Algebraic-Geometric Codes **Fall 2024/5**

Recitation 7: The Hermitian Function Field

Scribe: Tomer Manket

1 The Hermitian Function Field

Let p be a prime and $q = p^2$.

Example 1. $\mathbb{F}_q/\mathbb{F}_p$ is a field extension of degree 2. Its Galois group is $G = \{\text{Id}, \text{Frob}\}$ where $\text{Frob}(x) = x^p$ is the Frobenius automorphism. Thus, for every $\alpha \in \mathbb{F}_q$ we have

$$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha) = \alpha^p + \alpha$$

and

$$\text{N}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) = \alpha^p \cdot \alpha = \alpha^{p+1}$$

In what follows, we write Tr and N for $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ and $\text{N}_{\mathbb{F}_q/\mathbb{F}_p}$, respectively.

Theorem 2. *Let* $E = {}^{\mathbb{F}_q(x)[y]}\big/_{\langle y^p + y - x^{p+1} \rangle}$. *Then* $E/\mathbb{F}_q(x)$ *is a field extension of degree* p*, and* $E/\mathbb{F}_q$ *is a function field, called the* Hermitian function field.

Remark 1. The corresponding curve

$$\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q \mid y^p + y = x^{p+1}\} = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q \mid \text{Tr}(y) = \text{N}(x)\}$$

is called *the Hermitian curve.*

We would like to find all the degree one places of $E/\mathbb{F}_q$. First, observe that if φ is such a place then its residue field is $\overline{E} = \mathbb{F}_q$, hence $\varphi\big|_{\mathbb{F}_q(x)}$ (which is a place of $\mathbb{F}_q(x)/\mathbb{F}_q$) is also of degree 1.

Recall that the valuations that correspond to degree one places in $\mathbb{F}_q(x)/\mathbb{F}_q$ are ν_∞ and $\nu_\alpha := \nu_{x-\alpha}$ for $\alpha \in \mathbb{F}_q$. Thus we need to consider the extensions of these valuations to E. We begin with the possible extensions of ν_∞ to E.

Let ν be an such a (discrete) extension. Since $\nu_\infty(x) = -1 < 0$ we must have $\nu(x) < 0$. Moreover,

$$\nu(y^p + y) = \nu(x^{p+1}) = (p + 1)\nu(x) < 0.$$

Thus we must have $\nu(y) < 0$ (otherwise $y \in \mathcal{O}_\nu$ which implies $y^p + y \in \mathcal{O}_\nu$). Hence $\nu(y^p) = p\nu(y) < \nu(y)$ and by the strict triangle inequality, $\nu(y^p + y) = p\nu(y)$. Therefore we obtain

$$p\nu(y) = (p+1)\nu(x) < 0 \implies p \mid \nu(x).$$

Writing $\nu(x) = -c \cdot p$ for some $c \in \mathbb{N}^+$, we get $\nu(y) = -c \cdot (p+1)$.

Claim. $v(E^\times) = c\mathbb{Z}$.

Proof of the Claim. On the one hand, $\nu\left(\frac{x}{y}\right) = \nu(x) - \nu(y) = c$ so that $c\mathbb{Z} \subseteq \nu(E^\times)$.
On the other hand, $\{1, y, y^2, \ldots, y^{p-1}\}$ is a basis of E over $\mathbb{F}_q(x)$, hence every element $a \in E^\times$ can be written as $a = \sum_{i=0}^{p-1} a_i(x) y^i$, where $a_i(t) \in \mathbb{F}_q(t)$ not all zero. It is easy to check that if $a_i(t) \neq 0$ then $\nu(a_i(x)) = \deg a_i \cdot \nu(x)$ (where $\deg \frac{f}{g} := \deg f - \deg g$). Hence

$$\begin{aligned}
\nu(a_i(x)y^i) &= \nu(a_i(x)) + \nu(y^i) \\
&= \deg a_i \cdot \nu(x) + i\nu(y) \\
&= -c \cdot [\deg a_i \cdot p + i(p+1)] \in c\mathbb{Z}.
\end{aligned}$$

In particular, if $0 \leq i < j \leq p-1$ are such that $a_i(x), a_j(x) \neq 0$ then $\nu(a_i(x)y^i) \neq \nu(a_j(x)y^j)$. Indeed, modulo cp the LHS is equivalent to $-ci$ and the RHS to $-cj$, and

$$-ci \not\equiv -cj \mod (cp) \quad \text{as} \quad i \not\equiv j \mod p.$$

Thus, by the strict triangle ineqaulity we get that $\nu(a) = \nu(a_k(x)y^k)$ for some $0 \leq k \leq p-1$, and in particular $\nu(a) \in c\mathbb{Z}$. □

Replacing ν with the equivalent valuation $\nu' := \frac{1}{c}\nu$, we may assume w.l.o.g that $\nu(E^\times) = \mathbb{Z}$, with $\nu(x) = -p$ and $\nu(y) = -(p+1)$. Up to equivalence, this is the only valuation of E which extends v_∞. In order to find the degree of the corresponding place P_∞, note that $\nu(\mathbb{F}_q(x)^\times) = p\mathbb{Z}$, so the ramification index is $(\nu(E^\times) : \nu(\mathbb{F}_q(x)^\times)) = (\mathbb{Z} : p\mathbb{Z}) = p$. By the two indices lemma,

$$[\overline{E} : \overline{\mathbb{F}_q(x)}] \cdot \big(\nu(E^\times) : \nu(\mathbb{F}_q(x)^\times)\big) \leq [E : \mathbb{F}_q(x)]$$

that is,

$$[\overline{E} : \mathbb{F}_q] \cdot p \leq p \implies \deg P_\infty = [\overline{E} : \mathbb{F}_q] \leq 1$$

hence $\deg P_\infty = 1$.

It remains to check the extensions of the valuations of the form $v_\alpha = v_{x-\alpha}$ where $\alpha \in \mathbb{F}_q$. In this case the corresponding place $\varphi_\alpha \colon \mathbb{F}_q(x) \to \mathbb{F}_q \cup \{\infty\}$ satisfies $\varphi_\alpha(x) = \alpha$. We are looking for extension $\varphi \colon E \to \mathbb{F}_q \cup \{\infty\}$ with $\varphi\big|_{\mathbb{F}_q(x)} = \varphi_\alpha$. Any such extension must satisfy

$$\varphi(y^p + y) = \varphi(x^{p+1}) = \alpha^{p+1}.$$

In particular, $y \in \mathcal{O}_\varphi$ (i.e. $\varphi(y) \in \mathbb{F}_q$) and $\varphi(y)^p + \varphi(y) = \alpha^{p+1}$, that is, $\mathrm{Tr}(\varphi(y)) = \mathrm{N}(\alpha)$.

Claim. *Let $\beta \in \mathbb{F}_p$. Then the equation $t^p + t = \beta$ has p distinct roots in $\mathbb{F}_q$.*

Proof of the Claim. For $\beta = 0$ the equation is $t^p + t = 0$, i.e. $\mathrm{Tr}(t) = 0$. As $\mathrm{Tr}\colon \mathbb{F}_q \to \mathbb{F}_p$ is a linear map, its kernel is a subspace $S_0 \subseteq \mathbb{F}_q$ of size at most p. For $\beta \neq 0$, the set of solutions S_β is either empty or an affine subspace of $\mathbb{F}_q$ (of the form $t_0 + S_0$, where $t_0^p + t_0 = \beta$). Since $\mathbb{F}_q = \bigsqcup_{\beta \in \mathbb{F}_p} S_\beta$, it must be that $|S_\beta| = p$ for all $\beta \in \mathbb{F}_p$. $\square$

Now, let $\beta = \mathrm{N}(\alpha) \in \mathbb{F}_p$. Then there are p distinct elements $\beta_1, \ldots, \beta_p \in \mathbb{F}_q$ such that $\mathrm{Tr}(\beta_i) = \beta$. Check that each one of them gives rise to a degree one place $\varphi_i \colon E \to \mathbb{F}_q \cup \{\infty\}$ which extends φ_α and satisfies

$$\varphi_i(x) = \alpha \quad \text{and} \quad \varphi_i(y) = \beta_i.$$

Moreover, any two such places are not equivalent.

Overall, we found that the number of degree one places of $E/\mathbb{F}_q$ is $N = 1 + q \cdot p = p^3 + 1$ (one which extends ν_∞, and for each $\alpha \in \mathbb{F}_q$ another p which extends ν_α).