Rational Algebraic Geometry Code

Dingyu Wang

24th August, 2020

1 Introduction

In this report, we will define the *algebraic geometry codes* and focus on the example of the *rational algebraic geometry codes*. The goal of this report is to teach readers about the concept of a general algebraic geometry code and demonstrate that the rational algebraic geometry code is exactly a generalized form of the Reed-Solomon code.

Why should we care about algebraic geometry code? One of the main reason is that it constructs a very large class of codes whose main parameters (code dimension and minimum distance) can be well estimated. Abstractly, whenever we realize that something satisfies some property (e.g. Reed-Solomon Code is MDS), we attempt to ask the question what in that thing enforces this property (e.g. what makes Reed-Solomon Code MDS?). Algebraic geometry code provides one step of answering this kind of question, which gives a very general version of Reed-Solomon Code that provides bounds on the minimum distance, and in many cases are also MDS.

In Section 2, some basic notions about group, ring, vector space and field that are essential to understand the algebraic geometry codes, are reviewed based on the textbook *Abstract Algebra* [1]. Then, in Section 3, I demonstrate related notions about the algebraic function field and in Section 4 the algebraic geometry code is defined. Finally in Section 5, the rational algebraic geometry code is constructed and discussed. Section 3, Section 4 and Section 5 are based on the first two chapters of the textbook *Algebraic Function Fields and Codes* [2].

2 Basic Notions in Algebra

In this section, I will introduce all the critical knowledge to understand what an algebraic field function field is. Only definitions are given here, all the results from the according theory are taken for granted. Each definition is followed by a concrete, simple but non-trivial example for a better understanding.

Readers that are already familiar with these concepts can safely skip to Section 3.

2.1 Groups

First of all, we need to define what a *group* is, since it underlies most of the interesting mathematical structures.

Definition (group)**.** A pair $(G, *)$ is called a group if

- G is some set and $*$ is a binary operation from $G \times G$ to G.
- $*$ is associative, i.e., $\forall a, b, c \in G$, $a * (b * c) = (a * b) * c$.
- There exists some $e \in G$ such that $\forall a \in G$, we have $a * e = e * a = a$.
- For all $a \in G$ there exists some $a^{-1} = G$ such that $a * a^{-1} = a^{-1} * a = e$.

We say $(G, *)$ is commutative (or abelian), if for any $a, b \in G$, we have $a * b = b * a$.

Example. Let $\mathrm{GL}(n, \mathbb{R})$ be the set of $n \times n$ matrices consisting of real entries that are invertible. The pair $(\mathrm{GL}(n, \mathbb{R}), \cdot)$ where $\cdot$ is the usual matrix multiplication, is a group. It is not commutative though.

2.2 Rings

To understand *places*, one needs to have a good understanding of the concepts of rings, ideals and quotient rings.

Definition (ring)**.** A triple $(R, +, \times)$ is called a ring if

- $(R, +)$ is an abelian group.
- $\times$ is an associative binary operation from $R \times R$ to R.
- For all $a, b, c \in R$, we have $(a + b) \times c = (a \times c) + (b \times c)$ and $a \times (b + c) = (a \times b) + (a \times c)$ (distributivity).

We say $(R, +, \times)$ is commutative if for all $a, b \in R$, we have $a \times b = b \times a$.

Example. Let $\mathrm{M}(n, \mathbb{R})$ be the set of all $n \times n$ matrices with real entries. The triple $(\mathrm{M}(n, \mathbb{R}), +, \cdot)$ where $+$ and $\cdot$ are the usual matrix addition and multiplication, is a ring. It is not commutative though.

Remark. When the context is clear, a group $(G, *)$ is often written as G and a ring $(R, +, \times)$ is often written as R.

Definition (subring)**.** A subset I of a ring $(R, +, \times)$ is called a subring if $(I, +\,|_I\, , \times\,|_I)$ is a ring.

Example. Let $\mathrm{D}(n, \mathbb{R})$ be the set of all diagonal $n \times n$ matrices with real entries. Then $\mathrm{D}(n, \mathbb{R})$ is a subring of $\mathrm{M}(n, \mathbb{R})$. Interestingly, while $\mathrm{M}(n, \mathbb{R})$ is not commutative, its subring $\mathrm{D}(n, \mathbb{R})$ is commutative.

Definition (ideal)**.** A subring I of a ring R is called an ideal of R if for any $r \in R, i \in I$, we have both $ri, ir \in I$.

We say an ideal I is maximal if there is no other proper subset of R that is an ideal while containing I.

Example. $\mathbb{Z}$ is a ring with usual addition and multiplication and $2\mathbb{Z} = \{2x \mid x \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$.

Definition (quotient ring)**.** Let R be a ring and I be an ideal of R, the quotient ring R/I is the set $\{r + I \mid r \in R\}$ with the projected operations. Note that $r + I$ is the set $\{r + i \mid i \in I\}$. For $r, s \in R$, the projected addition is defined as

$$(r + I) + (s + I) = (r + s) + I,$$

and the projected multiplication is defined as

$$(r + I) \times (s + I) = rs + I.$$

These operations are well defined, thanks to I being an ideal. Quotient rings are rings. Another important point is that when the ideal I is maximal, the quotient ring R/I is a field (which will be defined later).

Remark. It is common to just write $r + I$ as r when the context is clear.

Example. $\mathbb{Z}/2\mathbb{Z}$ is a quotient ring which contains two elements.

We introduce a common way to produce a larger ring based on a given ring, which will serve as the first step to get the rational function field.

Definition (polynomial ring)**.** A polynomial over a ring R is a formal sum

$$a_0 + a_1 x + \ldots + a_n x^n$$

where x is a formal symbol, $n \in \mathbb{N}$ and $a_i \in R$ for all $i = 0, 1, \ldots, n$. The set of all polynomials over R is denoted as $R[x]$. In fact, $R[x]$ is a ring with the usual addition and multiplication.

The degree of a polynomial $f \in R[x]$ is equal to the maximal natural number n with $a_n \neq 0$, which is denoted as $\deg f$. A simple result is that for any $f, g \in R[x]$, $\deg fg = \deg f + \deg g$.

Example. $\mathrm{M}(n, \mathbb{R})[x]$ is a polynomial ring.

For example, $\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} x + \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} x^2 \in \mathrm{M}(2, \mathbb{R})[x]$.

Rings can be complicated, but here we mostly care about commutative rings with multiplicative identity. Thus we assume R is a ring having such properties by default from now on.

It is useful to have the notion of divisors and, units the notion of irreducibility.

Definition (divisor)**.** Let $a, b \in R$ with $a \neq 0$. We say $a \mid b$ if there exists some $x \in R$ such that $ax = b$.

Example. In the ring $\mathbb{Z}[x]$, $1 - x \mid 1 - x^2$, since $(1 - x)(1 + x) = 1 - x^2$.

Definition (unit)**.** An element $x \in R$ is called a unit if it has an multiplicative inverse in R. The set of units is denoted as $R^\times$.

Definition (irreducibility)**.** Let $a \in R$. We say a is irreducible if for any $x, y \in R$, $xy = a$ implies at least one of x, y is a unit.

Example. In the ring $\mathbb{Z}[x]$, $1 - x$ is irreducible.

2.3 Vector Spaces

The *Riemann-Roch space* is a vector space over some field and the dimension of the Riemann-Roch space is critical in the estimates of the parameters of the algebraic geometry codes. We have to know what a vector space is and how its dimension is defined in a general case.

Definition (vector space)**.** Let $(V, +)$ be an abelian group and F be a field that acts on V (each $x \in F$ maps each $v \in V$ to $xv \in V$). We call $(V, +)$ is a vector space over F if for all $x, y \in F$ and $u, v \in V$,

- $(x + y)u = xu + yu$.
- $x(yu) = (xy)u$.
- $x(u + v) = xu + xv$.

Example. $\mathrm{M}(n, \mathbb{R})$ is a vector space over $\mathbb{R}$ if we just define that $\mathbb{R}$ acts on $\mathrm{M}(n, \mathbb{R})$ by entry-wise scalar multiplication.

We want to define the *dimension* of a vector space, which requres the following series of definitions.

Definition (linear independence)**.** Let V be a vector space over F. We say a subset $S \subset V$ is a set of linearly independent elements if for any $n \in \mathbb{N}$, for all $i \in [n]$, $\alpha_i \in F$ and $v_i \in V$,

$$\sum_{i=1}^{n} \alpha_i v_i = 0 \implies \alpha_i = 0, \ \forall i \in [n]$$

Example. The set $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \pi & 0 \\ 0 & \pi \end{pmatrix} \right\}$ is a set of linearly independent elements in the vector space $\mathrm{M}(2, \mathbb{R})$ over $\mathbb{Q}$. It is not linearly independent in the vector space $\mathrm{M}(2, \mathbb{R})$ over $\mathbb{R}$.

Definition (linear subspace)**.** Let V be a vector space over F. A subset $U \subset V$ is a linear subspace if U is itself a vector space over F with the restricted operations.

Example. Let $\mathrm{M}(n, \mathbb{Q})$ be the set of $n \times n$ matrices with entries in $\mathbb{Q}$. Then $\mathrm{M}(n, \mathbb{Q})$ is a linear subspace of the vector space $\mathrm{M}(n, \mathbb{R})$ over $\mathbb{Q}$.

Definition (span)**.** Let V be a vector space over F and $S \subset V$. We define the span of S is the smallest linear subspace of V that contains S.

This definition makes sense since the intersection of two subspaces is also a subspace.

Example. Consider the vector space $\mathrm{M}(2, \mathbb{R})$ over $\mathbb{Q}$. The span of $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \pi & 0 \\ 0 & \pi \end{pmatrix} \right\}$ is equal to the set $\{(a + b\pi)\mathrm{id} \mid a, b \in \mathbb{Q}\}$, where id is the identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Definition (basis)**.** Let V be a vector space over F. If a subset $S \subset V$ is linearly independent and spans the whole space V, we call S a set of basis of V.

Example. $\left\{\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\1 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}\right\}$ is a basis of the vector space $\mathrm{M}(2,\mathbb{R})$ over $\mathbb{R}$.

Definition (dimension)**.** Let V be a vector space over F. If there exists some finite subset $S \subset V$ that is a basis, then the dimension of V is defined to be the size of the set S. Otherwise, the dimension is defined to be ∞.

This is well-defined, since any two finite basis have the same size- a result from linear algebra.

Example. The vector space $\mathrm{M}(2,\mathbb{R})$ over $\mathbb{R}$ have dimension of 4. The vector space $\mathrm{M}(2,\mathbb{R})$ over $\mathbb{Q}$ have dimension of ∞.

2.4 Fields

We need to know what a *field* is and what *field extension* is *algebraic*.

Definition (field and its multiplicative group)**.** A field F is a commutative ring with multiplicative identity and each nonzero element of F has an inverse. $F^\times = F - \{0\}$ is the multiplicative group where the group operation is just the multiplication in F, which is abelian by the definition.

Example. $\mathbb{Q}$ is a field. $\mathbb{Q} - \{0\}$ is its multiplicative group.

Definition (subfield and field extension)**.** Let K be a field and $F \subset K$. If F is also a field with the restricted operations, then F is called a subfield of K and K is called an extension of F, denoted as K/F.

Example. $\mathbb{Q}$ is a subfield of $\mathbb{R}$. $\mathbb{R}/\mathbb{Q}$ is a field extension.

Definition (generated field)**.** Let K/F be a field extension and $x \in K$. Then the field generated by x is the smallest subfield of K containing both x and F, denoted as $F(x)$.

This is well-defined since the intersection of two subfields is again a subfield.

Example. $\mathbb{R}/\mathbb{Q}$ is a field extension and $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a field generated by $\sqrt{2}\mathbb{R}$.

Definition (degree of a field extension)**.** Let K/F be a field extension. The degree of K/F is equal to the dimension of the vector space K over F, denoted as $[K : F]$.

F acts on K just by multiplication. One can be easily verified that this action constitutes a vector space K over F.

Example. $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, since $\{1, \sqrt{2}\}$ is a basis of the vector space $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.

Definition (algebraic element and extension)**.** Let K/F be a field extension. An element $x \in K$ is called algebraic over F if there exists some polynomial $f \in F[x]$ such that $f(x) = 0$. Elements that are not algebraic over F are called transcendental over F.

The field extension K/F is called algebraic if for all $x \in K$, x is algebraic over F.

Remark. An important result from the field theory to keep in mind is that all extensions of finite degrees are algebraic.

Example. $x = \sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ since $x^2 - 2 = 0$. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is an algebraic extension.

$\pi \in \mathbb{R}$ is transcedental over $\mathbb{Q}$ and, by the definition, $\mathbb{Q}(\pi)/\mathbb{Q}$ is not an algebraic extension.

Finally, we introduce a common way to extend a polynomial ring to a field.

Definition (field of rational functions)**.** Let K be a field. We define

$$K(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], g(x) \neq 0 \right\}$$

to be the rational function field over K. The operations are defined in the usual way.

Remark. Previously we have defined $K(x)$ to be the field generated by x over K and here we define $K(x)$ to be the rational function field over K. This is definitely an abuse of notation. However, in fact, when x is transcendental over K, the generated field and the rational function field are isomorphic, e.g. by the map $\phi : K(x) \to K(\pi)$, where

$$\phi(f(x)) = f(\pi).$$

Thus when x is transcendental over K, this abuse works.

Example. $\frac{x}{1+x} \in \mathbb{Q}(x)$.

3 Foundations of Algebraic Function Fields

Now we have enough definitions from the basic abstract algebra. We can define what an algebraic function field is and also define the related notions of it. For a better understanding, while defining the notions in algebraic function fields, we give a series of examples that choose $F = K(x)$ to be the rational function field over K.

3.1 Algebraic Function Fields

Definition (algebraic function field)**.** A field extension F/K is called an *algebraic function field* if there exists some $x \in F$ that is transcendental over K and $[F : K(x)] < \infty$.

Remark. The name "algebraic function field" makes lots of sense- it is just an algebraic extension (since the extension degree is finite) of some rational function field.

Example. $\mathbb{Q}(\pi)/\mathbb{Q}$ is an algebraic function field (in fact it is isomorphic to the rational function field over $\mathbb{Q}$). $\mathbb{Q}(\pi, \sqrt{2})/\mathbb{Q}$ is an algebraic function field. However, $\mathbb{Q}(\pi, e)/\mathbb{Q}$ is not an algebraic function field.

When F is $K(x)$, the elements can be easily written in a fraction form $\frac{f(x)}{g(x)}$, which gives a clear way to construct a function with specific zeros and poles of specific orders. However, in general an algebraic function field F is way more complex than the rational function field $K(x)$. In order to construct elements with specific zeros and poles of specific orders in a general case, we need to know the notions of valuation rings and places.

3.2 Valuation Rings and Places

Definition (valuation ring)**.** Let F/K be an algebraic function field. A subring $\mathcal{O} \subset F$ is called a valuation ring if

- $K \subsetneq \mathcal{O} \subsetneq F$, and
- for all $z \in F$, we have $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

Example. Let $\alpha \in K$, we define

$$\mathcal{O}_\alpha = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], (x-\alpha) \nmid g(x) \right\}$$

and

$$\mathcal{O}_\infty = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], \deg f \leq \deg g \right\}.$$

Claim. For any $\alpha \in K$, both $\mathcal{O}_\alpha$ and $\mathcal{O}_\infty$ are valid valuation rings of the algebraic function field $K(x)$.

Proof Sketch. Indeed, for any $\frac{f}{g}, \frac{f'}{g'} \in \mathcal{O}_\alpha$, we have $(x-\alpha) \nmid g, g'$. Thus $(x-\alpha) \nmid gg'$ since $(x-\alpha)$ is irreducible in $K[x]$. Thus $\frac{f}{g} \cdot \frac{f'}{g'} = \frac{ff'}{gg'}$ and $\frac{f}{g} + \frac{f'}{g'} = \frac{fg'+f'g}{gg'}$ are both still in $\mathcal{O}_\alpha$. In addition, for any $\frac{f}{g} \in R[x]$, after cancelling, at least one of f, g have no factor $(x-\alpha)$. We see $\mathcal{O}_\alpha$ is a valuation ring.

For any $\frac{f}{g}, \frac{f'}{g'} \in \mathcal{O}_\infty$, we have $\deg ff' = \deg f + \deg f' \leq \deg g + \deg g' = \deg gg'$ and similarly $\deg fg', \deg f'g \leq \deg gg'$. Thus $\mathcal{O}_\infty$ are closed under addition and multiplication. In addition, for any $\frac{f}{g}$, if $\deg f \leq \deg g$, then it is in $\mathcal{O}_\infty$; if $\deg f > \deg g$ then its inverse $\frac{g}{f}$ is in $\mathcal{O}_\infty$. We see $\mathcal{O}_\infty$ is also a valuation ring. □

Next, we define the places of an algebraic function field.

Definition (place)**.** Let F/K be an algebraic function field, P is a place if there exists some valuation ring $\mathcal{O} \subsetneq F$ such that $P = \mathcal{O} \setminus \mathcal{O}^\times$.

Claim. Let P be a place of F/K. There is a unique valuation ring $\mathcal{O}$ such that $P = \mathcal{O} \setminus \mathcal{O}^\times$.

Proof. Let $\mathcal{O}$ be any valuation ring such that $P = \mathcal{O} \setminus \mathcal{O}^\times$.

First we must have $0 \in \mathcal{O}$ since it is a subring.

For any $0 \neq x \in F$, if $x^{-1} \in P$, then by the definition of P, $x \notin \mathcal{O}$; if $x^{-1} \notin P$ we must have both x and x^{-1} in $\mathcal{O}$ and therefore we have $x \in \mathcal{O}$.

We see that the valuation ring $\mathcal{O}$ can be identified by the set $\{x \mid x^{-1} \notin P\}$. □

Having this, it makes sense to first have a place P, then refer to its valuation ring $\mathcal{O}_P$.

Claim. Let P be a place of F/K. P is a maximal ideal of $\mathcal{O}_P$.

Proof. For any $o \in \mathcal{O}_P$ and $p \in P$, if we have $op \in \mathcal{O}_P^\times$, then we must have some $w \in \mathcal{O}_P$ such that $opw = 1$, which implies p is a unit, contradicting the fact that $p \in P$. Thus we must have $op \in P$.

Let $a, b \in P$, if $ab \notin P$, then there exists some $w \in \mathcal{O}_P$ such that $abw = 1$, which contradicts the fact that $a, b \in P$. Similarly if $a + b \notin P$, without loss of generality we assume $\frac{a}{b} \in \mathcal{O}_P$, then $a + b = (1 + \frac{a}{b})b \in P$ since $b \in P$. Thus P is subring.

Note that any larger ideal will have a unit which will force it to be the whole ring $\mathcal{O}_P$. We conclude that P is a maximal ideal. □

We give an important theorem without proof.

Theorem 1. *Let P be a place. There exists some $t \in P$ so that for any $0 \neq z \in F$, there exists a unique pair of $n \in \mathbb{Z}$ and $u \in \mathcal{O}^\times$ such that $z = t^n u$. The value of n is independent from the choice of t.*

This theorem gives a map, parametrized by places, that maps F to $\mathbb{Z}$.

Definition (discrete valuation)**.** Let P be a place. The function $v_P : F \to \mathbb{Z}$ maps z to n such that $z = t^n u$ where t and u are specified as the previous theorem, is called a discrete valuation of F/K.

These maps have very nice properties.

Claim. Let P be a place and $v = v_P$, then for any $x, y \in F$

- $v(xy) = v(x) + v(y)$.
- $v(x + y) \geq \min\{v(x), v(y)\}$.
- $v(x + y) = \min\{v(x), v(y)\}$ if $v(x) \neq v(y)$.

Secondly, it also gives a characterization of $\mathcal{O}_P$ and P.

- $\mathcal{O}_P = \{x \in F \mid v_P(x) \geq 0\}$;
- $P = \{x \in F \mid v_P(x) > 0\}$.

We can define zeros and poles in a general sense based on the discrete valutations

Definition (zeros and poles)**.** Let P be a place and $z \in F$, we say z is a zero if $v_P(z) > 0$; we say z is a pole if $v_P(z) < 0$.

Example. Let $\alpha \in K$, we define

$$P_\alpha = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], (x - \alpha) \mid f(x), (x - \alpha) \nmid g(x) \right\}$$

and

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], \deg f < \deg g \right\}.$$

Clearly we have $P_\alpha = \mathcal{O}_\alpha \setminus \mathcal{O}_\alpha^\times$ and $P_\infty = \mathcal{O}_\infty \setminus \mathcal{O}_\infty^\times$.

Additionally, for any $\frac{f}{g} \in K(x)$, we have $v_{P_\alpha}\left(\frac{f}{g}\right)$ equal to the order of the factor $(x - \alpha)$ and $v_{P_\infty}\left(\frac{f}{g}\right) = \deg g - \deg f$. One can easily check that these two discrete valuations satisfy the previous claim.

Finally, we see for the P_αs, the generalized definitions of zeros and poles conform with the elementary definitions of zeros and poles.

3.3 Residue Class Field of Places

In the previous subsection, we proved that P is a maximal ideal of $\mathcal{O}_P$. Thus the quotient ring $\mathcal{O}_P/P$ is in fact a field.

Definition (residue class field and map)**.** Let P be a place. We define $F_P = \mathcal{O}_P/P$ to be the residue class field of P. The map $x \mapsto x + P$ is the residue class field.

Note that by the definition of valuation ring, we have $K \subset \mathcal{O}_P$. Also, since K is a field, thus different $x, y \in K$ will be mapped to different residue classes because $x - y$ has an inverse in K. Therefore, we can embed K to any residue class field, which makes the following definition sensible.

Definition (degree of places)**.** We define the degree of a place to be $\deg P = [F_P : K]$. Here K is identified by its embedding in F_P.

The degree of places are bounded by the following proposition.

Proposition 1. *Let P be a place, and $0 \neq x \in P$ then*

$$\deg P \leq [F : K(x)] < \infty.$$

Example. For any $\alpha \in K$, one can identify the residue class field F_{P_α} can be identified by K through the map

$$\phi : F_{P_\alpha} \to K, \quad \phi\left(\frac{f}{g} + P\right) = \frac{f(\alpha)}{g(\alpha)}.$$

This can be sort of predicted by the previous proposition, since we must have $\deg P = [F_P : K] \leq [K(x) : K(x)] = 1$.

3.4 Divisors

By the weak approximation theorem (see [2]), one can deduce that every element $z \in F$ has only finitely many zeros and poles. This pushes us to define a structure to record the assignments of zeros and poles.

Definition (divisor)**.** Let S be a finite set of places, a divisor D with support S is defined as a formal sum

$$D = \sum_{P \in S} n_P P$$

with $n_P \in \mathbb{Z}$. The space of all possible divisors form the divisor group $\mathrm{Div}(F/K)$, the operation is defined by the component-wise addition.

Now since all element $z \in F$ has only finitely many zeros and poles, it is natural to have the following definition.

Definition (principal divisor)**.** Let $z \in F$, we define the divisor $(z) \in \mathrm{Div}(F)$ as the formal sum

$$\sum_{P \in S} v_P(z) P,$$

where S is a finite set containing all places P such that $v_P(z) \neq 0$. If a divisor D can be written in the form (z) of some $z \in F$, we call D a principal divisor.

The principal divisors are special, which can be seen from the quantity defined as follows.

Definition (degree of a divisor)**.** Let $D = \sum_{P \in S} n_P P$ where S is some finite set of places. The degree of the divisor D is defined as

$$\deg D = \sum_{P \in S} n_P.$$

The degree of all principal divisors are zero, and later on we will see in some cases, all divisors with degree zero are principle.

Example. This can be verified in the rational function field $\mathbb{C}(x)/\mathbb{C}$. Since $\mathbb{C}$ is algebraically closed, one can prove that the only places are P_α and P_∞ for $\alpha \in \mathbb{C}$. Now for any $\frac{f}{g} \in \mathbb{C}(x)$, we can evaluate the degree of the corresponding principal divisor.

$$\begin{aligned}\deg\left(\frac{f}{g}\right) &= \sum_{\text{zeros}} \text{multiplicity of the zero} - \sum_{\text{poles}} \text{multiplicity of the pole} + v_\infty(f/g) \\ &= \deg f - \deg g + (\deg g - \deg f) \\ &= 0\end{aligned}$$

3.5 Riemann-Roch Spaces

Let A, B be two divisors, we say $A \leq B$ if for all places P, we have $n_{PA} \leq n_{PB}$.

Definition (Riemann-Roch Spaces)**.** Let A be a divisor, we define the Riemann-Roch space associated to A to be

$$\mathscr{L}(A) = \{x \in F \mid (x) + A \geq 0\} \cup \{0\}.$$

It looks a little bit abstract though, it has the following equivalent interpretation. The Riemann-Roch space $\mathscr{L}(A)$ associated to a divisor A is the set of all $z \in F$ such that

- z may only have poles at a place P such that $n_{PA} > 0$ and the degree $v_P(z)$ is bounded by n_{PA}.
- z must have zeros at places P such that $n_{PA} < 0$ and the degree $v_P(z)$ at least $-n_{PA}$.

Thus a divisor can be seen as a filter of the space F. In fact, every Riemann-Roch space $\mathscr{L}(A)$ is a vector space over K with finite dimension.

Definition (dimension of divisors)**.** Let A be a divisor. We define the dimension of the divisor A to be $\ell(A) = \dim \mathscr{L}(A)$ over K.

3.6 Genus

One nicest result is that, the dimension of divisors can be estimated by the following result.

$$\deg A - \gamma \leq \ell(A) \leq \deg A + 1,$$

where γ is a constant that depends only on the function field F/K.

Thus naturally, we define the most important invariant of a function field- genus.

Definition (genus)**.** The genus g of F/K is defined by

$$g = \max\{\deg A - \ell(A) + 1 \mid A \in \mathrm{Div}(F)\}.$$

Just by the definition of genus, we have $\ell(A) \geq \deg A + 1 - g$.

4 Algebraic Geometry Code

Now, though some of the proofs are skipped, we have been familiar with all the notions that are needed to understand the definition of a general algebraic geometry code.

Definition (algebraic geometry code)**.** Let

- $\mathbb{F}_q$ be a finite field;
- $F/\mathbb{F}_q$ be an algebraic function field of genus g;
- $D = P_1 + \ldots + P_n$ be a divisor of F, where P_is is distinct places of degree 1, i.e. $[\mathcal{O}_{P_i}/P_i : \mathbb{F}_q] = 1$;
- G be a divisor of F and for every place P_i we have $n_{P_i G} = 0$.

The algebraic geometry code $C_{\mathscr{L}}(D, G)$ is defined as

$$C_{\mathscr{L}}(D, G) = \{(x + P_1, x + P_2, \ldots, x + P_n) \mid x \in \mathscr{L}(G)\}.$$

Note that for each $i \in [n]$, since $n_{P_i G} = 0$, we must have $v_{P_i}(x) \geq 0$, which implies $x \in \mathcal{O}_{P_i}$. Thus $x + P_i$ is some residue class in the residue class field F_{P_i}. Since $[F_{P_i} : K] = 1$, we can identify each residue class in F_{P_i} by some unique element in $\mathbb{F}_q$. By this identification, we can consider the set $C_{\mathscr{L}}(D, G)$ as a subset of $\mathbb{F}_q^n$.

A direct application of the results from the algebraic function fields yield the following theorem about the estimates of the parameters of algebraic geometry codes.

Theorem 2. *$C_{\mathscr{L}}(D, G)$ is an $[n, k, d]$ code where k is the dimension of the code and d is the minimum distance* $\min\{wgt(z) \mid z \in C_{\mathscr{L}}(D, G)\}$*. $wgt(\cdot)$ is just equal to the number of nonzero entries (Hamming weight). We have the following estimates.*

$$k = \ell(G) - \ell(G - D)$$

and

$$d \geq n - \deg G.$$

The estimate is used for general algebraic geometry codes. The following claim gives a sharper estimate when the code have specific properties.

Claim. If $2g - 2 < \deg G < n$, then $k = \deg G + 1 - g$.

5 Rational Algebraic Geometry Code

When $F = \mathbb{F}_q(x)$ be a rational function field extension of $\mathbb{F}_q$, the resulted code is called the rational algebraic geometry code. Additionally, we assume that $n > \deg G \geq 0$. Note that all rational function field has genus 0. Thus we have $k = \deg G + 1$.

Rational algebraic geometry code only have places of degree 1, according to the previous proposition in Section 3.3. This makes it special. Specifically, we have the following results from the algebraic function field theory.

Claim. If A is a divisor of degree at least 0 of a rational function field F/K, then

$$\ell(A) = \deg A + 1$$

and A is principal, i.e. there exists some $z \in F$ such that $A = (z)$.

This claim gives a strong guarantee in two aspects:

- Whenever a divisor A has degree at least 0, the dimension of the Riemann-Roch space associated with divisor A can be accurately determinied by the degree of the divisor A.
- Whenever a divisor A has degree at least 0, there exists some $z \in F$ such that $A = (z)$.

We can play with divisors happily with these two guarantees. In fact, we can prove that all rational algebraic geometry code has a specific form that is similar with Reed-Solomon code.

Theorem 3. *Let $C_{\mathscr{L}}(D, G)$ be a $[n, k, d]$ code. If $n \leq q$ then there exist distinct element $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ and some $v_1, \ldots, v_n \in \mathbb{F}_q^\times$ such that*

$$C_{\mathscr{L}}(D, G) = \{(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)) \mid f \in \mathbb{F}_q[z], \deg f \leq k - 1\}.$$

Proof. Since $n \leq q$ (note that there are $q + 1$ places- q of them in the form of P_α with $\alpha \in \mathbb{F}_q$ and one P_∞), we can choose a pair (Q, P) where Q is different from all P_is and P is some P_i. Then by the previous claim, we must have some $z \in \mathbb{F}_q(x)$ such that $P - Q = (z)$.

Note that by assumption we have $\deg G = k - 1 \geq 0$. We construct another divisor $(k-1)Q - G$ which has degree zero. Then there exists some $u \in F$ such that $(k-1)Q - G = (u)$. Thus for any $i = 0, \ldots, k-1$, we have $(z^i u) + G = i(z) + (u) + G = iP - iQ + (k-1)Q - G + G = iP + (k-1-i)Q \geq 0$, which implies $z^i u \in \mathscr{L}(G)$. In addition, since z is transcendental over $\mathbb{F}_q$ (otherwise z must have a zero divisor), $(u, zu, \ldots, z^{k-1}u)$ must be linearly independent over $\mathbb{F}_q$.

Note that, by the claim, since we assume $\deg G \geq 0$, we have $\ell(G) = \deg G + 1 = k$. Thus $(u, zu, \ldots, z^{k-1}u)$ is a basis of $\mathscr{L}(G)$. Thus any $x \in \mathscr{L}(G)$ can be written as $uf(z)$ where $f \in \mathbb{F}_q[x]$ with $\deg f \leq k - 1$.

Now insert what we have to the definition of algebraic geometry code, we have

$$C_{\mathscr{L}}(D, G) = \{(u(P_1)f(z(P_1)), u(P_2)f(z(P_2)), \ldots, u(P_n)f(z(P_n))) \mid f \in \mathbb{F}_q[z], \deg f \leq k - 1\}.$$

Note that $u(P_i) \neq P_i$ because we have $(u) = (k-1)Q - G$ which does not have P_i in its support, i.e. $v_{P_i}(u) = 0$, which implies $u \in \mathcal{O}_{P_i}^\times$. Therefore the residue class of u is not the residue class identified by 0. This completes the whole proof. □

We define the code in that form as the generalized Reed-Solomon code.

Definition (generalized Reed-Solomon code)**.** Let $n \leq q$. For any distinct element $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ and any $v_1, \ldots, v_n \in \mathbb{F}_q^\times$, we define the corresponding generalized Reed-Solomon code to be

$$C_{\mathscr{L}}(D, G) = \{(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)) \mid f \in \mathbb{F}_q[z], \deg f \leq k-1\}.$$

Finally, we prove the converse is also true, i.e.,

Claim. Every generalized Reed-Solomon code can be written as a rational algebraic geometry code.

Proof. We can use the Langrange interpolation to find an element $u \in \mathbb{F}_q(x)$ such that $u(P_{\alpha_i}) = u(\alpha_i) = v_i$. Then let $D = P_{\alpha_1} + \ldots + P_{\alpha_n}$ and $G = (k-1)P_\infty - (u)$. We have for an $z \in \mathscr{L}(G)$, by the definition, we know

- z cannot have any factor in its denominator and can be at most of $k-1$ degree in its nominator;
- z must have zeros of at the zeros of u and have at least the same degree with u at each zero.

Thus we can write z as uf where $f \in \mathbb{F}_q[x]$ with $\deg f \leq k-1$.

Finally, note that for rational function field, $z \in \mathbb{F}_q(x)$ is identified by $z(\alpha_i)$ in the residue class field $\mathbb{F}_q(x)_{P_{\alpha_i}}$. Thus we have $z + P_i$ identified by $z(\alpha_i) = u(\alpha_i)f(\alpha_i) = v_i f(\alpha_i)$. This completes the proof. □

According to the algebraic function field theory, we have $d = n - \deg G$. Thus $k + d = n - \deg G + \deg G + 1 = n + 1$ which reaches the Singleton bound. Thus rational algebraic geometry code is MDS, and so is generalized Reed-Solomon code, since they are equivalent.

6 Conclusion

Throughout this report, we first focus on explaining the notions that constructs the algebraic geometry code. Then we define it and state some results on the estimates of parameters. Finally, we show that rational algebraic geometry code is equivalent to the generalized Reed-Solomon code.

References

[1] David Steven Dummit and Richard M Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.

[2] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer Science & Business Media, 2009.