1 Goppa Codes

Goppa Codes are constructed by using **curves over finite fields**.

We recall what a curve is:

$\mathbb{F}_q$ is the finite field with $q = p^n$ elements.

A curve over $\mathbb{F}_q$ is a pair $\Gamma = (F/\mathbb{F}_q, \mathfrak{M})$, where $F/\mathbb{F}_q$ is a **function field** of one variable, i.e.

1) $F/\mathbb{F}_q$ is a finitely generated field extension

2) $\mathrm{tr}\,(F/\mathbb{F}_q) = 1$

3) $\mathbb{F}_q$ is algebraically closed in F.

$\mathfrak{M} = \mathfrak{M}(F)$ is the set of **valuation rings** of $F/\mathbb{F}_q$, sometimes called the **abstract Riemann surface** of $F/\mathbb{F}_q$. The elements of $\mathfrak{M}$ are called **points** or **places** and denoted by $P = (R_P, m_P)$, where R_P is the **valuation ring** and $m_P = (t_P) = t_P \cdot R_P$ is the maximal ideal of R_P.

Recall: A **valuation ring R** of $F/\mathbb{F}_q$ is a ring with special properties. One of them is: If $x \in F$, then $x \in R$ or $\frac{1}{x} \in R$.

The **valuation** v_P, to $P = (R_P, m_P)$ is defined as follows. If $x \in R_P, x \neq 0$, we write $x = t_P^n \cdot u$, u a unit in R_P and define

$$v_P(x) = n.$$

If $x \notin R_P$, we have $\frac{1}{x} \in R_P$ and write $\frac{1}{x} = t_P^n \cdot u$, u a unit in R_P. Then we define

$$v_P(x) = -n.$$

Finally we put $$v_P(0) = \infty.$$

The thinking is: If $x \in m_P, x = t_P^n \cdot u$ for some $n \geq 1$. The x has a zero at P of order n. If $\frac{1}{x} \in m_P$, the x has a pole of the described order.

A point $P = (R_P, m_P)$ has a **degree**, defined as follows. We consider the **quotient map**, also called the **residue map**.

$$R_P \xrightarrow{\varphi_P} R_P/m_P = K_P$$

where K_P is a field, called the **residue field of** P. K_P is a finite field containing $\mathbb{F}_q$.

We define: $\deg(P) = [K_P : \mathbb{F}_q]$ = degree of the field extension K_P over $\mathbb{F}_q$.

There is an **interaction** between F and $\mathfrak{M}$. The elements of F are functions on $\mathfrak{M}$. Let $f \in F$ and $P = (R_P, m_P) \in \mathfrak{M}$. Then if $f \notin R_P$ we say: f has a pole at P and define

$$f(P) = \infty.$$

If $f \in R_P$, we consider the map

$$\varphi_P : R_P \longrightarrow R_P/m_P = K_P$$

and define $f(P) = \varphi_P(f) \in K_P$ as value of f at P.

Note: The values of a function $f \in F$ are not always in the same domain, as they are in K_P and K_P is changing with P.

A point P is called an $\mathbb{F}_q$- rational point if $\deg(P) = 1$. Equivalent to this is, $K_P = \mathbb{F}_q$.

Note: If $F/\mathbb{F}_q$ is defined by the irreducible homogenous polynomial $f(X,Y,Z)$ which we assume to be nonsingular, then the points $P \in \mathfrak{M}$ with $\deg(P) = 1$ are in $1-1$ correspondence with the points $(\alpha, \beta, \gamma) \in \mathbb{P}^2(\mathbb{F}_q)$ with coefficients in $\mathbb{F}_q$ which are solutions of $f(X,Y,Z) = 0$.

The **places of degree** 1 of a curve $\Gamma = (F/\mathbb{F}_q, \mathfrak{M})$ are used to **construct codes** over $\mathbb{F}_q$.

If we use n such places, then the code will have length n.

So the **number** $N(\Gamma) = N(F)$ of points of Γ of degree 1 is important. We have the **Hasse-Weil inequality**

$$|N - (q+1)| \leq 2gq^{\frac{1}{2}} \qquad g = \text{ genus of } \Gamma$$

or

$$N \leq (q+1) + [g2q^{\frac{1}{2}}]$$

Recall: If Γ is defined by a nonsingular homogenous equation $f(X,Y,Z) = 0$ of degree n, the genus of Γ is

$$g = \frac{(n-1)(n-2)}{2}.$$

Let $\Gamma = (F/\mathbb{F}_q, \mathfrak{M})$ be a curve of genus g and $P_1, \ldots, P_n$ be distinct points of Γ of degree 1. $D = P_1 + \cdots + P_n$ is the corresponding divisor.

Let G be a divisor of Γ (or $F/\mathbb{F}_q$) such that $\mathrm{supp}(G) \cap \mathrm{supp}(D) = \emptyset$, and consider $\mathcal{L}(G) = \{f \in F; (f) \geq -G\}$.

Keep the case in mind when G is a positive divisor, say $G = r_1Q_1 + r_2Q_2 + \cdots + r_sQ_s$ with $r_i > 0$.

Then $\mathcal{L}(G) = \{$functions in F which have poles at most at $Q_1, \ldots, Q_r$ of order $\leq r_i$ respectively.$\}$

By **Riemann-Roch** we know

$$\ell(G) = \dim_{\mathbb{F}_q} \mathcal{L}(G) = \deg G + 1 - g + \underbrace{i(G)}_{\geq 0}$$

where $i(G) = \dim \mathcal{L}(W - G)$, and W is a canonical divisor. If $\deg(G) > 2g - 2$ then $i(G) = 0$.

The **Goppa Code** associated to D and G is defined by

$$C(D, G) = \{(x(P_1), \ldots, x(P_n)); x \in \mathcal{L}(G)\} \subset \mathbb{F}_q^n.$$

What we consider is a linear map, the **evaluation map** at the points $P_1, \ldots, P_n$.

$$\begin{array}{ccc} \mathcal{L}(G) & \xrightarrow{\varphi} & \mathbb{F}_q^n \\ \varphi : x & \longrightarrow & (x(P_1), \ldots, x(P_n)) \end{array}$$

Then $C(D, G) = \varphi(\mathcal{L}(G)) =$ image of $\mathcal{L}(G)$ under φ.

Theorem: $C(D, G)$ is a (linear) $[n, k, d]$ code with parameters

$$\begin{aligned} k &= \dim \mathcal{L}(G) - \dim \mathcal{L}(G - D) \\ d &\geq n - \deg G. \end{aligned}$$

Proof: The kernel of the mapping φ is

$$\begin{aligned}
\ker(\varphi) &= \{x \in \mathcal{L}(G); x \text{ has a zero at } P_1, \ldots, P_n\} \\
&= \{x; (x) \geq -G + \underbrace{P_1 + \cdots + P_n}_{D}\} \\
&= \mathcal{L}(G - D).
\end{aligned}$$

Hence $k = \dim C(D,G) = \dim \mathcal{L}(G) - \dim \mathcal{L}(G - D)$.

Let $\varphi(x) \in C(D,G)$ with $wt(\varphi(x)) = d$. Then the function x vanishes at $n - d$ places $P_{i_1}, \cdots, P_{i_{n-d}}$. Hence

$$(x) \geq -G + P_{i_1} + \cdots + P_{i_{n-d}}.$$

As $x \neq 0$, this implies

$$\begin{aligned}
0 &= \deg(x) \geq \deg(-G + P_{i_1} + \cdots + P_{i_{n-d}}) \\
&= -\deg G + (n - d) \\
\Longrightarrow d &\geq n - \deg G.
\end{aligned}$$

Corollary: Assume $\deg G < n$. Then we have:

1) $\varphi : \mathcal{L}(G) \longrightarrow C(D,G)$ is injective and $C(D,G)$ is a $[n,k,d]$-Code with $d \geq n - \deg G, \qquad k = \dim \mathcal{L}(G) \geq \deg G + 1 - g$

2) If in addition $2g - 2 < \deg G < n$, then

$$k = \deg G + 1 - g$$

3) If $x_1, \cdots, x_k$ is a basis of $\mathcal{L}(G)$, then

$$M = \begin{pmatrix} x_1(P_1) & \cdots & x_1(P_n) \\ \vdots & & \vdots \\ x_k(P_1) & \cdots & x_k(P_n) \end{pmatrix}$$

is a generator matrix for $C(D, G)$.

Originally Goppa defined his Codes as follows:

For a divisor E we define

$$\Omega(E) = \left\{ \omega; \;\; \omega \text{ a differential form of } F/\mathbb{F}_q \text{ with } (\omega) \geq +E \right\}$$

The linear code $C^*(D, G)$ of length n associated to the pair (D, G) is the image of the linear mapping

$$\begin{aligned} \alpha^* : \Omega(G - D) &\longrightarrow \mathbb{F}_q^n \\ y &\longrightarrow (\mathrm{res}_{P_1}(y), \cdots, \mathrm{res}_{P_n}(y)) \end{aligned}$$

We get the theorem:

Theorem: $C^*(D, G)$ is an $[n, k^*, d^*]$ code with parameters

$$k^* = i(G - D) - i(G) \text{ and } d^* \geq \deg G - (2g - 2).$$

If $\deg G > 2g - 2$, we have $k^* = i(G - D) \geq n + g - 1 - \deg G$.

If $2g - 2 < \deg G < n$, we have

$$k^* = n + g - 1 - \deg G.$$

The codes $C(D, G)$ and $C^*(D, G)$ are dual to each other.

Examples of Goppa Codes

$\Gamma = (\mathbb{F}_q(x), \mathfrak{M}) =$ **projective line** over $\mathbb{F}_q = \mathbb{P}^1(\mathbb{F}_q)$.

$\mathfrak{M}$ we know: For every irreducible polynomial in $\mathbb{F}_q[x]$ with highest coefficient 1 there exists a place of Γ; in addition there is a place P_∞ belonging to $\frac{1}{x}$. These are all places of Γ. Γ has $q+1$ $\mathbb{F}_q$-rational points $(x-\alpha), \alpha \in \mathbb{F}_q$ and $\frac{1}{x}$ which corresponds to ∞. We denote the place defined by the irreducible polynomial $f(x)$ by $P_f = (f)$.

Let $P_0 = (x), P_\infty = \left(\frac{1}{x}\right)$

Let $G = rP_\infty, 0 < r < q-1$. Then $\mathcal{L}(G) = \left\{ \sum_{i=0}^r a_i x^i; a_i \in \mathbb{F}_q \right\}$

$1, x, \ldots, x^r$ is a basis of $\mathcal{L}(G)$.

Let $D = (x-\alpha) + (x-\alpha^2) + \cdots + (x-\alpha^{q-1}), \alpha$ a generator of $\mathbb{F}_q^*$.
The corresponding code $C(D,G)$ has the following generator matrix:

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha^1 & \alpha^2 & \alpha^3 & \cdots & \alpha^{q-1} \\ \alpha^2 & \alpha^{2\cdot 2} & \alpha^{2\cdot 3} & \cdots & \alpha^{2(q-1)} \\ \vdots & & & & \\ \alpha^r & \alpha^{r\cdot 2} & \alpha^{r\cdot 3} & \cdots & \alpha^{r(q-1)} \end{pmatrix}.$$

We get a so-called **Reed-Solomon-Code**. It is a maximal distance separating code. Actually all Goppa codes obtained from $\mathbb{P}^1$ are MDS-Codes.

A variation is : Let $G = sP_0 + rP_\infty$

For a code $C(D,G)$ with $\deg G < n$ one has

$$k + d \geq n + (1-g) = n + 1,$$

because $k = \dim L(G) - \underbrace{\dim(G-D)}_{=0} \geq \deg G + 1 - g$

$$d \geq n - \deg G \text{ and } g = 0.$$

From the Singleton Bound: $k + d \leq n + 1$

we infer: $\boxed{k + d = n + 1}$

This means, the codes are MDS codes (maximal distance separating codes).

We consider the Klein quartic curve, defined by

$$X^3Y + Y^3Z + Z^3X = 0 \qquad \text{over } \mathbb{F}_2$$

It is a smooth curve in $\mathbb{P}^2(\mathbb{F}_2)$, of genus 3.

Over $\mathbb{F}_2$, the rational points are $(1,0,0),(0,1,0),(0,0,1)$; over $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ with $\alpha^2 = 1 + \alpha$, there are two more rational points $(1,\alpha,1+\alpha),(1,1+\alpha,\alpha)$; over $\mathbb{F}_8 = \mathbb{F}_2(\zeta)$ with $\zeta^3 = \zeta + 1$, we have all together 24 rational points.

The **Hasse–Weil** bound for the Klein curve over $\mathbb{F}_8$ it is > 25, but the **Serre bound** which states $N \leq q + 1 + g[2q^{\frac{1}{2}}]$, gives 24 over $\mathbb{F}_8$ for the Klein curve. Hence the curve is optimal with respect to the Serre bound over $\mathbb{F}_8$.

Let $Q = (0,0,1)$, and D the sum of the other 23 points, and $G = 10Q$.

The code $C(D,G)$ has dimension 8 and minimum distance $d \geq 23 - 10 = 13$.

One more example

Hermitian curves

Let $q = p^{2k}, r = p^k$

$X^{r+1} + Y^{r+1} + Z^{r+1} = 0$ defines a plane projective curve Γ, which is smooth.

The genus of Γ is $g = (q - \sqrt{q})/2$.

The number of points over $\mathbb{F}_q$ is $1 + q\sqrt{q}$ and optimal with respect to the Hasse–Weil bound.

Take $G = mQ$, where Q is one of the $\mathbb{F}_q$-rational points and $D = P_1 + \cdots + P_{q\sqrt{q}}$ consists of the other $\mathbb{F}_q$-rational points.

Take $q - \sqrt{q} < m < q \cdot \sqrt{q}$. Then we find a Goppa-Code $C(D, G)$ with length $n = q\sqrt{q}$ and dimension $k = m - g + 1$ and minimum distance $d \geq n - m = n - k - g + 1$.

This leads to some interesting codes.

2 Long Codes

Good long codes are needed because of Shannon's theorem. For every linear $[n, k, d]$ Code C over $\mathbb{F}_q$ we have the **rate** $R = R(C) = \frac{k}{n}$ and the **relative minimal distance**

$$\delta = \delta(C) = \frac{d}{n}.$$

Let $V_q = \{(\delta(C), R(C)); C \text{ code over } \mathbb{F}_q\} \subseteq [0,1]^2$ and $U_q \subseteq [0,1]^2$ the set of **limit points** of V_q.

Then there exists the so-called Manin function $\alpha_q : [0,1] \longrightarrow [0,1]$ such that

$$U_q = \{(\delta, R); 0 \leq \delta \leq 1, 0 \leq R \leq \alpha_q(\delta)\}$$

where α_q has the following properties:

1) α_q is continuous and decreasing

2) $\alpha_q(0) = 1, \qquad \alpha_q(\delta) = 0 \qquad 1 - q^{-1} \leq \delta \leq 1.$

For $\alpha_q(\delta)$ we have **bounds** from above and below (see the picture below).

$$\begin{aligned} \alpha_q(\delta) &\leq 1 - \frac{q}{q-1}\delta \\ \alpha_q(\delta) &\geq 1 - H_q(\delta) \quad 0 \leq \delta \leq 1 - q^{-1} \\ \text{with } H_q(\delta) &= \delta \log_q(q-1) - \delta \log_q(\delta) - (1-\delta)\log_q(1-\delta), \quad 0 \leq \delta \leq 1 - q^{-1} \end{aligned}$$

Problem: Construct a sequence of codes (C_i) such that

$$\lim_{i \to \infty} (\delta(C_i), R(C_i)) = (\delta_0, R_0)$$

is on the Gilbert–Varskomov bound or above this bound.

It has been well known for over 30 years that there exists a sequence of codes which are constructed using rational curves such that the Gilbert bound is reached. For about 20 years it has been known that one can do much better and can get above the Gilbert bound if the basis field $\mathbb{F}_q$ is such that q is a square.

The strategy for the construction is to construct **a sequence of functions fields** $F_i/\mathbb{F}_q$ such that $\lim_{i\to\infty} g(F_i) \longrightarrow \infty$ and F_i has many $\mathbb{F}_q$-rational points.

Important in this context is the number

$$N_q(g) = \max \left\{ \begin{array}{ll} N(F); & N(F) \text{ number of places of } F/\mathbb{F}_q \text{ of degree } 1, \\ & F/\mathbb{F}_q \text{ a function field of genus } g. \end{array} \right\}$$

Then define $A(q) = \lim_{g\to\infty} \frac{N_q(g)}{g}$.

Note: $N_q(g) \leq 1 + q + 2gq^{\frac{1}{2}}$ by Hasse–Weil and $A_q \leq 2q^{\frac{1}{2}}$.

Proposition: Suppose $A(q) > 1$. Then $\alpha_q(\delta) \geq (1 - A(q)^{-1}) - \delta$ in the interval $0 < \delta < 1 - A(q)^{-1}$.

To prove the proposition we need the lemma:

Lemma Let $P_1, \ldots, P_n$ be distinct places of $F/\mathbb{F}_q$ of degree 1. Then for every integer $r > 0$ there exists a divisor G with $\deg(G) = r$ and $P_i \notin \mathrm{supp}(G),\ i = 1, \ldots, n$.

Proof of the Lemma

The Lemma is trivial if $\exists$ place $Q \neq P_i$ of degree 1. If $P_1, \ldots, P_n$ are all places of degree 1 we choose a divisor $G \sim rP_1$ such that $v_{P_i}(G) = 0 \quad i = 1, \ldots, n$, which is possible by the approximation theorem.

By this theorem, there exists an $x \in F$ such that

$$\begin{aligned} v_{P_i}(x) &= 0 \qquad i = 2, \ldots, n \\ v_{P_1}(x) &= -r. \end{aligned}$$

Then $rP_1 + (x) = G$ is a divisor with this property.

Proof of the Proposition

Let $\delta \in (0, 1 - A(q)^{-1})$.

Choose a sequence of function fields $F_i/\mathbb{F}_q$ of genus g_i such that

$$g_i \to \infty, \qquad \frac{N(F_i)}{g_i} \to A(q) \qquad \text{for } i \to \infty.$$

Let $n_i = N(F_i)$. Then $n_i \to \infty$.

Choose $r_i > 0$ such that $\frac{r_i}{n_i} \to 1 - \delta$, for $i \longrightarrow \infty$.

Let $D_i =$ sum of all places of degree 1 of F_i. Then $\deg D_i = n_i$. By the lemma $\exists$ a divisor G_i of $F_i/\mathbb{F}_q$ with degree $G_i = r_i$ and $\operatorname{supp} G_i \cap \operatorname{supp} D_i = \emptyset$.

Consider the code

$$C_i = C(D_i, G_i)$$

which is an $[n_i, k_i, d_i]$ code with parameters

$$\begin{aligned} k_i &\geq \deg G_i + 1 - g_i = r_i + 1 - g_i \\ d_i &\geq n_i - \deg G_i = n_i - r_i. \end{aligned}$$

We get

$$R_i = R(C_i) \geq \frac{r_i + 1}{n_i} - \frac{g_i}{n_i} \qquad \delta_i = \delta(C_i) \geq 1 - \frac{r_i}{n_i}$$

We may assume that $\lim R_i = R$ and $\lim \delta_i = \tilde{\delta}$ exist and get

$$R \geq 1 - \delta - A(q)^{-1}, \qquad \tilde{\delta} \geq 1 - (1 - \delta) = \delta$$

and therefore

$$\alpha_q(\tilde{\delta}) \geq R \geq 1 - \delta - A(q)^{-1}.$$

As $\alpha_q(\delta) \geq \alpha_q(\tilde{\delta})$ we get

$$\alpha_q(\delta) \geq 1 - \delta - A(q)^{-1}. \tag{1}$$

Next we have the important inequality

$$A(q) \leq q^{\frac{1}{2}} - 1, \tag{2}$$

called the **Dringfeld–Vladut** bound.

To combine (1) and (2) we need the following result

Theorem (Tsfasman, Vladut, Zink) If q is a square, then

$$A(q) = q^{\frac{1}{2}} - 1$$

More precisely, there exists a sequence of function fields $F_\lambda/\mathbb{F}_q$ with $g(F_i) \to \infty$ such that $N(F_i)/g(F_i) \to q^{\frac{1}{2}} - 1$ for $i \to \infty$.

This theorem was first shown by Tsfasman, Vladut, Zink if $\underline{q = p^2}$.

If one uses the theorem, one obtains, if q is a square, a new lower bound.

$$\alpha_q(\delta) \geq \left(1 - \frac{1}{q^{\frac{1}{2}} - 1}\right) - \delta \qquad \text{for } 0 \leq \delta \leq 1 - \frac{1}{q^{\frac{1}{2}} - 1}.$$

This **bound** is called the **Tsfasman-Vladut-Zink Bound**.

For $q \geq 49$ this bound is better the Gilbert-Varshamov Bound.

The picture is as follows

It remains to say something to the construction of sequences of field $F_i/\mathbb{F}_q$ with the above properties.

1982 Tsfasman, Vladut, Zink proved their theorem by considering modular curves $X_0(N)$.

$X_0(N)$ is a curve which solves the moduli problem, to parameterize the pairs (E, G) where E is an elliptic curve and G a cyclic subgroup of E of order N. $X_0(N)$ is a curve defined over $\mathbb{Z}[\frac{1}{N}]$. For a prime number $p, p \not| N$ they determined that the number of points of degree 1 on $X_0(N)$ over $\mathbb{F}_{p^2}$ is

$$N_1 = \#X_0(N)(\mathbb{F}_{p^2}) \approx g(p-1)$$

moreover, $g(X_0(N))$ goes to infinity if N goes to infinity, which means

$$\frac{N_1}{g} \to p-1 \qquad \text{and the } \textbf{Dringfeld-Vladut bound} \text{ is obtained .}$$

Nowadays there are simpler ways to show this result.

Gracia and Stichtenoth have shown in 1995 the existence of a tower of fields

$$F_1 \subseteq F_2 \subseteq F_3 \subseteq \dots$$

such that $F_i/\mathbb{F}_{q^2}$ is a function field over $\mathbb{F}_{q^2}$, and such that

$$\lim_{i\to\infty} \frac{N_i}{g_i} \longrightarrow A(q^2) = q-1$$

They made the following construction

Let $F_1 = \mathbb{F}_{q^2}(x_1)$ be the rational function field over $\mathbb{F}_{q^2}$. For $n \geq 1$ let

$$F_{n+1} = F_n(z_{n+1}),$$

where z_{n+1} satisfies the equation

$$z_{n+1}^q + z_{n+1} = x_n^{q+1} \qquad \text{with } x_n = \frac{z_n}{x_{n-1}} \in F_n \qquad n \geq 2$$

We get:

$$\begin{aligned} F_2 &= F_1(z_2) \qquad \text{with} \\ & \quad z_2^q + z_2 = x_1^{q+1} \\ F_3 &= F_2(z_3) \\ & \quad z_3^q + z_3 = \left(\frac{z_2}{x_1}\right)^{q+1} \end{aligned}$$

etc.

They are able to calculate the genus and get

$$(1) \qquad g_n = g(F_n) = \begin{cases} q^n + q^{n-1} - q^{\frac{n+1}{2}} - 2q^{\frac{n-1}{2}} + 1 & n \equiv 1 \mod 2 \\ q^n + q^{n-1} - \frac{1}{2}q^{\frac{n}{2}+1} - \frac{3}{2}q^{\frac{n}{2}} - q^{\frac{n}{2}-1} + 1 & n = 0 \mod 2 \end{cases}$$

And they calculate

$$N_n = \text{ number of } \mathbb{F}_{q^2} - \text{rational points of } F_n/\mathbb{F}_{q^2}$$

and get

$$N_n \geq (q^2-1)q^{n-1} + 2q \qquad (2)$$

By (1) and (2) one get

$$\lim \frac{N_n}{g_n} = q - 1$$

Various people such as Garcia, Stichtenoth, Elkik, M. Thomas, **Wulftange** have studied in the past 8 years field towers which lead to good long codes.

An important paper concerning the basis theory on field towers is the paper Garcia/Stichtenoth: On tame towers of function fields. To appear in: Journal für reine und angewandte Mathematik.

The latest paper on this matter of which I know, is the thesis of Jörg Wulftange, which he wrote in 2002 at the University of Essen under Stichtenoth. The title is: **Zahme Türme algebraischer Funktionenkörper.**

I say a few words to its content.

Let $\mathbb{F}_q$ be a finite field.

A field extension $\mathcal{T}/\mathbb{F}_q$ is called a field tower if

1) The transcedence degree of $\mathcal{T}/\mathbb{F}_q$ is 1

2) $\mathbb{F}_q$ is algebraic closed in $\mathcal{T}$.

3) $\mathcal{T}$ is not finitely generated over $\mathbb{F}_q$.

4) $\exists$ a function field $F, \mathbb{F}_q \subseteq F \subseteq \mathcal{T}$ with $g(F) > 1$ and $\mathcal{T}/F$ separable.

A tower $\mathcal{T}/\mathbb{F}_q$ can be described by a sequence of subfields. We choose a function field $F/\mathbb{F}_q$ with $F \subseteq \mathcal{T}$ and $g(F) > 1$ and then starting from $F_0 = F$ we construct a sequence of function fields $F_0, F_1, F_2, \ldots$ such that

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \qquad \text{with } \mathcal{T} = \bigcup_{i=0}^{\infty} F_i.$$

Clearly, by the Hurwitz genus formula $g(F_i) \longrightarrow \infty$ if $i \longrightarrow \infty$.

We define

$$\lambda(\mathcal{T}) = \lim_{i \to \infty} \frac{N(F_i)}{g(F_i)}$$

which turns out to be an invariant of $\mathcal{T}$.

We have

$$0 \leq \lambda(\mathcal{T}) \leq \sqrt{q} - 1$$

by the Dringfield-Vladut bound.

Definition: The tower $\mathcal{T}/\mathbb{F}_q$ is called asymptotically good (resp. bad, resp. optimal) if $\lambda(\mathcal{T}) > 0$(resp. $\lambda(\mathcal{T}) = 0$ resp.$\lambda(\mathcal{T}) = \sqrt{q} - 1$)

Wulftange constructs towers in a recursive way as follows.

Let $f(x,y) \in \mathbb{F}_q[x,y]$ be a separable polynomial in x and y, absolutely irreducible with $\deg_x f(x,y) > 1, \deg_y(f(x,y)) > 1$. Construct a field tower as follows:

1) Take $F_0 = \mathbb{F}_q(x_0)$ the rational function field in x_0 over $\mathbb{F}_q$

2) If $f(x_{k-1}, T)$ is absolutely irreducible over the field $\mathbb{F}_q(x_0, x_1, \ldots, x_{k-1}) = F_{k-1}$, then take

$$F_k = F_{k-1}(x_k) \text{ with } f(x_{k-1}, x_k) = 0.$$

If this procedure does not stop, we get a tower. On must make sure that $g(F_k) > 1$ for on k.

Dr.Wulftange could find that the following equations lead to field towers.

Literature

Jacobus H. van Lint and Gerard van der Geer: Introduction to coding theory and algebraic geometry, Birkhäuser, 1988.

Jacobus Hendricus van Lint: Introduction to coding theory, Springer, 1998.

Stichtenoth, H.: Algebraic Function Fields and Codes, Springer-Verlag, Heidelberg 1993.

J. Wulftange: Zahme Türme algebraischer Funktionenkörper, Thesis at the University of Essen 2002