Goppa Codes

Unit 12

Gil Cohen

December 7, 2024

Overview

1. Overview
2. Goppa Codes
3. Reed-Solomon Revisited
4. Where to now?

Rational places

Definition 1

Let F/K be a function field. A prime divisor $\mathfrak{p} \in \mathbb{P}$ of degree 1 is called a rational prime divisor or a rational place.

The place associated with a prime divisor $\mathfrak{p}$ is of the form

$$\varphi_{\mathfrak{p}} : \mathsf{F} \to \mathsf{K} \cup \{\infty\}.$$

For $f \in \mathsf{F}$ we write $f(\mathfrak{p})$ for $\varphi_{\mathfrak{p}}(f)$ to be suggestive regarding our intuition of $\varphi_{\mathfrak{p}}$ being an evaluation of the given function f at $\mathfrak{p}$.

Goppa Codes

Definition 2 (Goppa Codes)

Let F/K be a function field, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathbb{P}$ rational. Let $\mathfrak{a} \in \mathcal{D}$ s.t.

$$\forall i \in [n] \quad \upsilon_{\mathfrak{p}_i}(\mathfrak{a}) = 0.$$

Define

$$C = \{(f(\mathfrak{p}_1), \ldots, f(\mathfrak{p}_n)) \mid f \in \mathcal{L}(\mathfrak{a})\} \subseteq \mathrm{K}^n.$$

We will consider the special case in which $\mathfrak{p}_0 \in \mathcal{D}$ is rational, $\mathfrak{p}_0 \neq \mathfrak{p}_i$ for $i \geq 1$, and $\mathfrak{a} = r\mathfrak{p}_0$ for some $r < n$.

Theorem 3

C is a linear code of dimension $\geq r - g + 1$ having distance $\geq n - r$. In particular,

$$\rho + \delta \geq 1 - \frac{g-1}{n}.$$

Goppa Codes

Proof.

First note that C is well-defined. Indeed,

$$\begin{aligned} f \in \mathcal{L}(r\mathfrak{p}_0) \quad &\Longrightarrow \quad \forall i \in [n] \quad \upsilon_{\mathfrak{p}_i}(f) \geq 0 \\ &\Longrightarrow \quad f(\mathfrak{p}_i) = \varphi_{\mathfrak{p}_i}(f) \in \mathrm{K} \setminus \{\infty\}. \end{aligned}$$

That C is K-linear follows since for $f, g \in \mathcal{L}(r\mathfrak{p}_0)$,

$$\begin{aligned} f(\mathfrak{p}_i) + g(\mathfrak{p}_i) &= \varphi_{\mathfrak{p}_i}(f) + \varphi_{\mathfrak{p}_i}(g) \\ &= \varphi_{\mathfrak{p}_i}(f+g) \\ &= (f+g)(\mathfrak{p}_i), \end{aligned}$$

and $f + g \in \mathcal{L}(r\mathfrak{p}_0)$. Moreover, for $a \in \mathrm{K} \subseteq \mathcal{O}_{\mathfrak{p}_i}$,

$$\begin{aligned} a \cdot f(\mathfrak{p}_i) = a \cdot \varphi_{\mathfrak{p}_i}(f) = a \cdot (f + \mathfrak{m}_{\mathfrak{p}_i}) = af + \mathfrak{m}_{\mathfrak{p}_i} \\ = \varphi_{\mathfrak{p}_i}(af) = (af)(\mathfrak{p}_i). \end{aligned}$$

Goppa Codes

Proof.

Distance analysis.

Take $0 \neq f \in \mathcal{L}(r\mathfrak{p}_0)$ and let $\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_z}$ be the zeros of f. Then,

$$f \in \mathcal{L}(\mathfrak{a}),$$

where

$$\mathfrak{a} = r\mathfrak{p}_0 - \mathfrak{p}_{i_1} - \cdots - \mathfrak{p}_{i_z}.$$

Recall that for every $\mathfrak{b} \in \mathcal{D}$,

$$\deg \mathfrak{b} < 0 \quad \Longrightarrow \quad \dim \mathfrak{b} = 0.$$

Since $0 \neq f \in \mathcal{L}(\mathfrak{a})$ we get $\dim \mathfrak{a} > 0$, and so

$$r - z = \deg \mathfrak{a} \geq 0.$$

Thus, $z \leq r$, and so the distance $\geq n - r$.

Proof.

Rate analysis.

As $r < n$, the distance analysis in particular implies that

$$\dim C = \dim(r\mathfrak{p}_0).$$

By Riemann's Theorem,

$$\begin{aligned}\dim(r\mathfrak{p}_0) &\geq \deg(r\mathfrak{p}_0) - g + 1 \\ &= r - g + 1,\end{aligned}$$

completing the proof. □

Overview

1. Overview
2. Goppa Codes
3. Reed-Solomon Revisited
4. Where to now?

Reed-Solomon Revisited

Consider the rational function field $\mathsf{F}/\mathsf{K} = \mathbb{F}_q(x)/\mathbb{F}_q$.

We showed that for every $\alpha \in \mathbb{F}_q$ there is a rational place $\mathfrak{p}_\alpha$.

Moreover, there is the additional rational place $\mathfrak{p}_\infty$, and $\mathcal{L}(r\mathfrak{p}_\infty)$ consists of all polynomials of degree $\leq r$.

RS is thus a Goppa code, obtained by working with the rational function field.

Overview

1. Overview
2. Goppa Codes
3. Reed-Solomon Revisited
4. Where to now?

Where to now?

In light of the Theorem 3, for a given prime power q we would like to find a function field that minimizes the quantity

$$\frac{g}{n} = \frac{\text{genus}}{\text{number of rational points}}.$$

This turns out to be an extremely deep problem.

The Hasse-Weil bound (1948), which is essentially equivalent to the validity of Riemann's Hypothesis for function fields, yields (for all $g \geq 1$)

$$\frac{g}{n} \geq \frac{1}{2\sqrt{q}}.$$

Drinfeld and Vladhut (1983), based on ideas by Ihara, sharpened this bound to

$$\frac{g}{n} \geq \frac{1}{\sqrt{q}-1}.$$

Where to now?

Remarkably, the Drinfeld-Vladut bound is tight! (at least for $q = p^{2m}$).

Ihara and independently Tsfasman-Vladut-Zink (1982) proved the existence of function fields (with field of constant $\mathbb{F}_q$) with

$$\frac{g}{n} \leq \frac{1}{\sqrt{q} - 1}.$$

Their argument is non-explicit and is based on modular curves.

The first explicit construction was obtained by Garcia and Stichtenoth (1995). Their proof is based on a construction of tower of a carefully chosen function field.

Most of the course from this point on is devoted to the study of function field extensions. But first we will prove a major result - the Riemann-Roch Theorem.