Goppa Codes

Gil Cohen

June 10, 2019

Without further ado

Definition

Let $L/\mathbb{F}_q$ be a function field associated to a nonsingular complete curve X with rational points $P_0, \ldots, P_n$. Let $r \geq 0$ be a parameter. We define the Goppa code

$$\mathcal{C} = \{(\alpha(P_1), \ldots, \alpha(P_n)) \mid \alpha \in \mathcal{L}(rP_0)\} \subseteq \mathbb{F}_q^n.$$

Theorem

Let g be the genus of X. Then, $\mathcal{C}$ is a linear code of dimension (at least) $k = r - g + 1$ and distance (at least) $n - r$. In particular,

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

where ρ, δ are the rate and relative distance, respectively.

Proof.

First observe that $\mathcal{C}$ is well-defined. Indeed, α has poles only at P_0 and so it is well-defined at $P_1, \ldots, P_n$. Furthermore, as $P_1, \ldots, P_n$ are rational points, $\alpha(P_i) \in K_{P_i} \cong \mathbb{F}_q$. Linearity follows since $\alpha(P_i) + \beta(P_i) = (\alpha + \beta)(P_i)$.

Distance analysis. Take $0 \neq \alpha \in \mathcal{L}(rP_0)$. Assume $P_{i_1}, \ldots, P_{i_z}$ are zeros of α. Then,

$$\alpha \in \mathcal{L}\left(rP_0 - (P_{i_1} + \cdots + P_{i_z})\right)$$

Thus, $\ell\left(rP_0 - (P_{i_1} + \cdots + P_{i_z})\right) > 0$ and so

$$r - z = \deg\left(rP_0 - (P_{i_1} + \cdots + P_{i_z})\right) \geq 0.$$

Thus, $z \leq r$ implying that the distance of $\mathcal{C}$ is at least $n - r$.

Rate analysis. The assertion regarding $k = \dim \mathcal{C}$ follows by Riemann's Theorem. □

Discussion

Let $L/\mathbb{F}_q$ be a function field associated to a nonsingular complete curve X. Let g be the genus of X and n the number of rational points on X.

In light of the theorem above, for a given prime power q we would like to find a nonsingular complete curve X that minimizes the quantity g/n.

This turns out to be an extremely deep problem.

Discussion

The Hasse-Weil bound (1948) which is equivalent to the validity of Riemann's Hypothesis for the Zeta function associated to the curve gives

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

This can be sharpened further based on ideas by Ihara.

Theorem (Drinfeld-Vladut (1983))

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

Discussion

Remarkably, the Drinfeld-Vladut bound is tight!

Ihara and independently Tsfasman-Vladut-Zink (1982) proved the existence of curves with such g/n ratio based on modular curves (at least for every q which is an even power of a prime). The proofs are non-explicit however.

The first explicit construction was obtained by Garcia-Stichtenoth (1995). Much of the next course will be about their as well as other constructions.