15. Rationale Funktionen in der Codierungstheorie – Goppa-Codes

15.1. Codierung

Codes. Sei K ein endlicher Körper,
z.B. $K = \mathbb{Z}_2 = \{0, 1\}$.
Nachrichten werden als „Wörter“ $v \in K^k$ gegeben.
Codierung der Nachricht, um Übertragungsfehler entdecken und korrigieren zu können.
Ein *Code* (*Encoding*) ist eine injektive Abbildung

$$E : K^k \quad \to \quad K^n$$

Beispiele.

(1)

$$\begin{array}{rcl} E : K^k & \to & K^{2k} \\ (v_1, \ldots, v_k) & \mapsto & (v_1, v_1, v_2, v_2, \ldots, v_k, v_k) \end{array}$$

Manche Übertragungsfehler kann man durch diese Codierung entdecken,

$$(0, 0, 1, 1, \ldots, 0, 0, 0, 1) \notin \text{Bild}(E)$$

aber nicht korrigieren.

(2)

$$\begin{array}{rcl} E : K^k & \to & K^{3k} \\ (v_1, \ldots, v_k) & \mapsto & (v_1, v_1, v_1, v_2, v_2, v_2, \ldots, v_k, v_k, v_k) \end{array}$$

Hier gilt:

$$(0,0,0,1,1,1,\ldots,0,0,1) \notin \mathrm{Bild}(E)$$

liegt am nächsten zu

$$(0,0,0,1,1,1,\ldots,0,0,0) \in \mathrm{Bild}(E)$$

Man kann bei diesem Code 1 Fehler korrigieren.

Hamming-Abstand von $v, w \in K^n$:

$$\boxed{d(v,w) := \#\{i \mid v_i \neq w_i\}}$$

Idee für Korrektur von Fehlern: Ersetze fehlerhaftes Codewort durch ein zulässiges Codewort, das möglichst kleinen Hamming-Abstand hat.
Minimalabstand des Codes E:

$$\boxed{d_E := \min\{d(v,w) \mid v,w \in \mathrm{Bild}(E), v \neq w\}}$$

Für jedes $v \in K^n$ liegt höchstens ein Codewort im Abstand $< \frac{d}{2}$.
$\Longrightarrow$ Man kann $\left\lfloor \frac{d-1}{2} \right\rfloor$ Fehler korrigieren.
k, n, d_E sind die charakteristischen Parameter des Codes.

Ziel: Maximiere gleichzeitig

$\frac{k}{n}$ Übertragungsrate
$\frac{d_E}{n}$

Bemerkung: Wenn der Code linear ist (d.h. E eine lineare Abbildung), dann gilt

$$d_E = \min\{d(v,0) \mid v \in \text{Bild}(E), v \neq 0\}$$

Beispiele:

(1) $K^k \to K^{2k}$ (von oben): Hier ist $n = 2k$, also

$$\frac{k}{n} = \frac{1}{2} \qquad \text{und} \qquad d_E = 2$$

Man kann $\left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{1}{2} \right\rfloor = 0$ Fehler korrigieren.

(2) $K^k \to K^{3k}$ (von oben): Hier ist $n = 3k$, also

$$\frac{k}{n} = \frac{1}{3} \qquad \text{und} \qquad d_E = 3$$

Man kann $\left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{2}{2} \right\rfloor = 1$ Fehler korrigieren.

(3) Zum Vergleich: Bei dem Code, der in Audio- und Daten-CDs eingesetzt wird (Reed-Solomon-Codes), kommen zu 24 Nutzerbytes jeweils 8 Kontrollbytes für Fehlererkennung und -korrektur hinzu.
Übertragungsrate:

$$\frac{k}{n} = \frac{24}{24+8} = \frac{3}{4}$$

(d.h. 33 Prozent Redundanz)

Singleton Bound. Für lineare Codes $E : K^k \to K^n$ gilt

$$\boxed{k + d_E \leqslant n + 1}$$

Beweis: Es ist $\dim \text{Bild}(E) = k$, also gibt es ein $v \in \text{Bild}(E)$, $v \neq 0$, der Form

$$v = (0, \ldots, 0, v_k, \ldots, v_n)$$

($k-1$ lineare Bedinungen)
Daher: $d(v, 0) \leqslant n - (k-1)$
und damit $d_E \leqslant n - (k-1)$. $\square$
Folgerung:

$$\boxed{\frac{k}{n} + \frac{d_E}{n} \leqslant 1 + \frac{1}{n}}$$

15.2. Divisoren und Riemann-Roch-Raum

Divisoren. Sie $V \subset \mathbb{P}^N$ eine glatte Kurve (1-dim. glatte proj. Varietät).
Ein *Divisor auf* V ist eine formale $\mathbb{Z}$-Linearkombination von Punkten aus V:

$$D = \sum_{i=1}^{r} n_i \, p_i$$

mit $n_i \in \mathbb{Z}$ und $p_i \in V$.
Beispiel: $V = \mathbb{P}^1$, $D = 2(1:0) - 3(0:1) + 27(2:3)$.
Der *Grad* von D ist

$$\deg(D) = \sum_{i=1}^{r} n_i \in \mathbb{Z}$$

Im Beispiel von oben: $\deg(D) = 2 - 3 + 27 = 26$.
Ordnungsrelation:

$$\begin{aligned} D \geqslant 0 \quad &:\Longleftrightarrow \quad n_i \geqslant 0 \ \forall i \\ D_1 \geqslant D_2 \quad &:\Longleftrightarrow \quad D_1 - D_2 \geqslant 0 \end{aligned}$$

Beispiel:

$$2(1:0) - 2(0:1) + 27(2:3) \geqslant 2(1:0) - 3(0:1)$$

Der Divisor einer rationalen Funktion. Jede rationale Funktion $f \in K(V)$ definiert einen Divisor auf V

$$\boxed{\operatorname{div}(f) := \text{Nullstellen} - \text{Polstellen}}$$

Beispiele:

(1) $V = \mathbb{P}^1$,

$$f = \frac{x_0^2 + x_1^2}{x_0^2}$$

$$\operatorname{div}(f) = (1:i) + (-1:i) - 2(0:1)$$

(2) $V = V(yz - x^2) \subset \mathbb{P}^2$,

$$f = \frac{y}{x} = \frac{yx}{x^2} = \frac{yx}{yz} = \frac{x}{z}$$

$$\operatorname{div}(f) = (0:0:1) - (0:1:0)$$

Man kann zeigen: Für jedes $f \in K(V)$ gilt

$$\boxed{\deg(\operatorname{div}(f)) = 0}$$

Der Riemann-Roch-Raum eines Divisors.

$$\boxed{H^0(V, D) := \{f \in K(V) \mid \operatorname{div}(f) \geqslant -D\}}$$

Beispiel: $V = \mathbb{P}^1$, $D = 2(0:1)$

$$H^0(\mathbb{P}^1, D) = \left\{f \in K(\mathbb{P}^1) \;\middle|\; \operatorname{div}(f) \geqslant -2(0:1)\right\}$$

(Rationale Funktionen f, die regulär sind außerhalb von $(0:1)$ und die in $(0:1)$ höchstens einen Pol zweiter Ordnung haben.)
Schreibweise:

$$h^0(V, D) := \dim H^0(V, D)$$

Bemerkung. Für den Nulldivisor $D = 0$ gilt:

$$\begin{aligned} H^0(V, D) &= \{f \in K(V) \mid \operatorname{div}(f) \geqslant 0\} \\ &= \{f \in K(V) \mid f \text{ regulär}\} \\ &= \mathcal{O}_V(V) \\ &= K \end{aligned}$$

also

$$h^0(V, 0) = 1$$

Der Satz von Riemann-Roch.

$$\boxed{h^0(V, D) \geqslant 1 - g(V) + \deg(D)}$$

wobei $g(V)$ das *Geschlecht* der Kurve V ist (eine topologische Invariante).

15.3. Goppa-Codes

Sei K ein endlicher Körper und $V \subset \mathbb{P}^N_K$ eine glatte Kurve.
Sei D ein Divisor auf V
und $p_1, \ldots, p_n$ Punkte auf V, die nicht in D vorkommen.
Der zugehörige *Goppa-Code* (Goppa, 1981) ist die Abbildung

$$\begin{array}{rcl} E : H^0(V, D) & \to & K^n \\ f & \mapsto & (f(p_1), \ldots, f(p_n)) \end{array}$$

(Beachte: $H^0(V, D) \cong K^k$, wobei $k = h^0(V, D)$.)
Fragen: $\frac{k}{n} = ?$, $d_E = ?$

Übertragungsrate.

$$k = h^0(V, D) \geqslant 1 - g(V) + \deg(D)$$

Minimalabstand. Für $f \in H^0(V, D)$ gilt

$$\begin{array}{rcl} d(E(f), 0) & = & n - \#\{\text{Nullstellen von } f\} \\ & = & n - \#\{\text{Polstellen von } f\} \\ & \geqslant & n - \deg(D) \end{array}$$

also

$$d_E \geqslant n - \deg(D)$$

Also

$$\frac{k}{n} + \frac{d}{n} \geqslant \frac{1 - g(V) + \deg(D)}{n} + \frac{n - \deg(D)}{n} \geqslant 1 + \frac{1 - g(V)}{n}$$

und andererseits

$$\frac{k}{n} + \frac{d}{n} \leqslant \frac{n+1}{n} = 1 + \frac{1}{n}$$

Ziel ist daher: Finde V mit

(1) $g(V)$ klein,

(2) n groß ($\sim V$ hat viele Punkte)

Beispiel: Kleinsche Quartik Sei $K = \mathbb{F}_8$

V die Kleinsche Quartik in $\mathbb{P}^2$,

$$V = V(x^3y + y^3z + yz^3)$$

V ist glatt. Für glatte Kurven in $\mathbb{P}^2$ gilt die *Adjunktionsformel*

$$\boxed{g(V) = 1 + \tfrac{1}{2}\deg(V) \cdot (\deg(V) - 3)}$$

Hier: $g(V) = 1 + \frac{1}{2} \cdot 4 \cdot (4 - 3) = 3$.

Wieviele Punkte $(x : y : z)$ mit $x, y, z \in K$ liegen auf V?

$(0 : 0 : 1), (0 : 1 : 0), (1 : 0 : 0)$ sind die einzigen mit $xyz = 0$.

Man kann zeigen: $\#X = 24$.

Sei P einer dieser Punkte und $P_1, \ldots, P_{23}$ die restlichen.

Wähle $D = 10P$.

Dann gilt:

$$n = 23$$
$$k \geqslant 1 - g(V) + \deg D = 1 - 3 + 10 = 8$$

Also

$$\boxed{\frac{k}{n} \geqslant \frac{8}{23}}$$

und

$$d_E \geqslant n - \deg D \geqslant 23 - 10 = 13$$

Man kann also

$$\left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{12}{2} \right\rfloor = 6$$

Fehler korrigieren.

15.4. Ein Beweis des Satzes von Riemann-Roch

Es sei V eine glatte projektive Kurve.

Informationen.

(1) Man kann jedem Divisor D auf V eine *Garbe* $\mathcal{O}_V(D)$ zuordnen.

(2) Jeder Garbe $\mathcal{F}$ auf V kann man *Kohomologiegruppen* zuordnen:

$$H^0(V,\mathcal{F}),\ H^1(V,\mathcal{F})$$

(3) Kurzschreibweisen:

$$H^0(D) := H^0(V,D) := H^0(V,\mathcal{O}_V(D))$$
$$H^1(D) := H^1(V,D) := H^1(V,\mathcal{O}_V(D))$$

Abkürzungen für die Dimensionen als K-Vektorräume:

$$h^0(D) := \dim H^0(D)$$
$$h^1(D) := \dim H^1(D)$$

(4) Es ist

$$\boxed{H^0(V,D) = \{f \in K(V)^* \mid \operatorname{div}(f) \geqslant -D\} \cup \{0\}}$$

Beispiel: Für $D = 0$ ist

$$H^0(V,0) = \{f \in K(V)^* \mid f \text{ regulär } \} \cup \{0\} \cong K$$

(5) Das *Geschlecht* der Kurve V ist die Zahl

$$\boxed{g(V) := h^1(V,0)}$$

(6) Die Satz von der *Serre-Dualität* besagt:

$$\boxed{h^1(V, D) = h^0(V, K_V - D)}$$

wobei K_V der *kanonische Divisor* auf V ist.

(7) Die Zahl

$$h^0(V, D) - h^1(V, D)$$

heißt *Euler-Charaktistik* von D.

Satz von Riemann-Roch.

$$\boxed{h^0(D) - h^1(D) = 1 - g(V) + \deg(D)}$$

Beweis. 1. Fall: $D = 0$.
Zu zeigen:

$$h^0(0) - h^1(0) = 1 - g(V) + 0$$

Folgt aus $h^0(0) = 1$.

2. Fall: D beliebig.
Sei $p \in V$. Wir zeigen:

$$\text{Behauptung gilt für } D \iff \text{Behauptung gilt für } D + p$$

Daraus folgt der Satz (mit Fall 1).
Strukturesequenz des Punkts $p \in V$:

$$\begin{array}{ccccccccc} 0 & \to & \mathcal{J}_p & \to & \mathcal{O}_V & \to & \mathcal{O}_p & \to & 0 \\ & & \| & & & & \| & & \\ & & \mathcal{O}_V(-p) & & & & K & & \end{array}$$

Tensoriere die Sequenz mit $\mathcal{O}_V(D+p)$:

$$0 \quad \to \quad \mathcal{O}_V(D) \quad \to \quad \mathcal{O}_V(D+p) \quad \to \quad \mathcal{O}_p \quad \to \quad 0$$

Die Sequenz bleibt exakt.
Die Euler-Charaktieristik ist additiv bei kurzen exakten Sequenzen, daher

$$\chi(\mathcal{O}_V(D+p)) = \chi(\mathcal{O}_V(D)) + \chi(\mathcal{O}_p)$$

Die Behauptung folgt nun aus $\chi(\mathcal{O}_p) = 1$ und

$$\deg(D+p) = \deg(D) + 1$$

□