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

Recitation 8: Adeles, Weil Differentials and AG Codes

Scribe: Tomer Manket

Let F/K be a function field with genus g.

1 Adeles and Weil Differentials

Definition 1. An *adele* of F/K is a mapping

$$\begin{aligned} \alpha\colon \mathbb{P}_F &\to F \\ \mathfrak{p} &\longmapsto \alpha_{\mathfrak{p}} \end{aligned}$$

such that $\nu_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) \geq 0$ for almost all $\mathfrak{p} \in \mathbb{P}_F$.

The set $\mathbb{A}$ of all the adeles of F/K is a K-vector space, called the *adele space* of F/K. For $\mathfrak{a} \in \mathcal{D}$, the set

$$\Lambda(\mathfrak{a}) := \{\alpha \in \mathbb{A} \mid \nu_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) + \nu_{\mathfrak{p}}(\mathfrak{a}) \geq 0 \text{ for all } \mathfrak{p} \in \mathbb{P}_F\}$$

is a K-subspace of $\mathbb{A}$. The *diagonal embedding* $F \hookrightarrow \mathbb{A}$ maps each $x \in F$ to its principal adele - the adele all of whose components are equal to x.

Definition 2. A *Weil differential* of F/K is a K-linear map $\omega\colon \mathbb{A} \to K$ such that

$$\ker \omega \supseteq \Lambda(\mathfrak{a}) + F$$

for some $\mathfrak{a} \in \mathcal{D}$.

The set Ω of all Weil differentials of F/K is a K-vector space. For $\mathfrak{a} \in \mathcal{D}$, the set

$$\Omega(\mathfrak{a}) := \{\omega \in \Omega \mid \omega(\Lambda(\mathfrak{a}) + F) = 0\}$$

is a K-subspace of Ω. Its dimension is

$$\delta(\mathfrak{a}) := \dim_K \Omega(\mathfrak{a}) = \dim_K {}^{\mathbb{A}}\!\diagup_{(\Lambda(\mathfrak{a}) + F)} = g - 1 - (\deg \mathfrak{a} - \dim \mathfrak{a}).$$

Theorem 3. *For each $0 \neq \omega \in \Omega$ there exists a unique divisor, denoted by (ω), such that*

$$\omega \in \Omega(\mathfrak{a}) \iff \mathfrak{a} \leq (\omega).$$

Definition 4. For $0 \neq \omega \in \Omega$ and $\mathfrak{p} \in \mathbb{P}_F$, we define $\nu_{\mathfrak{p}}(\omega) := \nu_{\mathfrak{p}}((\omega))$.

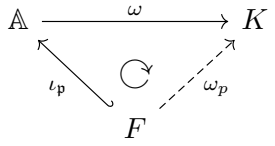
2 Local Components of Weil Differentials

Definition 5. Let $\mathfrak{p} \in \mathbb{P}_F$. The *local embedding* $\iota_\mathfrak{p} \colon F \hookrightarrow \mathbb{A}$ maps each $x \in F$ to $\iota_\mathfrak{p}(x)$, where

$$(\iota_\mathfrak{p}(x))_\mathfrak{q} := \begin{cases} x & \mathfrak{q} = \mathfrak{p} \\ 0 & \mathfrak{q} \neq \mathfrak{p} \end{cases}$$

For a Weil Differential $\omega \in \Omega$, its *local component* $\omega_\mathfrak{p} \colon F \to K$ is defined by

$$\omega_\mathfrak{p}(x) := \omega(\iota_\mathfrak{p}(x)).$$



In particular, $\omega_\mathfrak{p} \colon F \to K$ is K-linear.

Theorem 6. *Let $\omega \in \Omega$ and $\alpha \in \mathbb{A}$. Then $\omega_\mathfrak{p}(\alpha_\mathfrak{p}) = 0$ for almost all $\mathfrak{p} \in \mathbb{P}_F$, and*

$$\omega(\alpha) = \sum_{\mathfrak{p} \in \mathbb{P}_F} \omega_\mathfrak{p}(\alpha_\mathfrak{p}).$$

In particular,

$$\sum_{\mathfrak{p} \in \mathbb{P}_F} \omega_\mathfrak{p}(1) = 0.$$

Proposition 7. *Let $0 \neq \omega \in \Omega$, $\mathfrak{p} \in \mathbb{P}_F$ and $r \in \mathbb{Z}$. Then*

$$\nu_\mathfrak{p}(\omega) \geq r \iff \omega_\mathfrak{p}(x) = 0 \text{ for all } x \in F \text{ with } \nu_\mathfrak{p}(x) \geq -r.$$

Corollary 8. *$\nu_\mathfrak{p}(\omega) = m \in \mathbb{Z}$ if and only if*

1. *For every $x \in F$ with $\nu_\mathfrak{p}(x) \geq -m$ we have $\omega_\mathfrak{p}(x) = 0$; and*
2. *There exists $x \in F$ such that $\nu_\mathfrak{p}(x) = -(m+1)$ and $\omega_\mathfrak{p}(x) \neq 0$.*

In particular, $\omega_\mathfrak{p}$ is not identically zero.

Corollary 9. *A Weil differential is uniquely determined by its local component. That is, if $\omega, \omega' \in \Omega$ satisfy $\omega_\mathfrak{p} = \omega'_\mathfrak{p}$ for some $\mathfrak{p} \in \mathbb{P}_F$, then $\omega = \omega'$.*

3 AG Codes from Weil Differentials

Let $F/\mathbb{F}_q$ be a function field of genus g (i.e. $K = \mathbb{F}_q$), $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be distinct prime divisors of degree one, $\mathfrak{b} = \mathfrak{p}_1 + \ldots + \mathfrak{p}_n$ and $\mathfrak{a} \in \mathcal{D}$ such that $\nu_{\mathfrak{p}_i}(\mathfrak{a}) = 0$ for all $i \in [n]$.

Recall that if $\mathfrak{p}$ is a prime divisor of degree one and $x \in F$ satisfies $\nu_{\mathfrak{p}}(x) \geq 0$, then

$$x(\mathfrak{p}) := x + \mathfrak{m}_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}} = \mathbb{F}_q.$$

In class we defined the Goppa code

$$C_{\mathscr{L}}(\mathfrak{b}, \mathfrak{a}) := \{(f(\mathfrak{p}_1), \ldots, f(\mathfrak{p}_n)) \mid f \in \mathscr{L}(\mathfrak{a})\} \subseteq \mathbb{F}_q^n.$$

Definition 10. The algebraic geometry code $C_\Omega(\mathfrak{b}, \mathfrak{a}) \subseteq \mathbb{F}_q^n$ is defined by

$$C_\Omega(\mathfrak{b}, \mathfrak{a}) := \{(\omega_{\mathfrak{p}_1}(1), \ldots, \omega_{\mathfrak{p}_n}(1)) \mid \omega \in \Omega(\mathfrak{a} - \mathfrak{b})\}.$$

Claim 11. *Let $\mathfrak{p}$ be a prime divisor of degree one, $x \in F$ such that $\nu_{\mathfrak{p}}(x) \geq 0$ and $\omega \in \Omega$ such that $\nu_{\mathfrak{p}}(\omega) \geq -1$. Then*

$$\omega_{\mathfrak{p}}(x) = x(\mathfrak{p}) \cdot \omega_{\mathfrak{p}}(1).$$

Proof. As $x(\mathfrak{p}) \in \mathbb{F}_q$, we can write $x = c + y$ where $c = x(\mathfrak{p}) \in \mathbb{F}_q$ and $y \in \mathfrak{m}_{\mathfrak{p}}$ (i.e. $y \in F$ and $\nu_{\mathfrak{p}_i}(y) > 0$). Hence

$$\omega_{\mathfrak{p}}(x) = \omega_{\mathfrak{p}}(c) + \omega_{\mathfrak{p}}(y) = c \cdot \omega_{\mathfrak{p}}(1) + 0 = x(\mathfrak{p}) \cdot \omega_{\mathfrak{p}}(1)$$

(where $\omega_{\mathfrak{p}}(y) = 0$ by Proposition 7, as $\nu_{\mathfrak{p}}(\omega) \geq -1$ and $y \in F$ satisfies $\nu_{\mathfrak{p}}(y) \geq 1$). □

Theorem 12 (The parameters of the code $C_\Omega(\mathfrak{b}, \mathfrak{a})$)**.** *The code $C_\Omega(\mathfrak{b}, \mathfrak{a}) \subseteq \mathbb{F}_q^n$ has dimension*

$$\dim_K C_\Omega(\mathfrak{b}, \mathfrak{a}) = \delta(\mathfrak{a} - \mathfrak{b}) - \delta(\mathfrak{a})$$

and minimum distance

$$d \geq \deg \mathfrak{a} - (2g - 2).$$

Proof. We will only prove the first statement (the dimension of $C_\Omega(\mathfrak{b}, \mathfrak{a})$ over $\mathbb{F}_q$). The evaluation map $\mathrm{ev}\colon \Omega(\mathfrak{a} - \mathfrak{b}) \to C_\Omega(\mathfrak{b}, \mathfrak{a})$ given by

$$\mathrm{ev}(\omega) := (\omega_{\mathfrak{p}_1}(1), \ldots, \omega_{\mathfrak{p}_n}(1))$$

is a surjective, $\mathbb{F}_q$-linear map. We claim that $\ker(\mathrm{ev}) = \Omega(\mathfrak{a})$. Indeed,

($\supseteq$): Let $\omega \in \Omega(\mathfrak{a})$. Since $\mathfrak{a} - \mathfrak{b} \leq \mathfrak{a}$ we have $\Omega(\mathfrak{a} - \mathfrak{b}) \supseteq \Omega(\mathfrak{a})$, so $\omega \in \Omega(\mathfrak{a} - \mathfrak{b})$. In addition, $\mathfrak{a} \leq (\omega)$ so for every $i \in [n]$,

$$\nu_{\mathfrak{p}_i}(\omega) \geq \nu_{\mathfrak{p}_i}(\mathfrak{a}) = 0 \implies \omega_{\mathfrak{p}_i}(1) = 0$$

by Proposition 7.

($\subseteq$): Suppose $\omega \in \ker(\mathrm{ev})$. Then $\omega \in \Omega(\mathfrak{a} - \mathfrak{b})$ so $\mathfrak{a} - \mathfrak{b} \leq (\omega)$. Hence for $\mathfrak{p} \notin \mathrm{supp}(\mathfrak{b})$,

$$\nu_{\mathfrak{p}}(\omega) \geq \nu_{\mathfrak{p}}(\mathfrak{a} - \mathfrak{b}) = \nu_{\mathfrak{p}}(\mathfrak{a})$$

and for every $i \in [n]$,

$$\nu_{\mathfrak{p}_i}(\omega) \geq \nu_{\mathfrak{p}_i}(\mathfrak{a} - \mathfrak{b}) = -1.$$

In order to prove that $\omega \in \Omega(\mathfrak{a})$ it suffices to show that $(\omega) \geq \mathfrak{a}$, i.e. to show that for $i \in [n]$, $\nu_{\mathfrak{p}_i}(\omega) \geq \nu_{\mathfrak{p}_i}(\mathfrak{a}) = 0$. By Proposition 7, it suffices to show that if $x \in F$ satisfies $\nu_{\mathfrak{p}_i}(x) \geq 0$ then $\omega_{\mathfrak{p}_i}(x) = 0$. Indeed, given such $x \in F$ we get by Claim 11 that

$$\omega_{\mathfrak{p}_i}(x) = x(\mathfrak{p}_i) \cdot \omega_{\mathfrak{p}_i}(1) = x(\mathfrak{p}_i) \cdot 0 = 0.$$

It follows (by the rank-nullity Theorem) that

$$\dim_K \Omega(\mathfrak{a}) + \dim_K C_\Omega(\mathfrak{b}, \mathfrak{a}) = \dim_K \Omega(\mathfrak{a} - \mathfrak{b}),$$

i.e.

$$\dim_K C_\Omega(\mathfrak{b}, \mathfrak{a}) = \delta(\mathfrak{a} - \mathfrak{b}) - \delta(\mathfrak{a}).$$

□

Theorem 13. *The codes $C_{\mathscr{L}}(\mathfrak{b}, \mathfrak{a})$ and $C_\Omega(\mathfrak{b}, \mathfrak{a})$ are dual to each other, i.e.*

$$C_\Omega(\mathfrak{b}, \mathfrak{a}) = C_{\mathscr{L}}(\mathfrak{b}, \mathfrak{a})^\perp.$$

Proof. Let us first show that $C_\Omega(\mathfrak{b}, \mathfrak{a}) \subseteq C_{\mathscr{L}}(\mathfrak{b}, \mathfrak{a})^\perp$. Let $0 \neq \omega \in \Omega(\mathfrak{a} - \mathfrak{b})$ and $x \in \mathscr{L}(\mathfrak{a})$. Then by Claim 11 we obtain

$$(\omega_{\mathfrak{p}_1}(1), \ldots, \omega_{\mathfrak{p}_n}(1)) \cdot (x(\mathfrak{p}_1), \ldots, x(\mathfrak{p}_n)) = \sum_{i=1}^{n} x(\mathfrak{p}_i) \cdot \omega_{\mathfrak{p}_i}(1) = \sum_{i=1}^{n} \omega_{\mathfrak{p}_i}(x). \tag{1}$$

Note that for $\mathfrak{p} \notin \operatorname{supp}(\mathfrak{b})$ we have $\nu_{\mathfrak{p}}(x) \geq -\nu_{\mathfrak{p}}(\omega)$ (as $x \in \mathscr{L}(\mathfrak{a})$ implies $\nu_{\mathfrak{p}}(x) \geq -\nu_{\mathfrak{p}}(\mathfrak{a})$, and $\omega \in \Omega(\mathfrak{a} - \mathfrak{b})$ implies $(\omega) \geq \mathfrak{a} - \mathfrak{b}$, so $\nu_{\mathfrak{p}}(\omega) \geq \nu_{\mathfrak{p}}(\mathfrak{a} - \mathfrak{b}) = \nu_{\mathfrak{p}}(\mathfrak{a})$). Thus, by Proposition 7 we obtain $\omega_{\mathfrak{p}}(x) = 0$. It follows that

$$\sum_{i=1}^{n} \omega_{\mathfrak{p}_i}(x) = \sum_{\mathfrak{p} \in \mathbb{P}_F} \omega_{\mathfrak{p}}(x) = \omega(x) = 0,$$

where we used Theorem 6 and the fact that Weil differentials vanish on principal adeles. Together with (1) we get the desired result.

Now, the equality $C_\Omega(\mathfrak{b}, \mathfrak{a}) = C_{\mathscr{L}}(\mathfrak{b}, \mathfrak{a})^\perp$ follows from dimension considerations, as

$$\begin{aligned} \dim_K C_{\mathscr{L}}(\mathfrak{b}, \mathfrak{a})^\perp &= n - \dim_K C_{\mathscr{L}}(\mathfrak{b}, \mathfrak{a}) \\ &= n - (\dim \mathfrak{a} - \dim(\mathfrak{a} - \mathfrak{b})), \end{aligned}$$

which is equal (using Theorem 12) to

$$\begin{aligned} \dim_K C_\Omega(\mathfrak{b}, \mathfrak{a}) &= \delta(\mathfrak{a} - \mathfrak{b}) - \delta(\mathfrak{a}) \\ &= g - 1 - (\deg(\mathfrak{a} - \mathfrak{b}) - \dim(\mathfrak{a} - \mathfrak{b})) - [g - 1 - (\deg \mathfrak{a} - \dim \mathfrak{a})] \\ &= \deg \mathfrak{b} + \dim(\mathfrak{a} - \mathfrak{b}) - \dim \mathfrak{a} \\ &= n - (\dim \mathfrak{a} - \dim(\mathfrak{a} - \mathfrak{b})). \end{aligned}$$

□

Remarkably, the code $C_\Omega(\mathfrak{b}, \mathfrak{a})$ can be represented as a Goppa code $C_{\mathscr{L}}(\mathfrak{b}, \mathfrak{p})$ for an appropriate divisor $\mathfrak{p}$.

Claim 14. *There exists a Weil differential η such that for all $i \in [n]$,*

$$\nu_{\mathfrak{p}_i}(\eta) = -1 \quad \text{and} \quad \eta_{\mathfrak{p}_i}(1) = 1.$$

Theorem 15.

$$C_\Omega(\mathfrak{b}, \mathfrak{a}) = C_{\mathscr{L}}(\mathfrak{b}, \mathfrak{b} - \mathfrak{a} + (\eta))$$

where $\eta \in \Omega$ is as in Claim 14.