Omega_{\mathbb{K}}$ be the map which sends x to dx. Then d is a derivation of $\mathbb{K}$ into $\Omega_{\mathbb{K}}$. Indeed, since N is contains the sets (1) and (2), the map d is $\Bbbk$-linear, and (3) implies that d satisfies the product rule.

Definition 3.28. A *separating element* of $\mathbb{K}/\Bbbk$ is an element $x \in \mathbb{K}$ such that $\mathbb{K}/\Bbbk(x)$ is a finite separable extension.

Lemma 3.29.
(1) Let $t \in \mathbb{K}$. If for some place $P \in \mathbb{P}_{\mathbb{K}}$, t is a local parameter at P, then t is a separating element of $\mathbb{K}/\Bbbk$.
(2) If t is a separating element, then $dt \neq 0$.

Proof. See [4, proposition 3.10.2] for (1) and [4, proposition 4.1.8] for (2). □

Proposition 3.30. *$\Omega_{\mathbb{K}}$ is a one-dimensional $\mathbb{K}$-module.*

Proof. See [4, proposition 4.1.8]. □

It follows that if dx is nonzero, then every differential $\omega \in \Omega_{\mathbb{K}}$ factors uniquely as $\omega = f\,dx$ for an element $f \in \mathbb{K}$.

Definition 3.31. Let $\omega \in \Omega_K$ be a differential, and let $P \in \mathbb{P}_{\mathbb{K}}$ be a place with a local parameter t. Since $dt \neq 0$, we can write $\omega = f\,dt$. Set $\nu_P(\omega) := \nu_P(f)$.

It can also be shown that this definition is independent of the choice of local parameter, and that $\nu_P(\omega) \neq 0$ for only finitely many places P. It is then natural to define a divisor associated to a differential.

Definition 3.32. Let $\omega \in \Omega_{\mathbb{K}} \setminus \{0\}$. Then the divisor of ω, denoted by (ω), is defined to be $\sum_{P \in \mathbb{P}_{\mathbb{K}}} \nu_P(\omega) P$. This divisor is called a *canonical divisor* of $\mathbb{K}$. The divisor of zeroes of ω, $(\omega)_0$, and the divisor of poles of ω, $(\omega)_\infty$, are defined similarly to Definition 3.16.

Definition 3.33. Let $\omega, \omega' \in \Omega_{\mathbb{K}} \setminus \{0\}$. Then by Proposition 3.30, there exists some $f \in \mathbb{K}^*$ such that $\omega' = f\omega$. It follows that $(\omega') = (f) + (\omega)$, and hence all canonical divisors are in the same equivalence class. This equivalence class is called the *canonical class* of divisors of $\mathbb{K}$. We often denote an arbitrary divisor in this class by K.

Given a divisor D, we defined a space of functions $L(D)$; we can also define a similar space $\Omega(D)$ of differentials.

Definition 3.34. Let $D \in \operatorname{Div} \mathbb{K}$ be a divisor. Define the space

$$\Omega(D) := \{\omega \in \Omega_{\mathbb{K}} \setminus \{0\} : (\omega) + D \geq 0\} \cup \{0\}$$

Notice that if K is a canonical divisor, then $\Omega(D) \cong L(K+D)$. Indeed, if $K = (\omega)$, then the map $\varphi : L(K+D) \to \Omega(D)$, $\varphi(f) = f\omega$ is an isomorphism.

Recall from our definition of genus in Definition 3.25 that $g \geq \deg D - \ell(D) + 1$ for all divisors $D \in \operatorname{Div} \mathbb{K}$. The Riemann-Roch theorem, which we are finally ready to state, identifies the "missing term" which turns this into an equality. We do not attempt to prove the theorem here; it is quite a deep result. We do prove some of its immediate corollaries.

Theorem 3.35 (Riemann-Roch)**.** *Let $D \in \operatorname{Div} \mathbb{K}$ be a divisor, and let K be any divisor in the canonical class of $\mathbb{K}$. Then the following equality holds*

$$\ell(D) - \ell(K - D) = \deg D - g + 1$$

Proof. See [4, theorem 1.5.15], or [2, section 8.6]. □

Corollary 3.36. *If K is a canonical divisor, then $\ell(K) = g$.*

Proof. Setting $D = 0$ in the Riemann-Roch theorem gives the following

$$\ell(0) - \ell(K) = \deg 0 - g + 1$$

Since $\ell(0) = 1$, we find $\ell(K) = g$. □

Corollary 3.37. *If K is a canonical divisor, then $\deg K = 2g - 2$.*

Proof. Setting $D = K$ in the Riemann-Roch theorem gives the following

$$\ell(K) - \ell(0) = \deg K - g + 1$$

Since $\ell(K) = g$ and $\ell(0) = 1$, we obtain the desired equality. □

Corollary 3.38. *If D is a divisor such that $\deg D > 2g - 2$, then*

$$\ell(D) = \deg D - g + 1$$

Proof. From the previous corollary, $\deg(K - D) < 0$, and thus $\ell(K - D) = 0$. The result follows by Riemann-Roch. □

3.4. **Residues of Differentials.** Before we introduce algebraic geometry codes, we must define the *residue* of a differential, which will be necessary to construct the duals of algebraic geometry codes.

Definition 3.39. Let $f \in \mathbb{K}$, let $P \in \mathbb{P}_{\mathbb{K}}$, and let t be a local parameter at P. Then f can be expanded as a Laurent series

$$f = \sum_{i=-M}^{\infty} a_i t^i$$

We define the *residue of f at P with respect to t* by

$$\operatorname{Res}_{P,t}(f) := a_{-1}$$

Definition 3.40. Let $\omega \in \Omega_{\mathbb{K}}$, and let $P \in \mathbb{P}_{\mathbb{K}}$. Let t be a local parameter at P. Then we can write $\omega = f\,dt$ for some $f \in \mathbb{K}$. The *residue of ω at P* is defined as

$$\operatorname{Res}_P(\omega) := \operatorname{Res}_{P,t}(f)$$

It can be shown that this definition of $\operatorname{Res}_P(\omega)$ is independent of the choice of t, see [4, proposition 4.2.9]. We then have the following useful formula.

Theorem 3.41 (Residue Formula)**.** *Let $\omega \in \Omega_{\mathbb{K}}$. Then*

$$\sum_{P \in \mathbb{P}_{\mathbb{K}}} \operatorname{Res}_P(\omega) = 0$$

Proof. See [4, proposition 1.7.2], as well as [4, corollary 4.4.3]. □

4. Algebraic Geometry Codes

We now use the ideas developed in the previous section to construct the *algebraic geometry code*, linear codes constructed using algebraic function fields. We will also use results of the previous section to prove bounds on the parameters of these codes. Here we return to working over a finite field $\mathbb{F}_q$.

Definition 4.1. Let $\mathbb{K}/\mathbb{F}_q$ be a function field. Let $\mathcal{P} = \{P_1, \ldots, P_n\} \subset \mathbb{P}_{\mathbb{K}}$ be a subset of the places of $\mathbb{K}$ of degree 1. Let $D \in \operatorname{Div} \mathbb{K}$ be a divisor such that $\operatorname{Supp} D \cap \mathcal{P} = \emptyset$. Consider the map $\operatorname{Ev}_{\mathcal{P}} : L(D) \to \mathbb{F}_q^n$ given by

$$\operatorname{Ev}_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n))$$

This image of this map is a linear code of length n, which we denote by $(\mathbb{K}, \mathcal{P}, D)_L$. This construction is referred to as the L-construction.

The following example shows how the L-construction is a generalization of the process we used to construct the Reed-Solomon codes in Example 2.7.

Example 4.2. Consider the rational function field $\mathbb{F}_q(x)/\mathbb{F}_q$. Let Q_∞ be the place of degree 1 which is the unique pole of x, and let $\mathcal{P}$ be some set of the remaining places of degree 1, $n = |\mathcal{P}|$. Let $D = aQ_\infty$ for some integer $a < n$. Then $L(D)$ contains functions which have no poles anywhere except for at Q_∞, and which have a pole of order at most a at Q_∞, i.e. $L(D)$ consists precisely of the polynomials in x of degree at most a. Therefore, the code $C = (\mathbb{F}_q(x), \mathcal{P}, D)_L$ is exactly the Reed-Solomon code with parameters $[n, a+1, n-a]_q$.

Let $\mathbf{P} = \sum_{P \in \mathcal{P}} P$. The dimension of the code $(\mathbb{K}, \mathcal{P}, D)_L$ is given precisely by

$$k = \ell(D) - \ell(D - \mathbf{P}) \tag{4.3}$$

Indeed, $L(D - \mathbf{P})$ is exactly the kernel of the evaluation map $\operatorname{Ev}_{\mathcal{P}}$. Since $\operatorname{Supp} D \cap \mathcal{P} = \emptyset$, $L(D - \mathbf{P})$ consists of those functions in $L(D)$ which have a zero of order at least 1 at each place in $\mathcal{P}$.

Remark 4.4. Applying the Riemann-Roch theorem to (4.3), we obtain

$$k = (\deg D + 1 - g - \ell(K - D)) - (\deg D - n + 1 - g - \ell(K - D + \mathbf{P}))$$

When $\deg D > \deg(K + \mathbf{P}) = n + 2g - 2$, then both $\ell(K - D)$ and $\ell(K - D + \mathbf{P})$ are 0, and hence $k = n$. Also, if $\deg D < 0$, then $k = 0$. Thus the only interesting cases occur when $0 \leq \deg D \leq n + 2g - 2$.

Of course, determining the values of $\ell(D)$ and $\ell(D - \mathbf{P})$ is difficult, so (4.3) does not completely answer the question of how to determine the dimension. Moreover, we do not have any precise formula for the minimum distance. However, we do have the following lower estimates.

Theorem 4.5. *Let $C = (\mathbb{K}, \mathcal{P}, D)_L$ be a code. Let $a = \deg D$, and suppose that $0 \leq a < n$. Then we have the following lower bounds on the dimension and minimum distance of C.*

$$k \geq a - g + 1 \tag{4.6}$$

and

$$d \geq n - a \tag{4.7}$$

Proof. Note that since $a < n$, we have $\ell(D - \mathbf{P}) = 0$. Thus, (4.3) implies that k is exactly equal to $\ell(D)$. By Riemann-Roch, we know $\ell(D) \geq a - g + 1$.

Now, to prove the estimate for d, we want to show that a function $f \in L(D) \setminus \{0\}$ can have at most a zeroes in $\mathcal{P}$. We write $D = D^+ - D^-$, where D^+ and D^- are effective divisors with disjoint support. Notice that f has at least $\deg D^+$ zeroes in $\operatorname{Supp} D$, and at most $\deg D^-$ poles. Since the principal divisor of f has degree 0, the number of zeroes of f outside of $\operatorname{Supp} D$ is therefore at most $\deg D^+ - \deg D^- = a$. Since we have required in the construction that $\operatorname{Supp} D \cap \mathcal{P} = \emptyset$, f can have at most a zeroes in $\mathcal{P}$. □

The estimates (4.6) and (4.7) are quite important, and are in fact given their own special names. The value $a - g + 1$ is denoted k_c, and is called the *designed dimension* of C. The value $n - a$ is denoted d_c, and is called the *designed distance* of C.

Given the same data (namely, a function field, a divisor, and a set of places of degree 1), we can also construct another code.

Definition 4.8. Let $\mathbb{K}/\mathbb{F}_q$, $\mathcal{P}$, and D be as in Definition 4.1. Consider the map $\operatorname{Res}_{\mathcal{P}} : \Omega(\mathbf{P} - D) \to \mathbb{F}_q^n$ given by

$$\operatorname{Res}_{\mathcal{P}}(\omega) = (\operatorname{Res}_{P_1}(\omega), \dots, \operatorname{Res}_{P_n}(\omega))$$

The image is a code which we denote by $(\mathbb{K}, \mathcal{P}, D)_\Omega$, and this construction is referred to as the Ω-construction.

Recalling that $\Omega(D) \cong L(K + D)$ where K is any canonical divisor, we have the following precise formula for the dimension of the code $(\mathbb{K}, \mathcal{P}, D)_\Omega$.

$$k = \dim_{\mathbb{k}} \Omega(\mathbf{P} - D) - \dim_{\mathbb{k}} \Omega(-D) = \ell(K + \mathbf{P} - D) - \ell(K - D) \tag{4.9}$$

Indeed, $\Omega(-D)$ is the kernel of the residue map $\operatorname{Res}_{\mathcal{P}}$. Since $\operatorname{Supp} D \cap \mathcal{P} = \emptyset$, the space $\Omega(-D)$ consists exactly of those differentials in $\Omega(\mathbf{P} - D)$ which have no poles at any places in $\mathcal{P}$, and thus whose residue at each place of $\mathcal{P}$ is 0.

Again, the values of $\ell(K + \mathbf{P} - D)$ and $\ell(K - D)$ are not generally easy to determine, and we do not in general know the minimum distance of an Ω-code. However, we do have lower estimates on the parameters of the Ω-construction as well.

Theorem 4.10. *Let $C = (\mathbb{K}, \mathcal{P}, D)_\Omega$ be a code. Let $a = \deg D$, and suppose that $a > 2g - 2$. Then*

$$k \geq n - a + g - 1 \tag{4.11}$$

and

$$d \geq a - 2g + 2 \tag{4.12}$$

Proof. Notice that since $a > 2g-2 = \deg K$, we have $\ell(K-D) = 0$. Thus, (4.9) implies that k is exactly equal to $\ell(K+\mathbf{P}-D)$. By Riemann-Roch, we know $\ell(K+\mathbf{P}-D) \geq (2g-2+n-a)-g+1 = n-a+g-1$, as desired.

To show that $d \geq a-2g+2$, we must show that for a nonzero differential $\omega \in \Omega(\mathbf{P}-D)$, there are at least $a-2g+2$ places of $\mathcal{P}$ where ω has nonzero residue. As before, we write $D = D^+ - D^-$, where D^+ and D^- are effective divisors with disjoint support. Note that we have $(\omega)_0 \geq \omega \geq D \geq D^+$, and therefore

$$(\omega)_\infty = (\omega)_0 - (\omega) \geq D^+ - (\omega) = D - (\omega) - D^-$$

Taking degrees, we find that

$$\deg(\omega)_\infty \geq a - 2g + 2 - \deg D^-$$

Then ω must have at least $a-2g+2$ poles outside of $\operatorname{Supp} D$. But since $\omega \in \Omega(\mathbf{P}-D)$, these poles must lie in $\mathcal{P}$, and moreover, their order must be exactly 1, meaning ω has a nonzero residue at each pole. So there are at least $a-2g+2$ places of $\mathcal{P}$ where ω has a nonzero residue, as desired. □

The estimates (4.11) and (4.12), respectively, are also referred to as the designed dimension and distance for the corresponding Ω-code. The following theorem gives the relation between the two constructions.

Theorem 4.13. *The codes $C_L = (\mathbb{K}, \mathcal{P}, D)_L$ and $C_\Omega = (\mathbb{K}, \mathcal{P}, D)_\Omega$ are dual to each other.*

Proof. Let $f \in L(D)$, and let $\omega \in \Omega(\mathbf{P}-D)$. By the Residue formula, it follows that

$$\sum_{i=1}^{n} f(P_i) \operatorname{Res}_{P_i}(\omega) = \sum_{i=1}^{n} \operatorname{Res}_{P_i}(f\omega) = 0$$

So $C_L \perp C_\Omega$. It remains to check that $\dim C_L + \dim C_\Omega = n$. Using the precise values of the dimensions from (4.3) and (4.9), along with the Riemann-Roch theorem, it follows that

$$\begin{aligned}
\dim C_L + \dim C_\Omega &= \ell(D) - \ell(D-\mathbf{P}) + \ell(K+\mathbf{P}-D) - \ell(K-D) \\
&= (\ell(D) - \ell(K-D)) - (\ell(D-\mathbf{P}) - \ell(K+\mathbf{P}-D)) \\
&= (\deg D + 1 - g) - (\deg(D-\mathbf{P}) + 1 - g) \\
&= n
\end{aligned}$$

Thus C_L and C_Ω are each other's duals. □

5. Hermitian Codes

Recall that for a Reed-Solomon code, we must select a set $\mathcal{P} \subset \mathbb{F}_q$. This has the disadvantage that we must have $n \leq q$. In this section, we will look at codes arising from Hermitian function fields, which allow for a longer length in comparison to the size of the alphabet. We first define the Hermitian function field and examine some of its properties. Then we use the Hermitian function field to construct codes, and investigate their parameters.

Definition 5.1. Let $q = r^2$. The *Hermitian function field* H over $\mathbb{F}_q$ is given by $\mathbb{F}_q(x,y)$, where

$$x^{r+1} = y^r + y$$

In the following lemma, we state some properties of the Hermitian function field which will be useful in calculating the parameters of Hermitian codes.

Lemma 5.2.
(1) The genus of H is $g = r(r-1)/2$.
(2) H has exactly r^3+1 places of degree 1, which consist of (1) the common pole of x and y, denoted by Q_∞, and (2) for each of the r^3 pairs (α, β) which satisfy $\alpha^{r+1} = \beta^r + \beta$, a place $P_{\alpha,\beta}$ which satisfies $x(P_{\alpha,\beta}) = \alpha$ and $y(P_{\alpha,\beta}) = \beta$.
(3) The principal divisors of $x-\alpha$ and $y-\beta$ are

$$(x-\alpha) = \sum_{\beta^r+\beta=\alpha^{r+1}} P_{\alpha,\beta} - rQ_\infty$$

$$(y-\beta) = \begin{cases} (r+1)P_{0,\beta} - (r+1)Q_\infty & \text{if } \beta^r+\beta = 0 \\ \sum_{\beta^r+\beta=\alpha^{r+1}} P_{\alpha,\beta} - (r+1)Q_\infty & \text{otherwise} \end{cases}$$

(4) The canonical divisor (dx) is given by $(r^2-r-2)Q_\infty$.
(5) For an integer m, the set

$$B(m) := \{x^i y^j : 0 \le i, 0 \le j \le r-1, ir + j(r+1) \le m\}$$

is a basis of $L(mQ_\infty)$.

Proof. See [4, lemma 6.4.4]. □

We use the Hermitian function field H to construct a code in the following way. Let $\mathcal{P}$ consist of all of the places of degree 1 except for Q_∞. Given an integer m, let C_m be the code given by $(H, \mathcal{P}, mQ_\infty)_L$, which is a code of length $n = r^3$. Denote the dimension of C_m by k_m, and the minimum distance by d_m. As in the previous section, let $\mathbf{P}$ be the divisor $\sum_{P\in\mathcal{P}} P$. Recalling Remark 4.4, we consider only those values of m for which $0 \le m \le n + 2g - 2 = r^3 + r^2 - r - 2$.

Lemma 5.3. *Let $z = x^q - x$. Let $\omega = dz/z$. Then $(\omega) = (r^3+r^2-r-2)Q_\infty - \mathbf{P}$. Moreover, at each $P_{\alpha,\beta}$, we have $\operatorname{Res}_{P_{\alpha,\beta}}(\omega) = 1$.*

Proof. Note that $dz = -dx$ since $d(x^q) = qx^{q-1} = 0$. Thus $(\omega) = (dx) - (z)$. We know that $(dx) = (r^2-r-2)Q_\infty$ by Lemma 5.2, so it suffices to show that $(z) = \mathbf{P} - r^3 Q_\infty$. Notice that we can write $z = \prod_{\alpha\in\mathbb{F}_q}(x-\alpha)$. Since we know the principal divisor of $x-\alpha$, we can easily compute the principal divisor of z,

$$(z) = \sum_{\alpha\in\mathbb{F}_q} (x-\alpha) = \sum_{\alpha,\beta} P_{\alpha,\beta} - r^3 Q_\infty$$

Finally, since z has a zero of order 1 at each $P_{\alpha,\beta}$, it is a local parameter at each $P_{\alpha,\beta}$. Thus we have $\operatorname{Res}_{P_{\alpha,\beta}}(\omega) = \operatorname{Res}_{P_{\alpha,\beta},z}(1/z) = 1$. □

Proposition 5.4. *The codes C_m and $C_{r^3+r^2-r-2-m}$ are dual to each other.*

Proof. Let $D = mQ_\infty$ and $D^\perp = (r^3+r^2-r-2-m)Q_\infty$, so that $C_m = (H, \mathcal{P}, D)_L$ and $C_{r^3+r^2-r-2-m} = (H, \mathcal{P}, D^\perp)_L$. By Lemma 5.3, we have $D^\perp = (\omega) + \mathbf{P} - D$.

As a consequence of L-Ω duality, it suffices to show that $(H, \mathcal{P}, D)_\Omega = (H, \mathcal{P}, D^\perp)_L$. We first observe that $\operatorname{Res}_{\mathcal{P}}(f\omega) = \operatorname{Ev}_{\mathcal{P}}(f)$ for all $f \in L(D^\perp)$. Indeed, we have shown that the residue of ω at every place $P \in \mathcal{P}$ is 1, and thus $\operatorname{Res}_P(f\omega) = f(P)\operatorname{Res}_P \omega = f(P)$. Now, it remains to be shown that the map $f \mapsto f\omega$ is an isomorphism from $L(D^\perp)$ to $\Omega(\mathbf{P} - D)$. If $f \in L(D^\perp)$, then $(f) + D^\perp \ge 0$, which

implies $(f)+(\omega)+\mathbf{P}-D \geq 0$, and hence $f\omega \in \Omega(\mathbf{P}-D)$. So the map does indeed go from $L(D^\perp)$ to $\Omega(\mathbf{P}-D)$. Moreover, given $\eta \in \Omega(\mathbf{P}-D)$, we can recover f by writing $\eta = f\omega$ (by Proposition 3.30). So this map is an isomorphism. □

Lemma 5.5. *If we write $m = ar+b$ where $0 \leq b \leq r-1$, then the size of $B(m)$ is given by*

$$\big|B(m)\big| = \begin{cases} a(a+1)/2 + \min(a,b) + 1 & \text{if } 0 \leq m \leq r^2-r-2 \\ m+1-\frac{r(r-1)}{2} & \text{if } m > r^2-r-2 \end{cases}$$

Proof. The second case follows by Riemann-Roch. The condition $m > r^2-r-2 = 2g-2$ implies that $\ell(mQ_\infty) = m+1-g$ by Corollary 3.38.

In the first case, we must count the number of pairs (i,j) such that $ir+j(r+1) \leq m = ar+b$. We must have $0 \leq i+j \leq a$. All pairs such that $i+j < a$ are valid, and the number of such pairs is $a(a+1)/2$. It remains to count the number of pairs with $i+j = a$. In this case, we have $ir+j(r+1) = ar+j$, so we must have $j \leq b$. So j may take on any value from 0 to $\min(a,b)$, which determines the value of i, and so the number of such pairs is $\min(a,b)+1$. □

Proposition 5.6. *The dimension of C_m is given by*

$$k_m = \begin{cases} \big|B(m)\big| & \text{if } 0 \leq m < r^3 \\ r^3 - \big|B(r^3+r^2-r-2-m)\big| & \text{if } r^3 \leq m \leq r^3+r^2-r-2 \end{cases}$$

Proof. When $m < r^3$, the map $\mathrm{Ev}_\mathcal{P}$ is injective, and thus $k_m = \ell(D) = \big|B(m)\big|$. The second case follows by Proposition 5.4. □

It is more difficult to determine the exact value of the minimum distance of C_m. We of course have the designed distance $d_c = r^3 - m$, which is useful whenever $m < r^3$. We can also prove the following.

Proposition 5.7. *Suppose that $m = ir+j(r+1) < r^3$ for $0 \leq i$ and $0 \leq j \leq r-1$. Then if $j = 0$ or $i < r^2-r-2$, we have $d_m = d_c = r^3 - m$.*

Proof. If $j = 0$, then $m = ir$. Since $i < r^2$, we may choose distinct elements $\alpha_1, \ldots, \alpha_i \in \mathbb{F}_q$. Let $f = (x-\alpha_1)\ldots(x-\alpha_i)$. Then f has exactly ir zeroes in $\mathcal{P}$. Since $f \in L(mQ_\infty)$, $d_m = r^3 - m$ follows.

If $i < r^2-r-2$, then we may choose distinct elements $\alpha_1, \ldots, \alpha_i$ such that $\alpha_l^{r-1} \neq 1$. There are r^2-r-1 such elements, namely, the elements in $\mathbb{F}_q \setminus \mathbb{F}_r^*$, so we can indeed choose them to be distinct. Now choose j distinct elements $\beta_1, \ldots, \beta_j$ such that $\beta_k^j + \beta_k = 1$. Let $f = (x-\alpha_1)\ldots(x-\alpha_i)(y-\beta_1)\ldots(y-\beta_j)$. Then $f \in L(mQ_\infty)$, and f has precisely m zeroes in $\mathcal{P}$. Indeed, each function $x-\alpha_l$ has r zeroes, and each function $y-\beta_k$ has $r+1$ zeroes, hence f has a total of $ir+j(r+1) = m$ zeroes. Since we have chosen α_l and β_k such that $\alpha_l^{r+1} \neq 1$ and $\beta_k^r + \beta_k = 1$, all m zeroes are distinct. Since $f \in L(mQ_\infty)$, it follows that $d_m = r^3 - m$. □

A more complete picture of the minimum distance of Hermitian codes can be found in [6, section 4.3].

Acknowledgments

I am deeply grateful to Yulia Kotelnikova for her mentorship throughout the program, for her patience when teaching me algebraic geometry, as well as for suggesting the topic of coding theory in the first place. I would also like to thank Peter May for organizing yet another virtual REU under difficult circumstances, along with all of the speakers for giving excellent talks.

References

[1] Michael Tsfasman, Serge Vladut, and Dmitry Nogin. *Algebraic Geometric Codes: Basic Notions.* American Mathematical Society. 2007.
[2] William Fulton. *Algebraic Curves.* 2008.
[3] Jacobus H. van Lint and Gerard van der Geer. *Introduction to Coding Theory and Algebraic Geometry.* Birkhäuser Verlag, Basel. 1988.
[4] Henning Stichtenoth. *Algebraic Function Fields and Codes.* Springer-Verlag Berlin Heidelberg. 2008.
[5] Dominic L. Wynter. *An Exposition of the Riemann-Roch Theorem for Curves.* 2016.
[6] Kyeongcheol Yang. *On the Weight Hierarchy of Hermitian Codes and Other Geometric Goppa Codes.* 1992.