Algebraic Geometry Codes

Group 5.239A
Martin Sig Nørbjerg

Institute of Mathematics
Aalborg University

AALBORG UNIVERSITY
DENMARK

Martin Sig Nørbjerg

Definition 1.1 & 1.5. Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear subspace of dimension k, then $\mathcal{C}$ is called a $[n, k]_q$ code. Furthermore if $\mathcal{C}$ has minimum distance d, then $\mathcal{C}$ is called a $[n, k, d]_q$ code.

Definition 1.1 & 1.5. Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear subspace of dimension k, then $\mathcal{C}$ is called a $[n,k]_q$ code. Furthermore if $\mathcal{C}$ has minimum distance d, then $\mathcal{C}$ is called a $[n,k,d]_q$ code.

- If $\mathcal{C}$ has minimum distance d, then it can correct $\lfloor \frac{d-1}{2} \rfloor$ errors but detect $d-1$ errors.

Martin Sig Nørbjerg

Corollary 1.18. Let $\mathcal{C}$ be a $[n, k, d]_q$ code, then $d - 1 \leq n - k$.

Institute of Mathematics
Aalborg University

Martin Sig Nørbjerg

Corollary 1.18. Let $\mathcal{C}$ be a $[n, k, d]_q$ code, then $d - 1 \leq n - k$.
Proof: Let H be a parity check matrix of $\mathcal{C}$.

Martin Sig Nørbjerg

Corollary 1.18. Let $\mathcal{C}$ be a $[n,k,d]_q$ code, then $d-1 \leq n-k$.
Proof: Let H be a parity check matrix of $\mathcal{C}$.

- $\dim(\mathcal{C}) = \dim(null(H)) = k \implies rank(H) = n-k$

Corollary 1.18. Let $\mathcal{C}$ be a $[n,k,d]_q$ code, then $d-1 \leq n-k$.
Proof: Let H be a parity check matrix of $\mathcal{C}$.

- $\dim(\mathcal{C}) = \dim(null(H)) = k \implies rank(H) = n-k$
- $rank(H) \geq d-1$, by the Proposition 1.16.

Martin Sig Nørbjerg

Definition 2.81 & 2.82. Let $\mathcal{X}$ be an aboslutely irreducible regular projective plane curve, over $\mathbb{F}_q$.

Martin Sig Nørbjerg

Definition 2.81 & 2.82. Let $\mathcal{X}$ be an aboslutely irreducible regular projective plane curve, over $\mathbb{F}_q$.

- A divisor D on $\mathcal{X}$ is a formal sum:

$$D = \sum_{P \in \mathcal{X}} n_P P$$

where $n_P = 0$ for all but a finite number of points $P \in \mathcal{X}$.

Divisors

Definition 2.81 & 2.82. Let $\mathcal{X}$ be an aboslutely irreducible regular projective plane curve, over $\mathbb{F}_q$.

- A divisor D on $\mathcal{X}$ is a formal sum:

$$D = \sum_{P \in \mathcal{X}} n_P P$$

  where $n_P = 0$ for all but a finite number of points $P \in \mathcal{X}$.
- Let $f \in \overline{\mathbb{F}}_q(\mathcal{X}) \setminus \{0\}$, then $(f) := \sum_{P \in \mathcal{X}} v_P(f) P$ is called a principal divisor.

Definition 2.81 & 2.82. Let $\mathcal{X}$ be an aboslutely irreducible regular projective plane curve, over $\mathbb{F}_q$.

- A divisor D on $\mathcal{X}$ is a formal sum:

$$D = \sum_{P \in \mathcal{X}} n_P P$$

  where $n_P = 0$ for all but a finite number of points $P \in \mathcal{X}$.
- Let $f \in \overline{\mathbb{F}}_q(\mathcal{X}) \setminus \{0\}$, then $(f) := \sum_{P \in \mathcal{X}} v_P(f) P$ is called a principal divisor.
  - $\forall f \in \overline{\mathbb{F}}_q(\mathcal{X}) \setminus \{0\}$ we have $\deg((f)) = 0$ by Proposition 2.83.

The vector space $L(D)$

Definition 2.84. Let $D \in Div(\mathcal{X})$, then we define the vector space $L(D)$ as:

$$L(D) := \left\{ f \in \overline{\mathbb{F}}_q(\mathcal{X}) \setminus \{0\} \mid (f) + D \text{ is effective} \right\} \cup \{0\}$$

and let $\ell(D) := \dim_{\overline{\mathbb{F}}_q}(L(D))$.

The vector space $L(D)$

Definition 2.84. Let $D \in Div(\mathcal{X})$, then we define the vector space $L(D)$ as:

$$L(D) := \left\{ f \in \overline{\mathbb{F}}_q(\mathcal{X}) \setminus \{0\} \mid (f) + D \text{ is effective} \right\} \cup \{0\}$$

and let $\ell(D) := \dim_{\overline{\mathbb{F}}_q}(L(D))$.

Proposition 2.88. (i) Let $D \in Div(\mathcal{X})$, then $\deg(D) < 0$ implies that $\ell(D) = 0$.

Definition 2.84. Let $D \in Div(\mathcal{X})$, then we define the vector space $L(D)$ as:

$$L(D) := \left\{ f \in \overline{\mathbb{F}}_q(\mathcal{X}) \setminus \{0\} \mid (f) + D \text{ is effective} \right\} \cup \{0\}$$

and let $\ell(D) := \dim_{\overline{\mathbb{F}}_q}(L(D))$.

Proposition 2.88. (i) Let $D \in Div(\mathcal{X})$, then $\deg(D) < 0$ implies that $\ell(D) = 0$.
Proof: For all $f \in \overline{\mathbb{F}}_q(\mathcal{X}) \setminus \{0\}$ we have:

$$\deg((f) + D) = \deg((f)) + \deg(D) = \deg(D) < 0$$

since $\deg((f)) = 0$.

The vector space $L(D)$

Definition 2.84. Let $D \in Div(\mathcal{X})$, then we define the vector space $L(D)$ as:

$$L(D) := \left\{ f \in \overline{\mathbb{F}}_q(\mathcal{X}) \setminus \{0\} \mid (f) + D \text{ is effective} \right\} \cup \{0\}$$

and let $\ell(D) := \dim_{\overline{\mathbb{F}}_q}(L(D))$.

Proposition 2.88. (i) Let $D \in Div(\mathcal{X})$, then $\deg(D) < 0$ implies that $\ell(D) = 0$.
Proof: For all $f \in \overline{\mathbb{F}}_q(\mathcal{X}) \setminus \{0\}$ we have:

$$\deg((f) + D) = \deg((f)) + \deg(D) = \deg(D) < 0$$

since $\deg((f)) = 0$. Meaning $L(D) = \{0\}$.

The Riemann-Roch Theorem

Let $\mathcal{X}$ be a regular projective plane curve of genus g.
Theorem 2.91. Let $D \in Div(\mathcal{X})$, then for all canonical $W \in Div(\mathcal{X})$ we have

$$\ell(D) - \ell(W - D) = \deg(D) - g + 1$$

Martin Sig Nørbjerg

The Riemann-Roch Theorem

Let $\mathcal{X}$ be a regular projective plane curve of genus g.

Theorem 2.91. Let $D \in Div(\mathcal{X})$, then for all canonical $W \in Div(\mathcal{X})$ we have

$$\ell(D) - \ell(W - D) = \deg(D) - g + 1$$

Corollary 2.92. If $\deg(D) > 2g - 2$, then $\ell(D) = \deg(D) - g + 1$.

Institute of Mathematics
Aalborg University

The Riemann-Roch Theorem

Let $\mathcal{X}$ be a regular projective plane curve of genus g.
Theorem 2.91. Let $D \in Div(\mathcal{X})$, then for all canonical $W \in Div(\mathcal{X})$ we have

$$\ell(D) - \ell(W - D) = \deg(D) - g + 1$$

Corollary 2.92. If $\deg(D) > 2g - 2$, then $\ell(D) = \deg(D) - g + 1$.
Proof:

- $\deg(W - D) < 0$.

Martin Sig Nørbjerg

Let $\mathcal{X}$ be a regular projective plane curve of genus g.

Theorem 2.91. Let $D \in Div(\mathcal{X})$, then for all canonical $W \in Div(\mathcal{X})$ we have

$$\ell(D) - \ell(W - D) = \deg(D) - g + 1$$

Corollary 2.92. If $\deg(D) > 2g - 2$, then $\ell(D) = \deg(D) - g + 1$.

Proof:

- $\deg(W - D) < 0$.
- $\ell(W - D) = 0$ by Proposition 2.88 (i), combining this with Theorem 2.91 yields the result.

Institute of Mathematics
Aalborg University

Definition 3.3. Let $P_1, P_2, \ldots, P_n \in \mathcal{X}$ be n distinct rational points.

Martin Sig Nørbjerg

Definition 3.3. Let $P_1, P_2, \ldots, P_n \in \mathcal{X}$ be n distinct rational points.

- Let $D = \sum_i^n P_i$ and $G \in Div(\mathcal{X})$ such that $supp(D) \cap supp(G) = \emptyset$.

Definition 3.3. Let $P_1, P_2, \ldots, P_n \in \mathcal{X}$ be n distinct rational points.

- Let $D = \sum_i^n P_i$ and $G \in Div(\mathcal{X})$ such that $supp(D) \cap supp(G) = \emptyset$.
- If $\mathcal{P} := (P_1, P_2, \ldots, P_n)$, then $\mathcal{C}_{D,G} := Ev_{\mathcal{P}}(L(G))$ is called a *Goppa Code*.

Parameters of Goppa Codes

Theorem 3.5. If $\mathcal{C}_{D,G}$ is a $[n, k, d]_q$ code. Then:

Theorem 3.5. If $\mathcal{C}_{D,G}$ is a $[n,k,d]_q$ code. Then:

(i) $k = \ell(G) - \ell(G-D)$.

Theorem 3.5. If $\mathcal{C}_{D,G}$ is a $[n,k,d]_q$ code. Then:

(i) $k = \ell(G) - \ell(G-D)$.

(ii) $d \geq n - \deg(G)$.

Theorem 3.5. If $\mathcal{C}_{D,G}$ is a $[n,k,d]_q$ code. Then:

(i) $k = \ell(G) - \ell(G-D)$.

(ii) $d \geq n - \deg(G)$.

Proof:

(i) Follows from the fact that $Ev_{\mathcal{P}} \restriction_{L(G)}$ is a surjective linear map, from $L(G)$ to $\mathcal{C}_{G,D}$.

Theorem 3.5. If $\mathcal{C}_{D,G}$ is a $[n,k,d]_q$ code. Then:

(i) $k = \ell(G) - \ell(G-D)$.

(ii) $d \geq n - \deg(G)$.

Proof:

(i) Follows from the fact that $Ev_{\mathcal{P}} \restriction_{L(G)}$ is a surjective linear map, from $L(G)$ to $\mathcal{C}_{G,D}$.

$$k = \dim_{\mathbb{F}_q}(image(Ev_{\mathcal{P}})) = \ell(G) - \dim_{\mathbb{F}_q}(ker(Ev_{\mathcal{P}}))$$

Theorem 3.5. If $\mathcal{C}_{D,G}$ is a $[n,k,d]_q$ code. Then:

(i) $k = \ell(G) - \ell(G-D)$.

(ii) $d \geq n - \deg(G)$.

Proof:

(i) Follows from the fact that $Ev_{\mathcal{P}} \restriction_{L(G)}$ is a surjective linear map, from $L(G)$ to $\mathcal{C}_{G,D}$.

$$k = \dim_{\mathbb{F}_q}(image(Ev_{\mathcal{P}})) = \ell(G) - \dim_{\mathbb{F}_q}(ker(Ev_{\mathcal{P}}))$$

But $ker(Ev_{\mathcal{P}}) = L(G-D)$ since:

Theorem 3.5. If $\mathcal{C}_{D,G}$ is a $[n,k,d]_q$ code. Then:

(i) $k = \ell(G) - \ell(G-D)$.

(ii) $d \geq n - \deg(G)$.

Proof:

(i) Follows from the fact that $Ev_{\mathcal{P}} \restriction_{L(G)}$ is a surjective linear map, from $L(G)$ to $\mathcal{C}_{G,D}$.

$$k = \dim_{\mathbb{F}_q}(image(Ev_{\mathcal{P}})) = \ell(G) - \dim_{\mathbb{F}_q}(ker(Ev_{\mathcal{P}}))$$

But $ker(Ev_{\mathcal{P}}) = L(G-D)$ since:

- $f \in L(G)$ & $Ev_{\mathcal{P}}(f) = 0 \implies v_{P_i}(f) \geq 1$ and hence $f \in L(G-D)$. As $(f) + G - D$ is effective.

Theorem 3.5. If $\mathcal{C}_{D,G}$ is a $[n,k,d]_q$ code. Then:

(i) $k = \ell(G) - \ell(G-D)$.

(ii) $d \geq n - \deg(G)$.

Proof:

(i) Follows from the fact that $Ev_{\mathcal{P}} \restriction_{L(G)}$ is a surjective linear map, from $L(G)$ to $\mathcal{C}_{G,D}$.

$$k = \dim_{\mathbb{F}_q}(image(Ev_{\mathcal{P}})) = \ell(G) - \dim_{\mathbb{F}_q}(ker(Ev_{\mathcal{P}}))$$

But $ker(Ev_{\mathcal{P}}) = L(G-D)$ since:

- $f \in L(G)$ & $Ev_{\mathcal{P}}(f) = 0 \implies v_{P_i}(f) \geq 1$ and hence $f \in L(G-D)$. As $(f) + G - D$ is effective.
- $f \in L(G-D) \implies f(P) = 0 \forall P \in supp(D)$ as $supp(G) \cap supp(D) = \emptyset$. Meaning $f \in ker(Ev_{\mathcal{P}})$.

Parameters of Goppa Codes (Continued.)

Corollary 3.6 (i). If $\deg(G) < n$, then $k = \ell(G)$.

Parameters of Goppa Codes (Continued.)

Corollary 3.6 (i). If $\deg(G) < n$, then $k = \ell(G)$.
Proof: $\deg(G - D) < 0$, the rest follows by Proposition 2.88 (i) and Theorem 3.5 (i).

Parameters of Goppa Codes (Continued.)

Corollary 3.6 (i). If $\deg(G) < n$, then $k = \ell(G)$.
Proof: $\deg(G - D) < 0$, the rest follows by Proposition 2.88 (i) and Theorem 3.5 (i).

Remark 3.7.

- $k = \ell(G) \geq \deg(G) - g + 1$ by the Riemann-Roch Theorem 2.91.

Parameters of Goppa Codes (Continued.)

Corollary 3.6 (i). If $\deg(G) < n$, then $k = \ell(G)$.
Proof: $\deg(G - D) < 0$, the rest follows by Proposition 2.88 (i) and Theorem 3.5 (i).

Remark 3.7.

- $k = \ell(G) \geq \deg(G) - g + 1$ by the Riemann-Roch Theorem 2.91.
- Combining this with Theorem 3.5 (ii), we see:

$$d + k \geq \underbrace{(n - \deg(G))}_{\geq d} + \underbrace{(\deg(G) - g + 1)}_{\geq k} = n - g + 1 \qquad (1)$$

Martin Sig Nørbjerg

Corollary 3.6 (i). If $\deg(G) < n$, then $k = \ell(G)$.
Proof: $\deg(G - D) < 0$, the rest follows by Proposition 2.88 (i) and Theorem 3.5 (i).

Remark 3.7.

- $k = \ell(G) \geq \deg(G) - g + 1$ by the Riemann-Roch Theorem 2.91.
- Combining this with Theorem 3.5 (ii), we see:

$$d + k \geq \underbrace{(n - \deg(G))}_{\geq d} + \underbrace{(\deg(G) - g + 1)}_{\geq k} = n - g + 1 \qquad (1)$$

- Combinig this with the Singleton Bound we see that $n + 1 \geq d + k \geq n - g + 1$, and that $g = 0$ implies that $\mathcal{C}_{G,D}$ is an MDS code.

Institute of Mathematics
Aalborg University

End

Thank you for listening.