Ruprecht-Karls-Universität Heidelberg
Interdisziplinäres Zentrum für
Wissenschaftliches Rechnen

Codierungstheorie

Bernd Heinrich Matzat
Ausarbeitung von Thorsten Lagemann

Vorwort

Vorliegendes Skriptum enthält die Ausarbeitung meiner Vorlesung Codierungstheorie aus dem Wintersemester 2003/2004 an der Universität Heidelberg. Neben den vorliegenden Kapiteln enthält diese zusätzlich einen Abschnitt über Algebraische Funktionenkörper. Da hierzu mit dem Buch von H. Stichtenoth bereits sehr gutes und preiswertes Lehrmaterial zur Verfügung steht, werden hier die wichtigsten Resultate dieses Zwischenkapitels im Anhang ohne Beweise zusammengestellt.

Der Inhalt der Vorlesungsausarbeitung gliedert sich grob in zwei Teile, deren erster ohne Kenntnisse aus der algebraischen Geometrie auskommt und daher mit *Elementare Codierungstheorie* überschrieben ist. Er enthält eine Einführung in die Grundfragen und Grundlagen der Theorie der linearen Codes. Daneben werden nach strukturellen Gesichtspunkten geordnet gängige Klassen von Codes samt zugehöriger Decodieralgorithmen vorgestellt. Zu diesen gehören u. a. Reed-Solomon-Codes, Hamming-Codes, Golay-Codes, BCH-Codes, quadratische Reste-Codes, Reed-Muller-Codes sowie die klassischen Goppa-Codes. Daneben werden einige der asymptotischen Schranken für die Informationsrate von Codes bewiesen. Insbesondere wird auch gezeigt, dass die Gilbert-Varshomov-Schranke, welche eine asymptotische untere Schranke für die Informationsrate darstellt, durch die klassischen Goppa-Codes erreicht wird.

Das zweite Kapitel ist den geometrischen Goppa-Codes gewidmet, die hier kurz *Arithmetische Codes* genannt werden. Dieses sind lineare Codes, die aus Riemann-Roch-Räumen bzw. Vektorräumen von Differentialen algebraischen Kurven gewonnen werden. Dabei werden insbesondere Codes auf rationalen, elliptischen und hyperelliptischen und auch Fermat-Kurven, die sogenannten Hermiteschen Codes, studiert und mit der MDS-Vermutung verglichen. Zudem werden Algorithmen zu deren Decodierung besprochen. Gegen Ende der Vorlesung wird das Verhalten von Codes in Türmen von Artin-Schreier-Erweiterungen untersucht. Dabei wird unter anderen auch ein Beweis für das Resultat von Garcia und Stichtenoth vorgeführt, dass es Codes über dem Norm-Spur-Turm gibt, welche die Gilbert-Varshomov-Schranke sogar übertreffen. Zur Abrundung wird abschließend gezeigt, dass jeder lineare Code als Teilkörpercode eines arithmetischen Codes (über dem gewöhnlichen Spurturm) gewonnen werden kann, womit eine in beide Richtungen begehbare Brücke zum ersten Teil geschlagen ist.

Zum Schluss dieses Vorworts möchte ich noch Herrn T. Lagemann für die geduldige und sorgfältige Ausarbeitung des Skriptums danken. Trotzdem ist nicht auszuschließen, dass sich hier und da noch eine kleine Ungenauigkeit oder ein kleiner Fehler eingeschlichen hat. Für entsprechende Hinweise bzw. Korrekturvorschläge wären wir beide sehr dankbar.

B. H. Matzat Heidelberg, den 31. Mai 2007

Inhaltsverzeichnis

Teil I

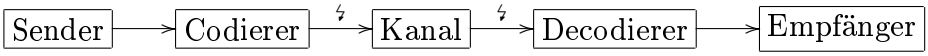
Elementare Codierungstheorie

Kapitel 1

Einführung

1.1 Das Problem der Codierungstheorie

Die Codierungstheorie ist eine recht junge mathematische Theorie, die in den 40er Jahren entstanden ist und einige mathematische Disziplinen wie die Informatik, Stochastik und Algebra vereint. Ihre Problemstellung stammt aus der Nachrichtenübermittlung:
Das Übertragen von (binären) Informationen über Telefonleitungen, Funk oder Satelliten verläuft oft nicht ungestört, da diese Informationen durch äußere Einflüsse wie schlechtes Wetter und Blitzeinschläge etc. möglicherweise zerstört oder verändert werden. Auch das Auslesen von Speichermedien ist sehr fehleranfällig, da viele Bits durch hohe Auslesegeschwindigkeit oder auch diversen Verunreinigungen der Disketten verloren gehen können. Abhilfe dagegen verschafft man sich durch Einbau von Redundanzen, die ein oder mehrere Fehler auffangen können. Zum Beispiel hat man die Möglichkeit, den Text mehrfach hintereinander zu senden, damit der Empfänger durch Vergleich der einzelnen Versionen auf die ursprüngliche schließen kann. Das Erweitern der Information mit Redundanzen nennt man *Codierung*, die Rückübersetzung der empfangenen Nachricht in den Klartext *Decodierung*.



Beispielsweise kann man jedem Buchstaben des deutschen Alphabets einen binären 5-Tupel zuordnen vermöge

$$A \mapsto 00000, B \mapsto 00001, C \mapsto 00010, \ldots.$$

Fügt man ein sechstes Bit als Quersumme hinzu, so läßt sich beim Empfang überprüfen, ob während der Übertragung ein Bit des Buchstabens verändert wurde.

Konvention. Es bezeichne A ein Alphabet, das wir ohne Einschränkung als Teilmenge eines endlichen Körpers $\mathbb{F}_q$ betrachten können. Die k-Tupel $(a_1, \ldots, a_k)$ von Buchstaben aus A nennen wir **Codewörter** oder **Blöcke**, die Menge aller Codewörter bezeichnen wir mit $B \subset \mathbb{F}_q^k$. Ein **Code** oder **Codierer** der Länge n ist eine injektive Abbildung

$$C : B \hookrightarrow \mathbb{F}_q^n$$

von B auf $C = C(B) \subset \mathbb{F}_q^n$. Wir werden einen Code C je nach Bedarf als injektive Abbildung oder als Bildmenge dieser betrachten. Zu jedem Code gibt es einen **Decodierer**

$$D : \mathbb{F}_q^n \twoheadrightarrow B$$

mit $D \circ C = \mathrm{id}_B$.

Definition 1.1. (Hamming-Abstand, Minimaldistanz, Informationsrate)
Für zwei Elemente $\boldsymbol{x} = (x_1, \ldots, x_n)$ und $\boldsymbol{y} = (y_1, \ldots, y_n)$ aus $\mathbb{F}_q^n$ definieren wir den **Hamming-Abstand** von $\boldsymbol{x}$ und $\boldsymbol{y}$ durch

$$d(\boldsymbol{x}, \boldsymbol{y}) := \#\{1 \leq i \leq n : x_i \neq y_i\}.$$

Bei einen Code $C \subset \mathbb{F}_q^n$ nennen wir den kleinsten aller Hamming-Abstände von Paaren verschiedener Codewörter, d.h. die Zahl

$$d = d(C) := \min\{d(\boldsymbol{x}, \boldsymbol{y}) : (\boldsymbol{x}, \boldsymbol{y}) \in C \times C, \boldsymbol{x} \neq \boldsymbol{y}\}$$

Minimaldistanz (oder kürzer **Distanz**) von C. Ein Code $C \subset \mathbb{F}_q^n$ der Kardinalität c und Minimaldistanz d heißt auch $(n, c)_q-$ bzw. $(n, c, d)_q-$**Code**. Das Verhältnis

$$r(C) := \frac{\log_q(C)}{n}$$

nennen wir **Informationsrate von** C.

Bemerkung 1.2. (a) *Der Hamming-Abstand genügt der Dreiecksungleichung, d.h für alle* $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \mathbb{F}_q^n$ *gilt*

$$d(\boldsymbol{x}, \boldsymbol{z}) \leq d(\boldsymbol{x}, \boldsymbol{y}) + d(\boldsymbol{y}, \boldsymbol{z}).$$

(b) *Über* $\mathbb{F}_2$ *ist der Hamming-Abstand das Quadrat des Euklidischen Abstandes, d.h. für zwei Elemente* $\boldsymbol{x} = (x_1, \ldots, x_n)$ *und* $\boldsymbol{y} = (y_1, \ldots, y_n)$ *aus* $\mathbb{F}_2^n$ *gilt*

$$d(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^{n} (x_i - y_i)^2 = \langle \boldsymbol{x}, \boldsymbol{y} \rangle^2. \qquad \square$$

Korollar 1.3. *Der Decodierer eines Codes* C *kann bis zu* $\lfloor \frac{d(C)}{2} \rfloor$ *Fehler (über das nächstgelegene Codewort) korrigieren.* $\square$

1.2 Übertragungswahrscheinlichkeit

Definition 1.4. (Binärer symmetrischer Kanal, Kapazität, Fehlerwahrscheinlichkeit eines Codes)
Ein (Nachrichtenübertragungs-)Kanal heißt **binär**, falls der Kanal nur zwei Zustände - 0 und 1 - übertragen kann. Ein binärer Kanal heißt **symmetrisch**, falls die Fehlerwahrscheinlichkeit beim Übertragen eines Bits unabhängig vom Wert (0 oder 1) des Bits ist. Ist diese Fehlerwahrscheinlichkeit $p \in [0,1]_{\mathbb{R}}$, so bezeichnet

$$K_p := 1 + p\log_2(p) + (1-p)\log_2(1-p)$$

die **Kapazität** eines binären symmetrischen Kanals. Für ein Wort $\boldsymbol{a} \in B$ sei $P(\boldsymbol{a})$ die Wahrscheinlichkeit, daß $\boldsymbol{a}$ mit dem Codierer C und Decodierer D in diesen Kanal fehlerhaft übertragen und falsch decodiert wird. Dann bezeichnet

$$P(C,D) := \frac{1}{\#C} \sum_{\boldsymbol{a}\in B} P(\boldsymbol{a})$$

die **Fehlerwahrscheinlichkeit des Codes** C. Desweiteren sei

$$P^*(c,n,p) := \min\{P(C,D) : B \overset{C}{\hookrightarrow} \mathbb{F}_2^n \overset{D}{\twoheadrightarrow} B, D\circ C = \mathrm{id}_B, \#C = c\}$$

die minimale Fehlerwahrscheinlichkeit eines binären Codes der Länge n und Kardinalität c bei Verwendung eines binären symmetrischen Kanals mit Übertragungsfehlerwahrscheinlichkeit p.

Ziel dieses Kapitels ist der Beweis des Satzes von Shannon, der besagt, daß zu jedem binären symmetrischen Kanal mit Kapazität $K_p \neq 0$ (das ist äquivalent zu $p \neq \frac{1}{2}$) "fehlerarme Codes" gibt. Genauer wird gezeigt werden:

$$\lim_{n\to\infty} P^*(c_n,n,p) = 0.$$

Dazu benötigen wir einiges an elementarem stochastischen Instrumentarium, was wir im folgenden kurz wiederholen möchten. Die Beweise können in jedem einführenden Lehrbuch (z.B. [Kre02]) nachgelesen werden.
Es seien X eine Zufallsvariable auf einer abzählbaren Menge $M = \{x_i : i \in \mathbb{N}\}$. Die Wahrscheinlichkeit, daß X den Wert x_i annimmt, sei p_i, d.h. es gelte

$$P(X = x_i) = p_i.$$

Dann heißen

$$\mu(X) = \sum_{i\in\mathbb{N}} x_i p_i \qquad \text{der Mittelwert,}$$

$$\sigma^2(X) = \sum_{i\in\mathbb{N}} x_i^2 p_i - \mu(X)^2 \qquad \text{die Varianz,}$$

und

$$\sigma = \sqrt[+]{\sigma^2} \qquad \text{die Standardabweichung}$$

der Zufallsvariablen X. Für eine Abbildung $g : M \to \mathbb{R}$ definiert

$$E(g \circ X) = \sum_{i \in \mathbb{N}} g(x_i) p_i \qquad \text{den Erwartungswert}$$

von $g \circ X$. Somit gelten

$$\mu(X) = E(X) \qquad \text{und} \qquad \sigma^2(X) = E((X - \mu(X))^2).$$

Beispiel 1.5. ((p,q)-Binomialverteilung)
Es sei X die Anzahl der Fehler, die beim Übertragen eines binären Wortes der Länge n über einem binären symmetrischen Kanals mit bitweiser Fehlerwahrscheinlichkeit p entstehen. Es ist also X definiert auf $M = \{0, \ldots, n\}$. Mit $q = 1 - p$ gilt

$$p_i = P(X = i) = \binom{n}{i} p^i q^{n-i}.$$

Der Erwartungswert von X ist also

$$\begin{aligned} E(X) = \mu(X) &= \sum_{i=0}^{n} i \binom{n}{i} p^i q^{n-i} = n \cdot \sum_{i=1}^{n} \binom{n-1}{i-1} p^i q^{n-i} \\ &= n \cdot \sum_{i=0}^{n-1} \binom{n-1}{i} p^{i+1} q^{n-i-1} = np \cdot (p+q)^{n-1} = n \cdot p \end{aligned}$$

Die Varianz von X beträgt

$$\begin{aligned} \sigma^2(X) &= \sum_{i=0}^{n} i^2 \binom{n}{i} p^i q^{n-i} - \mu(X)^2 = np \sum_{i=0}^{n-1} (i+1) \binom{n-1}{i} p^i q^{n-i-1} - n^2 p^2 \\ &= np(1 + p(n-1)) - n^2 p^2 = np - np^2 = npq. \end{aligned}$$

Bemerkung 1.6. (Tschebyschevsche Ungleichung)
Es sei X eine Zufallsvariable mit Mittelwert μ und Varianz σ^2. Dann ist die Wahrscheinlichkeit, daß die Abweichung von X zu μ mehr als ε beträgt, nicht größer als $\frac{\sigma^2}{\varepsilon^2}$. Es gilt also

$$P(|X - \mu| > \varepsilon) \leq \frac{\sigma^2}{\varepsilon^2}\,.$$

Ohne Beweis. (siehe z.B. [Kre02, Satz 3.15])

Definition 1.7. (Binäre Entropiefunktion)
Die auf $\left[0, \frac{1}{2}\right)_{\mathbb{R}}$ definierte Funktion

$$H(x) := \begin{cases} -x \log_2(X) - (1-x) \log_2(1-x) & : \text{ für } 0 < x < \frac{1}{2} \\ 0 & : \ x = 0 \end{cases}$$

heißt **binäre Entropiefunktion**. Für $\boldsymbol{x}_0 \in \mathbb{F}_2^n$ bezeichnet

$$\mathbb{B}_r^n(\boldsymbol{x}_0) = \{\boldsymbol{x} \in \mathbb{F}_2^n : d(\boldsymbol{x}, \boldsymbol{x}_0) \leq r\}$$

die Kugel vom Radius r in $\mathbb{F}_2^n$ bezüglich des Hamming-Abstands. Die Kugel $\mathbb{B}_r^n(\mathbf{0})$ um $\mathbf{0} = (0, \ldots, 0)$ bezeichnen wir kürzer auch mit $\mathbb{B}_r^n$

Bemerkung 1.8. *Für $\delta \in \left[0, \frac{1}{2}\right]$ gelten:*

(a) *Die Anzahl der Gitterpunkte in der Kugel $\mathbb{B}_{\delta n}^n$ vom Radius δn beträgt*

$$\#\mathbb{B}_{\delta n}^n = \sum_{i=0}^{\lfloor \delta n \rfloor} \binom{n}{i} \leq 2^{nH(\delta)}.$$

(b) *Beim Grenzübergang $n \to \infty$ wird aus der Abschätzung in (a) eine Gleichung*

$$\lim_{n\to\infty} \left(\frac{1}{n} \log_2(\#\mathbb{B}_{\delta n}^n) \right) = H(\delta).$$

Beweis. Wir beweisen lediglich die Aussage (a), da wir Aussage (b) in diesen Kapitel nicht benötigen und später allgemeiner beweisen werden (Lemma 9.8).

Die Gleichheit von $\#\mathbb{B}_{\delta n}^n$ und $\sum_{i=0}^{\lfloor \delta n \rfloor} \binom{n}{i}$ ist offensichtlich, da $\binom{n}{i}$ die Anzahl der binären Wörter $\boldsymbol{x} \in \mathbb{F}_2^n$ mit Gewicht i bzw. mit Hamming-Abstand $d(\boldsymbol{x}, \mathbf{0}) = i$ ist. Nach Voraussetzung gilt $\delta \leq \frac{1}{2} \leq 1 - \delta$. Daraus ergibt sich die Abschätzung

$$\begin{aligned} 1 = (\delta + 1 - \delta)^n &= \sum_{i=0}^{n} \binom{n}{i} \delta^i (1-\delta)^{n-i} = \sum_{i=0}^{n} \binom{n}{i} (1-\delta)^n \left(\frac{\delta}{1-\delta} \right)^i \\ &\geq \sum_{i=0}^{\lfloor \delta n \rfloor} \binom{n}{i} (1-\delta)^n \left(\frac{\delta}{1-\delta} \right)^i \geq (1-\delta)^n \left(\frac{\delta}{1-\delta} \right)^{\delta n} \cdot \sum_{i=0}^{\lfloor \delta n \rfloor} \binom{n}{i}. \end{aligned}$$

Aufgrund

$$\begin{aligned} \log_2 (1-\delta)^n \left(\frac{\delta}{1-\delta} \right)^{\delta n} &= n \cdot (\log_2(1-\delta) + \delta \log_2 \left(\frac{\delta}{1-\delta} \right)) \\ &= n \cdot (\delta \log_2(\delta) + (1-\delta)\log_2(1-\delta)) = -n \cdot H(\delta) \end{aligned}$$

folgt hieraus die gewünschte Ungleichung

$$1 \geq 2^{-n \cdot H(\delta)} \cdot \sum_{i=0}^{\lfloor \delta n \rfloor} \binom{n}{i}. \qquad \square$$

Bemerkung 1.9. *Für zwei (stochastisch) unabhängige Zufallsvariablen X und Y gelten:*

(a) $E(X + Y) = E(X) + E(Y)$.

(b) $E(X \cdot Y) = E(X) \cdot E(Y)$.

Ohne Beweis. (siehe z.B. [Kre02, Satz 3.7])

1.3 Der Satz von Shannon

Satz 1.10. (Shannon 1948)
Es sei K_p die Kapazität eines binären symmetrischen Kanals mit $K_p \neq 0$. Desweiteren seien $0 < R < K_p$ und $c_n := 2^{\lfloor Rn \rfloor}$. Dann gilt

$$\lim_{n\to\infty} P^*(c_n, n, p) = 0.$$

Für hinreichend große Wortlängen n gibt es also fehlerarme Codes.

Beweis. Ohne Einschränkung kann $p \leq \frac{1}{2}$ angenommen werden, da man andernfalls die Interpretation der empfangenen Daten anpaßt, d.h. eine empfangene 1 wird als 0 interpretiert. Desweiteren ist $p \neq \frac{1}{2}$ aufgrund $K_p \neq 0$. Es sei

$$C = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_c\} \subset \mathbb{F}_2^n$$

ein binärer Code der Länge n und Kardinalität c. Die Zufallsvariable Y bezeichne die Anzahl der Fehler beim Übertragen und Decodieren eines Codewortes $\boldsymbol{x} \in C$. Da zur Übermittlung ein binärer symmetrischen Kanal mit bitweiser Fehlerwahrscheinlichkeit p verwendet wird, ist Y wie in Beispiel 1.5 (p, q)-binomialverteilt. Somit ist $\mu = E(Y) = np$ der Erwartungswert und $\sigma^2(Y) = npq$ die Varianz von Y. Für $\varepsilon > 0$ und $s := \sqrt{\frac{2}{\varepsilon} npq}$ gilt nach der Ungleichung von *Tschebyschev*

$$P(|Y - \mu| \geq s) \leq \frac{npq}{s^2} = \frac{\varepsilon}{2}\,.$$

Wir setzen $\rho := \lfloor np + s \rfloor$. Wegen $p < \frac{1}{2}$ gilt $\rho < \frac{n}{2}$ für große n. Nach Bemerkung 1.8 hat dies

$$\#\mathbb{B}_\rho^n = \sum_{i=0}^{\rho} \binom{n}{i} \leq 2^{\,n \cdot H(\frac{\rho}{n})}$$

zur Folge. Für zwei Elemente $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_2^n$ definieren wir

$$f(\boldsymbol{x}, \boldsymbol{y}) := \begin{cases} 0 & \text{bei } d(\boldsymbol{x}, \boldsymbol{y}) > \rho \\ 1 & \text{bei } d(\boldsymbol{x}, \boldsymbol{y}) \leq \rho \end{cases}$$

und

$$g_i(\boldsymbol{y}) := 1 - f(\boldsymbol{y}, \boldsymbol{x}_i) + \sum_{j \neq i} f(\boldsymbol{y}, \boldsymbol{x}_j).$$

Der Wert $g_i(\boldsymbol{y})$ verschwindet genau dann, wenn $\boldsymbol{x}_i$ das einzige Codewort in der Kugel $\mathbb{B}_\rho^n(\boldsymbol{y})$ ist und sonst gilt $g_i(\boldsymbol{y}) \geq 1$. Wir decodieren vermöge

$$D(\boldsymbol{y}) := \begin{cases} \boldsymbol{x}_i & \text{falls } g_i(\boldsymbol{y}) = 0, \\ \boldsymbol{x}_1 & \text{sonst.} \end{cases}$$

Bezeichnen nun $P(\boldsymbol{x}_i)$ die Wahrscheinlichkeit, daß $\boldsymbol{x}_i$ falsch decodiert wird und $P(\boldsymbol{y}|\boldsymbol{x}_i)$ die bedingte Wahrscheinlichkeit, daß beim Senden von $\boldsymbol{x}_i$ das Wort $\boldsymbol{y}$ empfangen wird und nicht als $\boldsymbol{x}_i$ decodiert wird, so gilt

$$P(\boldsymbol{x}_i) \leq \sum_{\boldsymbol{y}\in\mathbb{F}_2^n} P(\boldsymbol{y}|\boldsymbol{x}_i)g_i(\boldsymbol{y}) = \sum_{\boldsymbol{y}\in\mathbb{F}_2^n} P(\boldsymbol{y}|\boldsymbol{x}_i)(1-f(\boldsymbol{y},\boldsymbol{x}_i))+\sum_{\boldsymbol{y}\in\mathbb{F}_2^n} P(\boldsymbol{y}|\boldsymbol{x}_i)\sum_{j\neq i} f(\boldsymbol{y},\boldsymbol{x}_j).$$

Der erste Summand nach dem Gleichheitszeichen entspricht der Wahrscheinlichkeit, daß beim Übertragen von $\boldsymbol{x}_i$ mehr als ρ Fehler passieren und somit $\boldsymbol{x}_i$ nicht richtig decodiert wird. Es gilt wie oben nach der *Tschebyschevschen Ungleichung*

$$\sum_{\boldsymbol{y}\in\mathbb{F}_2^n} P(\boldsymbol{y}|\boldsymbol{x}_i)(1-f(\boldsymbol{y},\boldsymbol{x}_i)) = P(Y>\rho) \leq \frac{\varepsilon}{2}\,.$$

Die Fehlerwahrscheinlichkeit von C kann also durch

$$P(C,D) = \frac{1}{c}\sum_{i=1}^{c} P(\boldsymbol{x}_i) \leq \frac{\varepsilon}{2} + \frac{1}{c}\sum_{i=1}^{c}\sum_{\boldsymbol{y}\in\mathbb{F}_2^n}\sum_{j\neq i} P(\boldsymbol{y},\boldsymbol{x}_i)f(\boldsymbol{y},\boldsymbol{x}_j)$$

abgeschätzt werden. Der Grundgedanke des Beweises ist nun, daß der Minimalwert $P^*(c,n,p)$ kleiner oder gleich dem Erwartungswert der Fehlerwahrscheinlichkeit $P(C,D)$ von allen Codes $C\subset\mathbb{F}_2^n$ der Mächtigkeit c und der Decodierregel D ist. Aufgrund der stochastischen Unabhängigkeit der Variablen $P(\boldsymbol{y}|\boldsymbol{x}_i)$ und $f(\boldsymbol{y},\boldsymbol{x}_i)$ gilt dann nach Bemerkung 1.9

$$\begin{aligned}
P^*(c,n,p) &\leq \frac{\varepsilon}{2} + \frac{1}{c}\sum_{i=1}^{c}\sum_{\boldsymbol{y}\in\mathbb{F}_2^n}\sum_{j\neq i} E(P(\boldsymbol{y},\boldsymbol{x}_i))\cdot E(f(\boldsymbol{y},\boldsymbol{x}_j)) \\
&= \frac{\varepsilon}{2} + \frac{1}{c}\sum_{i=1}^{c}\sum_{\boldsymbol{y}\in\mathbb{F}_2^n}\sum_{j\neq i} E(P(\boldsymbol{y},\boldsymbol{x}_i))\cdot\frac{\#\mathbb{B}_\rho^n(\boldsymbol{y})}{\#\mathbb{F}_2^n} \\
&= \frac{\varepsilon}{2} + \frac{c-1}{c}\cdot\frac{\#\mathbb{B}_\rho^n}{2^n}\sum_{i=1}^{c}\sum_{\boldsymbol{y}\in\mathbb{F}_2^n} E(P(\boldsymbol{y},\boldsymbol{x}_i)) \\
&= \frac{\varepsilon}{2} + (c-1)\frac{\#\mathbb{B}_\rho^n}{2^n}\cdot\frac{1}{c}\sum_{i=1}^{c} E\left(\sum_{\boldsymbol{y}\in\mathbb{F}_2^n} P(\boldsymbol{y},\boldsymbol{x}_i)\right) \\
&\leq \frac{\varepsilon}{2} + (c-1)\frac{\#\mathbb{B}_\rho^n}{2^n}\,.
\end{aligned}$$

Hieraus folgt nun aus Bemerkung 1.8

$$\begin{aligned}
\frac{1}{n}\,\log_2\left(P^*(c,n,p)-\frac{\varepsilon}{2}\right) &\leq \frac{1}{n}\log_2(c-1) + \frac{1}{n}\log_2\frac{\#\mathbb{B}_\rho^n}{2^n} \\
&\leq \frac{1}{n}\log_2(c) + \frac{1}{n}(n\,H\left(\frac{\rho}{n}\right)-n).
\end{aligned}$$

Wegen

$$\frac{\rho}{n}\log_2(\frac{\rho}{n}) = p\log_2(p) + \mathcal{O}(\sqrt{n}^{-1})$$

und

$$\left(1-\frac{\rho}{n}\right)\log_2\left(1-\frac{\rho}{n}\right) = q\log_2(q) + \mathcal{O}(\sqrt{n}^{-1})$$

gilt dann $H\left(\frac{\rho}{n}\right) = -p\log_2(p) - q\log_2(q)$ und somit

$$\begin{aligned}\frac{1}{n}\ \log_2\left(P^*(c,n,p) - \frac{\varepsilon}{2}\right) &\leq \frac{1}{n}\log_2(c) - (1 + p\log_2(p) + q\log_2(q)) + \mathcal{O}(\sqrt{n}^{-1}) \\ &= \frac{1}{n}\log_2(c) - K_p + \mathcal{O}(\sqrt{n}^{-1}).\end{aligned}$$

Durch Substitution von c durch $c_n = 2^{\lfloor Rn \rfloor}$ erhält man wegen $R < K_p$

$$\frac{1}{n}\ \log_2\left(P^*(c_n,n,p) - \frac{\varepsilon}{2}\right) \leq R - K_p + \mathcal{O}(\sqrt{n}^{-1}) = -\gamma < 0$$

für ein positives γ und hinreichend große n. Somit ist

$$P^*(n,c_n,p) \leq \frac{\varepsilon}{2} + \frac{1}{2^{\gamma n}},$$

was für $n \to \infty$ gegen $\frac{\varepsilon}{2}$ strebt. Da ε beliebig klein gewählt werden kann, folgt hieraus der Satz von Shannon. □

Kapitel 2

Lineare Codes

2.1 Einführung linearer Codes

Allgemeine Codes $C \subset \mathbb{F}_q^n$ sind meist unübersichtlich und i.a. schwierig zu codieren und zu decodieren. Besser wird es mit einer zusätzlichen Vektorraumstruktur.

Definition 2.1. (Linearer Code, Gewicht von Codewörtern)
Einen Code $C \subset \mathbb{F}_q^n$ nennen wir **linear**, falls C ein Untervektorraum von $\mathbb{F}_q^n$ ist. Lineare Codes in $\mathbb{F}_q^n$ der Dimension k bezeichnen wir als $[n,k]_q-$**Code** bzw. als $[n,k,d]_q-$**Code**, wenn d die Minimaldistanz des Codes ist. Für ein Codewort $\boldsymbol{x} \in C$ heißt die natürliche Zahl

$$w(\boldsymbol{x}) := d(\boldsymbol{x}, \boldsymbol{0})$$

das **Gewicht** (bzw. die **Hamming-Norm**) von $\boldsymbol{x}$.

Anmerkung 2.2. Die Informationsrate eines (linearen) $[n,k]_q-$Code C ist der Quotient aus Dimension und Länge von C, d.h. es ist

$$r(C) = \frac{\log_q(\#C)}{n} = \frac{k}{n}.$$

Bemerkung 2.3. *Für einen linearen Code $C \leq \mathbb{F}_q^n$ gelten:*

(a) *Der Hamming-Abstand zweier Codewörter $\boldsymbol{x}, \boldsymbol{y}$ aus C ist identisch mit dem Gewicht ihrer Differenz, d.h. es gilt*

$$d(\boldsymbol{x}, \boldsymbol{y}) = w(\boldsymbol{x} - \boldsymbol{y}).$$

(b) *Die Minimaldistanz von C entspricht den minimalem Gewicht nichtverschwindender Codewörter aus C, d.h. es ist*

$$d(C) = \min\{w(\boldsymbol{x}) : \boldsymbol{0} \neq \boldsymbol{x} \in C\}.$$

Beweis. Man beachte, daß lineare Codes stets die Differenz ihrer Codewörter sowie auch das Nullwort $\mathbf{0} = (0, \ldots, 0)$ enthalten. Daher folgen die Aussagen (a) und (b) aus

$$d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{x} - \boldsymbol{y}, \mathbf{0}) = w(\boldsymbol{x} - \boldsymbol{y})$$

für $\boldsymbol{x}, \boldsymbol{y} \in C$. □

Als *Codierer* eines linearen Codes fungiert die sogenannte Erzeugermatrix. Dazu die

Definition 2.4. (Erzeugermatrix, Symmetriegruppe)
Es sei C ein $[n,k]_q-$Code mit Basis $\boldsymbol{x_1} = (x_{11}, \ldots, x_{1n}), \boldsymbol{x_2}, \ldots, \boldsymbol{x_k} \in \mathbb{F}_q^n$. Dann heißt die $k \times n-$Matrix

$$G = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{k1} & \cdots & x_{kn} \end{pmatrix}$$

eine **Erzeuger-** bzw. eine **Generatormatrix** von C. Eine Erzeugermatrix G von C nennen wir **reduziert**, falls G die Gestalt

$$G = (I_k|P) = \left(\begin{array}{ccc|c} 1 & & 0 & \\ & \ddots & & P \\ 0 & & 1 & \end{array}\right)$$

mit $P \in \mathbb{F}_q^{k\times(n-k)}$ hat. Dann sagen wir auch, daß G in **Standardform** vorliegt. Zwei Codes $C, \tilde{C}$ aus $\mathbb{F}_q^n$ heißen **äquivalent**, wenn es eine Permutation σ von n Elementen gibt, sodaß gilt:

$$(x_1, \ldots, x_n) \in C \Longleftrightarrow (x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \in \tilde{C}.$$

Ist $C = \tilde{C}$, so nennen wir σ eine **Symmetrie** von C. Die Menge aller Symmetrien des Codes C

$$\mathrm{Sym}(C) := \{\sigma \in S_n : \sigma \text{ ist Symmetrie von } C\}$$

heißt **Symmetriegruppe** von C.

Anmerkung 2.5. (a) Betrachtet man eine Erzeugermatrix G eines Codes C als lineare Abbildung von $\mathbb{F}_q^k$ in $\mathbb{F}_q^n$, so ist C das Bild von $\mathbb{F}_q^k$ unter G, d.h es gilt

$$C = \{\boldsymbol{a} \cdot G : \boldsymbol{a} \in \mathbb{F}_q^k\}.$$

Offensichtlich ist G injektiv und dient somit als Codierer von C.
(b) Ist G in Standardform, so bilden die ersten k Koordinaten $x_1, \ldots, x_k$ eines Codewortes $\boldsymbol{x}$ die **Informationssymbole** (information symbols) und die letzten $n-k$ Koordinaten $x_{k+1}, \ldots, x_n$ die **Kontrollsymbole** (parity check symbols) von $\boldsymbol{x}$.

Bemerkung 2.6. *Zu jedem linearen Code gibt es einen äquivalenten Code mit reduzierter Erzeugermatrix.*

Beweis. Es seien C ein (linearer) $[n,k]_q-$Code und G eine Erzeugermatrix von C. Dann gibt es eine Permutationsmatrix $Q \in \mathbf{GL}_n(\mathbb{F}_q)$, sodaß die ersten k Spalten von $\tilde{G} := G \cdot Q$ linear unabhängig sind. Also hat $\tilde{G}$ die Gestalt $(\tilde{J}|\tilde{P})$ mit $\tilde{J} \in \mathbf{GL}_k(\mathbb{F}_q)$. Unter der Basistransformation $\tilde{J}^{-1}$ besitzt der Code $\tilde{C} := \mathbb{F}_q^k \cdot \tilde{G}$ eine reduzierte Erzeugermatrix und ist wegen $C \cdot Q = \tilde{C}$ äquivalent zu C. □

Beispiel 2.7. (1) Der *n-fache Wiederholungscode* $C = \{\boldsymbol{x} \in \mathbb{F}_q^n : x_1 = \ldots = x_n\}$ besitzt die Erzeugermatrix $G_1 = (1, \ldots, 1)$.
(2) Es sei $C \leq \mathbb{F}_2^4$ ein linearer $[4,3]_2-$Code mit der Bedingung $\sum_{i=1}^4 x_i = 0$ an ein Codewort $\boldsymbol{x} \in C$. Dann besitzt C die Erzeugermatrix

$$G_2 = (I_3|P_2) = \left(\begin{array}{ccc|c} 1 & \cdot & \cdot & 1 \\ \cdot & 1 & \cdot & 1 \\ \cdot & \cdot & 1 & 1 \end{array}\right).$$

Allgemein heißen solche $[n, n-1, 2]_q-$Codes *parity check Codes* (der Länge n).
(3) Betrachten wir nun den $[6,3]_2-$Code C' mit den Bedingungen $x_4 = x_2 + x_3$, $x_5 = x_1 + x_3$ und $x_6 = x_1 + x_2$ für ein Codewort $(x_1, \ldots, x_6) \in C'$. Dann sind die Koeffizienten $x_1, x_2, x_3 \in \mathbb{F}_2$ die Informationssymbole und x_4, x_5, x_6 die Kontrollsymbole von C', und es ist

$$G_3 = (I_3|P_3) = \left(\begin{array}{ccc|ccc} 1 & \cdot & \cdot & \cdot & 1 & 1 \\ \cdot & 1 & \cdot & 1 & \cdot & 1 \\ \cdot & \cdot & 1 & 1 & 1 & \cdot \end{array}\right)$$

eine Erzeugermatrix von C'.

2.2 Duale Codes

Die Codierer linearer Code sind lineare Einbettungen $\mathbb{F}_q^k \hookrightarrow \mathbb{F}_q^n$, die durch die Erzeugermatrizen leicht beschrieben werden können. Zur Decodierung verwendet man sogenannte Kontrollmatrizen, die in diesen Abschnitt definiert und untersucht werden.

Definition 2.8. (Dualer Code, Kontrollmatrix, selbstdualer Code)
Für zwei Elemente $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$ bezeichnet

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle := \sum_{i=1}^{n} x_i y_i$$

das Standardskalarprodukt in $\mathbb{F}_q^n$. Für einen linearen Code $C \leq \mathbb{F}_q^n$ heißt

$$C^\perp := \{\boldsymbol{y} \in \mathbb{F}_q^n : \langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0 \text{ für alle Codewörter } \boldsymbol{x} \in C\}$$

der zu C **duale Code**. Im Falle $C = C^\perp$ nennen wir C **selbstdual**. Die Erzeugermatrix H von $C^\perp$ heißt **Kontrollmatrix** zu C.

Bemerkung 2.9. *Für einen $[n,k]_q-$Code C gelten:*

(a) *Der zu C duale Code $C^\perp$ ist ein $[n, n-k]_q-$Code.*

(b) *Die Dualisierung $(\,\cdot\,)^\perp$ von linearen Codes wirkt involutiv, d.h. es ist*

$$\left(C^\perp\right)^\perp = C.$$

Beweis. Es ist $C^\perp$ der zu C orthogonale Raum in $\mathbb{F}_q^{\,n}$. Aus der linearen Algebra ist bekannt, daß sich dann die Dimensionen von C und $C^\perp$ zu n aufsummieren. Also hat $C^\perp$ die Dimension $n-k$. Mit der Definition 2.8 gilt unmittelbar $C \leq \left(C^\perp\right)^\perp$. Aus Dimensionsgründen folgt dann die Gleichheit. □

Korollar 2.10. *Ein selbstdualer Code der Länge n hat Dimension $\frac{n}{2}$ und Informationsrate $\frac{1}{2}$.* □

Korollar 2.11. (Kontrollgleichung)
Für einen linearen Code $C \leq \mathbb{F}_q^{\,n}$ mit Kontrollmatrix H gilt die Gleichheit

$$C = \{\boldsymbol{x} \in \mathbb{F}_q^{\,n} : H \cdot \boldsymbol{x}^T = \mathbf{0}\}.$$ □

Bemerkung 2.12. *Es sei $G = (I_k|P)$ die reduzierte Erzeugermatrix eines $[n,k]_q-$Codes C. Dann hat die Kontrollmatrix von C die Gestalt*

$$H = (-P^T|I_{n-k}).$$

Beweis. Die Zeilen der Erzeugermatrix G bilden eine Basis von C. Wegen

$$(-P^T|I_{n-k}) \cdot \begin{pmatrix} I_k \\ P^T \end{pmatrix} = 0$$

folgt die Behauptung aus Korollar 2.11. □

Beispiel 2.13. Wir betrachten die dualen Codes zu Beispiel 2.7.
(1) und (2): Man sieht leicht, daß der n-fache Wiederholungscode und der parity check Code der Länge n dual zueinander sind. Somit bildet

$$H_1 = \left(\begin{array}{ccc|c} 1 & & 0 & 1 \\ & \ddots & & \vdots \\ 0 & & 1 & 1 \end{array}\right)$$

eine Kontrollmatrix zum n-fachen Wiederholungscode (und ist gleichzeitig eine Erzeugermatrix des parity check Codes). Weiter ist

$$H_2 = (1,1,1,1)$$

die Kontrollmatrix des in (2) definierten parity check Code (der Länge 4).
(3) Die Kontrollmatrix dieses Codes hat die Gestalt

$$H_3 = \left(\begin{array}{ccc|ccc} \cdot & 1 & 1 & 1 & \cdot & \cdot \\ 1 & \cdot & 1 & \cdot & 1 & \cdot \\ 1 & 1 & \cdot & \cdot & \cdot & 1 \end{array}\right)$$

Decodieralgorithmus 2.14. Sender und Empfänger einigen sich auf einen linearen Code C mit Erzeugermatrix G und Kontrollmatrix H. Es sei $\boldsymbol{y} \in \mathbb{F}_q^n$ die empfangene Nachricht.

(1) Bilde das sogenannte **Syndrom** $\boldsymbol{z} = H \cdot \boldsymbol{y}^T \in \mathbb{F}_q^{n-k}$ zu $\boldsymbol{y}$.

(2) Ermittle ein Element $\boldsymbol{e} \in \mathbb{F}_q^n$ vom minimalem Gewicht mit $H \cdot \boldsymbol{e}^T = \boldsymbol{z}$.

(3) Das Element $\tilde{\boldsymbol{y}} := \boldsymbol{y} - \boldsymbol{e}$ ist dann ein Codewort aus C mit minimalen Hamming-Abstand zu $\boldsymbol{y}$.

(4) Ist G reduziert, so ist $(\tilde{y}_1, \ldots, \tilde{y}_k)$ die decodierte Nachricht (ohne die Kontrollsymbole).

Anmerkung 2.15. Das Element $\boldsymbol{e}$ nennt man als Nebenklassenführer der Klasse $\boldsymbol{y} + C \in \mathbb{F}_q^n/C$ auch **Fehlervektor**. Die Komplexität beim Erstellen der Tabelle von Fehlervektoren steigt bei großen Codes erheblich an. Daher ist der Decodieragorithmus 2.14 in der Regel nicht optimal.

Bemerkung 2.16. *Für die Minimaldistanz eines linearen Codes mit Kontrollmatrix H gelten:*

$$\begin{aligned} d(C) &= \min\{l \geq 1 : \text{ es gibt } l \text{ linear abhängige Spalten in } H\} \\ &= \max\{l \geq 1 : \text{jeweils } (l-1) \text{ Spalten von } H \text{ sind linear unabhängig}\}. \end{aligned}$$

Beweis. Die zweite Gleichheit ist klar. Für den Nachweis der ersten Gleichung bezeichnen wir die Spalten von H mit $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n$. Die Codewörter $\boldsymbol{x} \neq 0$ aus C liefert mit der Kontrollgleichung

$$\sum_{i=1}^{n} x_i \boldsymbol{s}_i = H \cdot \boldsymbol{x}^T = 0$$

eine nichttriviale Linearkombination von 0. Ist also $\boldsymbol{x}$ ein Codewort von minimalem Gewicht d, so gibt es Indices $i_1, \ldots, i_d$ mit $x_{i_1}, \ldots, x_{i_d} \neq 0$ (und $x_i = 0$ bei $i \neq i_j$ für $1 \leq j \leq d$). Mit der Kontrollgleichung folgt dann die lineare Abhängig der Spalten $\boldsymbol{s}_{i_1}, \ldots, \boldsymbol{s}_{i_d}$. Das zeigt $d(C) \geq \min\{l \geq 1 : \text{ es gibt } l \text{ linear abhängige Spalten in } H\}$. Seien umgekehrt die Spalten $\boldsymbol{s}_{i_1}, \ldots, \boldsymbol{s}_{i_l}$ linear abhängig. Dann gibt es eine nichttriviale Linearkombination

$$\sum_{j=1}^{l} x_{i_j} \boldsymbol{s}_j = 0$$

mit Koeffizienten $x_{i_j} \in \mathbb{F}_q$ für $1 \leq j \leq l$. Das Codewort $\boldsymbol{x} = (x_1, \ldots, x_n)$ definiert durch

$$x_i = \begin{cases} x_{i_j} & : \text{ falls } i = i_j \text{ für } 1 \leq j \leq l \\ 0 & : \text{ sonst} \end{cases}$$

erfüllt dann die Kontrollgleichung $H \cdot \boldsymbol{x}^T = 0$ und ist somit ein Codewort aus C vom Gewicht l. Das schließt unseren Beweis. □

Beispiel 2.17. Wir untersuchen nun die Minimaldistanz der in den Beispielen 2.7 und 2.13 behandelten Codes.
(1) Die Minimaldistanz n-facher Wiederholungscodes ist (natürlich) n. Daher hat dieser Code die Parameter $[n, 1, n]_q$.
(2) Die Parameter der parity check Codes sind $[n, n-1, 2]_q$. Diese Codes können also lediglich 1 Fehler erkennen. Im Fall $q = 2$ und somit in unserem konkreten Beispiel ist dies sogar nur bei ungerader Fehleranzahl bei der Nachrichtenübermittlung möglich.
(3) Die Minimaldistanz dieses Codes ist 3. Dieser Code ermöglicht also dem Nutzer das Erkennen und Korrigieren eines Fehlers.
(4) Die Matrix

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \cdot & \cdot & 1 & \cdot & 1 & \cdot \\ \cdot & \cdot & 1 & \cdot & 1 & 1 & 1 & \cdot \\ 1 & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot \end{pmatrix}$$

erzeugt einen $[8, 4]_2-$Code C. Wegen $G \cdot G^T = 0$ ist C selbstdual. Mit einen kritischen Blick kann man sich davon überzeugen, daß G jeweils drei linear unabhängige Spalten besitzt. Somit gilt für die Minimaldistanz $d(C) \geq 1 + 3 = 4$. Da C Codewörter vom Gewicht 4 enthält (z.B. der dritte Zeilenvektor von G) folgt $d(C) = 4$. Somit ist C ein selbstdualer $[8, 4, 4]_2-$Code.

2.3 Das Gewichtspolynom

Definition 2.18. (Gewichtspolynom, Spektrum, erzeugende Funktion)
Es sei C ein linearer Code über $\mathbb{F}_q$ der Länge n. Die Anzahl aller Codewörter vom Gewicht r bezeichnen wir mit

$$w_r(C) := \#\{\boldsymbol{x} \in C : w(\boldsymbol{x}) = r\}.$$

Das **Spektrum** eines Codes ist die Menge $\{w_r(C) : 0 \leq r \leq n\}$. Das ganzzahlige homogene Polynom

$$W_C(X, Y) := \sum_{r=0}^{n} w_r(C) X^{n-r} Y^r$$

nennen wir **Gewichtspolynom** von C. Die **erzeugende Funktion** des Codes C ist durch

$$W_C(X) := W_C(X, 1) = \sum_{s=0}^{n} w_{n-s}(C) X^s$$

definiert.

Anmerkung 2.19. Das Gewichtspolynom eines linearen Codes C der Länge n und Minimaldistanz d hat die Gestalt

$$W_C(X, Y) = X^n + \sum_{r=d}^{n} w_r(C) X^{n-r} Y^r.$$

Lemma 2.20. *Es seien G eine endliche Gruppe und χ ein Charakter von G, d.h. ein Gruppenhomorphismus von G in $\mathbb{C}^\times$. Dann gilt*

$$\sum_{g\in G}\chi(g) = \begin{cases} \#G & \text{für } \chi = 1 \\ 0 & \text{sonst.} \end{cases}$$

Beweis. Die Aussage für $\chi = 1$ ist trivial. Im Fall $\chi \neq 1$ gibt es ein Gruppenelement $h \in G$ mit $\chi(h) \neq 1$. Aufgrund der Homomorphieeigenschaft von χ und der Transitivität der Linkstranslation von Gruppenelementen folgt dann

$$(\chi(h)-1)\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(h)\cdot\chi(g) - \sum_{g\in G}\chi(g) = \sum_{h\cdot g\in G}\chi(h\cdot g) - \sum_{g\in G}\chi(g) = 0$$

und somit $\sum_{g\in G}\chi(g) = 0$. □

Satz 2.21. (MacWilliams - Identität)
Die Gewichtspolynome eines linearen $[n,k]_q-$Code C und dessen dualem Code $C^\perp$ erfüllen die Gleichheit

$$W_{C^\perp}(X,Y) = \frac{1}{q^k}\, W_C(X+(q-1)Y,\ X-Y).$$

Beweis. Wir setzen $V := \mathbb{F}_q^n$. Es sei $\chi : \mathbb{F}_q \to \mathbb{W}_m \leq \mathbb{C}^\times$ ein nichttrivialer additiver Charakter von $\mathbb{F}_q$, wobei $\mathbb{W}_m$ die Menge der m-ten Einheitswurzeln in $\mathbb{C}$ bezeichne. Für einen Vektor $\boldsymbol{x} \in V$ definiert

$$\chi_{\boldsymbol{x}} : \begin{cases} V & \longrightarrow & \mathbb{C}^\times \\ \boldsymbol{y} & \longmapsto & \chi(\langle \boldsymbol{x}, \boldsymbol{y}\rangle) \end{cases}$$

einen additiven Charakter von V. Man beachte, daß wegen der Symmetrie des Skalarproduktes stets $\chi_{\boldsymbol{x}}(\boldsymbol{y}) = \chi_{\boldsymbol{y}}(\boldsymbol{x})$ gilt. Die Einschränkung von $\chi_{\boldsymbol{x}}$ auf C definiert ebenfalls einen Charakter. Für einen $\mathbb{Z}[\mathbb{W}_m]$-Modul M und eine Abbildung $f : V \to M$ setzen wir

$$\hat{f} : \begin{cases} V & \longrightarrow & M \\ \boldsymbol{x} & \longmapsto & \sum_{\boldsymbol{y}\in V}\chi_{\boldsymbol{x}}(\boldsymbol{y})f(\boldsymbol{y}). \end{cases}$$

Die Summation der Bilder aller Codewörter unter $\hat{f}$ ergibt dann nach Lemma 2.20

$$\begin{aligned}\sum_{\boldsymbol{x}\in C}\hat{f}(\boldsymbol{x}) &= \sum_{\boldsymbol{x}\in C}\sum_{\boldsymbol{y}\in V}\chi_{\boldsymbol{x}}(\boldsymbol{y})f(\boldsymbol{y}) = \sum_{\boldsymbol{y}\in V} f(\boldsymbol{y})\sum_{\boldsymbol{x}\in C}\chi_{\boldsymbol{x}}(\boldsymbol{y}) \\ &= \sum_{\boldsymbol{y}\in V} f(\boldsymbol{y})\sum_{\boldsymbol{x}\in C}\chi_{\boldsymbol{y}}(\boldsymbol{x}) = \sum_{\boldsymbol{y}\in C^\perp} f(\boldsymbol{y})\cdot \#C,\end{aligned}$$

da der Charakter $\chi_{\boldsymbol{y}}$ von C genau dann konstant 1 ist, wenn $\boldsymbol{y}$ ein Codewort des dualen Codes $C^\perp$ ist.

Nun verwenden wir für M den Modul $\mathbb{C}[X,Y]_n$ der komplexwertigen homogenen Polynome vom Grad n. M ist dann ein $\mathbb{Z}[\mathbb{W}_m]$-Modul via Linksmultiplikation. Zudem setzen wir

$$f : \begin{cases} V & \to & \mathbb{C}[X,Y]_n \\ \boldsymbol{x} & \longmapsto & X^{n-w(\boldsymbol{x})}Y^{w(\boldsymbol{x})}. \end{cases}$$

Dann erfüllt das Gewichtspolynom des dualen Codes $C^\perp$ die Gleichungen

$$W_{C^\perp}(X,Y) = \sum_{\boldsymbol{x}\in C^\perp} f(\boldsymbol{x}) = \frac{1}{\#C} \sum_{\boldsymbol{x}\in C} \hat{f}(\boldsymbol{x}).$$

Die Behauptung des Satzes folgt also mit dem Nachweis von

$$\hat{f}(\boldsymbol{x}) = (X+(q-1)Y)^{n-w(\boldsymbol{x})}(X-Y)^{w(\boldsymbol{x})}.$$

Per Definition von $\hat{f}$ und $\chi_{\boldsymbol{x}}$ gelten die beiden Gleichungen

$$\begin{aligned} \hat{f}(\boldsymbol{x}) &= \sum_{\boldsymbol{y}\in V} \chi_{\boldsymbol{x}}(\boldsymbol{y}) X^{n-w(\boldsymbol{y})}Y^{w(\boldsymbol{y})} \\ &= \sum_{\boldsymbol{y}\in V} \chi\left(\sum\nolimits_{i=1}^{n} x_i y_i\right) X^{n-w(\boldsymbol{y})}Y^{w(\boldsymbol{y})}. \end{aligned}$$

Unter Verwendung der Homomorphieeigenschaft von χ erhalten wir dann

$$\begin{aligned} \hat{f}(\boldsymbol{x}) &= \sum_{\boldsymbol{y}\in V} \prod_{i=1}^{n} \chi(x_i y_i) X^{1-y_i^{q-1}} Y^{y_i^{q-1}} \\ &= \prod_{i=1}^{n} \sum_{y_i\in\mathbb{F}_q} \chi(x_i y_i) X^{1-y_i^{q-1}} Y^{y_i^{q-1}}, \end{aligned}$$

wobei man beachte, daß $y_i^{q-1} = 1$ im Falle $y_i \neq 0$ gilt und somit das Produkt der $X^{1-y_i^{q-1}}$ tatsächlich $X^{n-w(\boldsymbol{y})}$ ergibt. Die Summe über alle Körperelemente y_i teilen wir auf in

$$\sum_{y_i\in\mathbb{F}_q} \chi(x_i y_i) X^{1-y_i^{q-1}} Y^{y_i^{q-1}} = X + Y \cdot \sum_{y_i\in\mathbb{F}_q^\times} \chi(x_i y_i) = X - Y + Y \cdot \sum_{y_i\in\mathbb{F}_q} \chi(x_i y_i).$$

Dieser Faktor ist nach Lemma 2.20 im Fall $x_i = 0$ gleich $X - Y + Y \cdot \#\mathbb{F}_q = X + (q-1)Y$, und sonst $X - Y$. Das ergibt schließlich

$$\begin{aligned} \hat{f}(\boldsymbol{x}) &= \prod_{i=1}^{n} (X-Y)^{x_i^{q-1}} (X+(q-1)Y)^{x_i^{q-1}} \\ &= (X-Y)^{w(\boldsymbol{x})} (X+(q-1)Y)^{n-w(\boldsymbol{x})}, \end{aligned}$$

was zu zeigen war. □

Satz 2.22. *Es sei C ein linearer $[n,k]_q-$Code mit Minimaldistanz $d(C) \geq d$ und der erzeugenden Funktion*

$$W_C(X) = X^n + \sum_{l=0}^{n-d} v_l (X-1)^l.$$

Der duale Code $C^\perp$ habe Minimaldistanz $d(C^\perp) \geq d^\perp$. Dann gelten:

(a) *Für $0 \leq l \leq d^\perp - 1$ ist*

$$v_l = \binom{n}{l} (q^{k-l} - 1).$$

(b) *Für $d^\perp \leq l \leq n-d$ gilt mit $a = \min\{n-d-l+1, k-d^\perp+1\}$*

$$\max\left\{0, \binom{n}{l}(q^{k-l}-1)\right\} \;\leq\; v_l \;\leq\; \binom{n}{l}(q^a - 1).$$

Beweis. Durch Koeffizientenvergleich bei

$$W_C(X) = X^n + \sum_{s=0}^{n-d} w_{n-s} X^s = X^n + \sum_{l=0}^{n-d} v_l (X-1)^l$$

erhält man die Relationen

$$w_{n-s} = \sum_{l=s}^{n-d} \binom{l}{s} (-1)^{l-s} v_l \qquad \text{und} \qquad v_l = \sum_{j=d}^{n-l} \binom{n-j}{l} w_j$$

zwischen dem Gewichtsspektrum $w_d, \ldots, w_n$ von C und den Koeffizienten v_l. Für eine Indexteilmenge $I \subseteq \{1, \ldots, n\}$ mit Elementanzahl $\#I = l$ ist

$$C_I := \{\boldsymbol{x} \in C : x_i = 0 \text{ für alle } i \in I\}$$

ein Teilcode von C, dessen Wörter höchstens Gewicht $n-l$ besitzen. Zudem ist jedes Codewort $\boldsymbol{x} \in C$ vom Gewicht $w(\boldsymbol{x}) = j \leq n-l$ in genau $\binom{n-j}{l}$ Teilcodes $C_I \leq C$ mit $\#I = l$ enthalten. Das zeigt

$$v_l = \sum_{j=d}^{n-l} \binom{n-j}{l} w_j = \sum_{\#I=l} \#C_I \backslash \{\mathbf{0}\} = \sum_{\#I=l} (q^{\dim(C_I)} - 1).$$

Für eine Indexteilmenge I hat der zu C_I duale Code $C_I^\perp$ die Gestalt

$$C_I^\perp = C^\perp + (\mathbb{F}_q^{\,n})_I^\perp,$$

wobei $(\mathbb{F}_q^{\,n})_I^\perp$ den Vektorraum $\{\boldsymbol{y} \in \mathbb{F}_q^{\,n} : y_i = 0 \text{ für alle } i \notin I\}$ der Dimension $\#I = l$ bezeichne. Hieraus erhalten wir vermöge der Dimensionsformeln für Summen und duale Räume

$$\dim(C_I) = \dim(C) - \#I + \dim(C^\perp \cap (\mathbb{F}_q^{\,n})_I^\perp) = k - l + \dim(C^\perp \cap (\mathbb{F}_q^{\,n})_I^\perp).$$

Der Raum $C^\perp \cap (\mathbb{F}_q^{\,n})_I^\perp$ enthält ausschließlich Wörter $\boldsymbol{y}$ vom Gewicht $w(\boldsymbol{y}) \leq l$. Im Fall $0 \leq l \leq d^\perp - 1$ ist er daher leer und es folgt Aussage (a). Außerdem erhalten wir die untere Ungleichung von Aussage (b), da sowohl v_l als auch $\dim(C^\perp \cap (\mathbb{F}_q^{\,n})_I^\perp)$ nach unten durch 0 abschätzbar sind. Für die obere Ungleichung müssen wir auf die *Singleton-Schranke* vorweggreifen, deren Formulierung und Beweis sich auf der nächsten Seite befindet. Der Code C_I kann als Code der Länge $n - l$ betrachtet werden und seine Distanz d_I ist durch $d \leq d_I \leq n-l$ beschränkt. Nach der *Singleton-Schranke* ergibt sich

$$\dim(C_I) \leq (n - l) - d_I + 1 \leq n - d - l + 1.$$

Der Code $C^\perp \cap (\mathbb{F}_q^{\,n})_I^\perp$ kann als Code der Länge l betrachtet werden. Seine Distanz $d_I^\perp$ ist durch $d^\perp \leq d_I^\perp \leq l$ beschränkt und wie oben gilt

$$\dim(C^\perp \cap (\mathbb{F}_q^{\,n})_I^\perp) \leq l - d_I^\perp + 1 \leq l - d^\perp + 1.$$

Daher läßt sich $\dim(C_I)$ durch $\min\{n - d - l + 1, k - d^\perp + 1\}$ abschätzen und es folgt Aussage (b). □

Kapitel 3

Pseudorationale Codes

3.1 Gewichtsverteilung pseudorationaler Codes

Die einfachste obere Schranke für die Distanz eines Codes ist die Singleton-Schranke.

Satz 3.1. (Singleton - Schranke)
Für einen Code C über $\mathbb{F}_q$ der Länge n und Minimaldistanz d gelten:

(a) *Die Anzahl der Codewörter ist durch q^{n-d+1} beschränkt.*

(b) *Ist C ein linearer Code der Dimension k, so gilt die Abschätzung*

$$k + d \leq n + 1.$$

Beweis. Zum Beweis genügt die Feststellung, daß sich zwei Codewörter aus C notwendigerweise schon in den ersten $n-(d-1)$ Komponenten unterscheiden. Also ist die Anzahl aller Codewörter durch $q^{n-(d-1)}$ beschränkt. □

Definition 3.2. (Pseudorationaler Code, Singletondefekt)
Ein Code C heißt **pseudorational**, falls die Anzahl seiner Codewörter die Singleton-Schranke annimmt oder $C = \{\mathbf{0}\}$ gilt. Es gilt dann $c = q^{n-d+1}$ für einen $(n, c, d)_q-$ Code $C \neq \{\mathbf{0}\}$ bzw. $d = n - k + 1$, falls C linear mit den Parametern $[n, k, d]_q$ ist. Pseudorationale Codes heißen auch **MDS - Codes**, was für *maximum distance separable* steht. Bei einem linearen Code C nennen wir die Differenz zwischen $n–k+1$ und d **Singletondefekt** oder (in Hinblick auf die *AG-Schranke* in Teil II) auch **Pseudogeschlecht** von C.

Beispiel und Definiton 3.3. Die Singleton-Schranke ist für alle Codewortlängen n scharf. Die n-fachen Wiederholungscodes, die Parity-Check-Codes sowie der gesamte Raum $\mathbb{F}_q^n$ geben Beispiele für pseudorationale Codes (vgl. 2.7, 2.13, 2.17). Zusammen mit dem Nullcode $\{\mathbf{0}\}$ nennen wir diese Typen von Codes, d.h. pseudorationale Codes der Länge n und Dimension $0, 1, n-1$ oder n, auch **triviale Codes**.

Bemerkung 3.4. *Ein linearer Code C ist genau pseudorational, wenn sein dualer Code $C^\perp$ pseudorational ist. Die Klasse pseudorationaler linearer Codes ist also abgeschlossen bezüglich der Dualisierung $(\,\cdot\,)^\perp$.*

Beweis. Es sei C ein pseudorationaler $[n,k,d]_q-$Code mit dualem $[n,k^\perp,d^\perp]_q-$Code $C^\perp$. Nach Bemerkung 2.9 gilt $k^\perp = n-k$ und somit folgt aus der *Singleton-Schranke*

$$d^\perp \leq n - k^\perp + 1 = k + 1.$$

Der duale Code ist also genau dann pseudorational, falls $d^\perp \geq k+1$ gilt.

Wir nehmen also an, $C^\perp$ besitze ein nichttriviales Codewort $\boldsymbol{x} \neq 0$ vom Gewicht $w(\boldsymbol{x}) \leq k$. Dann verschwinden mindestens $n-k$ Einträge von $\boldsymbol{x}$; es seien etwa $x_{i_1} = \ldots = x_{i_{n-k}} = 0$. Wir bezeichnen mit $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n$ die Spalten der Kontrollmatrix H von C. Da H die Erzeugermatrix von $C^\perp$ ist, können wir ohne Einschränkung annehmen, daß $\boldsymbol{x}$ eine Zeile von H bildet. Dann hat der von den Spalten $\boldsymbol{s}_{i_1}, \ldots, \boldsymbol{s}_{i_{n-k}}$ aufgespannte Unterraum höchstens Dimension $n-k-1$. Nach Bemerkung 2.16 sind aber jeweils $d-1 = n-k$ Spalten von H linear unabhängig. Somit führt unsere Annahme $0 < w(\boldsymbol{x}) \leq k$ zum Widerspruch und es folgt $d^\perp \geq k+1$. □

Bei pseudorationalen Codes ist das Gewichtspolynom und damit die Verteilung der Codewörter mit gegebenem Gewicht vollständig festgelegt.

Satz 3.5. (Gewichtsverteilung pseudorationaler Codes)
Für einen pseudorationalen $[n,k,d]_q-$Code C gelten:

(a) *C hat die erzeugende Funktion*

$$W_C(X) = X^n + \sum_{l=0}^{n-d} \binom{n}{l} (q^{k-l} - 1)(X-1)^l.$$

(b) *Die Anzahl der Codewörter vom Gewicht $r \neq 0$ ist*

$$w_r(C) = \binom{n}{r}(q-1) \sum_{i=0}^{r-d} (-1)^i \binom{r-1}{i} q^{r-d-i}.$$

Beweis. Die Aussage (a) folgt aus Bemerkung 2.22, wobei man beachte, daß $C^\perp$ Minimaldistanz $d^\perp > n-d$ besitzt. Ebenfalls unter Verwendung von Bemerkung 2.22 führen wir zum Beweis von (b) einen Koeffizientenvergleich bei $W_C(X)$ durch. Dies ergibt bei X^s

$$\begin{aligned} w_{n-s}(C) &= \sum_{l=s}^{n-d} (-1)^{s-l} \binom{l}{s} v_l = \sum_{l=s}^{n-d} (-1)^{s-l} \binom{l}{s} \binom{n}{l} (q^{k-l} - 1) \\ &= \binom{n}{s} \left(\sum_{l=s}^{n-d} (-1)^{s-l} \binom{n-s}{n-l} (q^{k-l} - 1) \right). \end{aligned}$$

Für $r = n - s$ erhalten wir

$$\begin{aligned} w_r(C) &= \binom{n}{r}\left(\sum_{l=n-r}^{n-d}(-1)^{n-r-l}\binom{r}{n-l}(q^{k-l}-1)\right) \\ &= \binom{n}{r}\left(\sum_{j=0}^{r-d}(-1)^{j}\binom{r}{r-j}(q^{r+k-n-j}-1)\right). \end{aligned}$$

Die rechte Seite ist durch $q-1$ teilbar und der Faktor $w_r(C)\binom{n}{r}^{-1}(q-1)^{-1}$ hat die Gestalt

$$\sum_{j=0}^{r-d}(-1)^{j}\binom{r}{r-j}\sum_{i=0}^{r-d-j}q^i = \sum_{i=0}^{r-d}q^i\sum_{j=0}^{r-d-i}(-1)^{j}\binom{r}{j}.$$

Man beachte dabei, daß $n-k = d-1$ gilt. Mit

$$\sum_{j=0}^{r-d-i}\binom{r}{j}(-1)^j = (-1)^i\binom{r-1}{r-d-i}$$

folgt hieraus schließlich

$$\begin{aligned} w_r(C) &= \binom{n}{r}(q-1)\sum_{i=0}^{r-d}(-1)^i\binom{r-1}{r-d-i}q^i \\ &= \binom{n}{r}(q-1)\sum_{i=0}^{r-d}(-1)^i\binom{r-1}{i}q^{r-d-i} \end{aligned}$$

□

Korollar 3.6. *Pseudorationale Codes der Dimension 2 über $\mathbb{F}_q$ sowie die dazu dualen Codes haben maximal Länge $q+1$.*

Beweis. Es sei C ein (pseudorationaler) $[n,2,n-1]_q-$Code. Dann gilt nach 3.5(b)

$$0 \le w_n(C) = (q-1)(q-(n-1))$$

und somit $0 \le q+1-n$. □

MDS-Vermutung. *Nichttriviale pseudorationale Codes der Dimension k über $\mathbb{F}_q$ besitzen höchstens die Länge*

$$\begin{cases} q+2 & \textit{falls } q \equiv 0 \pmod 2 \textit{ und } k \in \{3, q-1\} \\ q+1 & \textit{sonst.} \end{cases}$$

Diese Schranken sind scharf. Im Abschnitt 3.3 lernen wir die sogenannten *projektiven Reed-Solomon-Codes* kennen. Dies sind pseudorationale Codes der Länge $q+1$.

Beispiel 3.7. Für die Konstruktion eines nichttrivialen pseudorationalen Code der Länge $q+2$ betrachten wir den Fall $q=4$. Es sei $\mathbb{F}_4 = \{0,1,a,b\}$. Die Matrix

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & a & b \\ 0 & 0 & 1 & 1 & b & a \end{array}\right)$$

ist dann Erzeugermatrix eines $[6,3,4]_4-$ bzw. Kontrollmatrix eines $[6,4,3]_4-$Codes, da jeweils drei Spalten der Matrix linear unabhängig sind (vgl. Bemerkung 2.16). Dieser Code wird auch **Hexacode** genannt.

Die *MDS-Vermutung* konnte bisher für $q \leq 29$ oder $k \leq 5$ bestätigt werden. Wir beschäftigen uns näher mit der Vermutung in den Kapiteln 12 und 13, in denen wir die Vermutung für die arithmetischen Codeklassen der sogenannten *rationalen*, *elliptischen* und *hyperelliptischen* Codes beweisen.

3.2 Reed-Solomon-Codes

Die Klasse der Reed-Solomon-Codes ist die wichtigste und meistverwandte Klasse von (pseudorationalen) Codes. Zum Beispiel werden diese Codes in variierter Form als sogenannte *CIRC - Codes* bei Audio und Compact Discs verwendet. Darauf gehen wir im nächsten Kapitel ein. Zudem werden wir in Abschnitt 12.1 eine arithmetische Beschreibung der Reed-Solomon-Codes geben.

Definition 3.8. (Reed-Solomon-Code)
Es seien $q \geq n \geq k \geq 0$. Wir bezeichnen mit $\mathcal{P}_k := \mathbb{F}_q[X]_{<k}$ den Vektorraum der $\mathbb{F}_q$-Polynome vom Grad $< k$. Für paarweise verschiedene Körperelemente $a_1, \ldots, a_n \in \mathbb{F}_q$ und beliebige $b_1, \ldots, b_n \in \mathbb{F}_q^\times$ seien $\boldsymbol{a} := (a_1, \ldots, a_n)$ und $\boldsymbol{b} := (b_1, \ldots, b_n)$. Dann ist der **(verallgemeinerte) Reed-Solomon-Codes** $RS_k(\boldsymbol{a}, \boldsymbol{b})$ definiert durch den Codierer

$$C : \left\{ \begin{array}{ccc} \mathcal{P}_k & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & (b_1 f(a_1), \ldots, b_n f(a_n)). \end{array} \right.$$

Man nennt $\boldsymbol{a}$ daher auch **Auswertungsvektor**. $RS_k(\boldsymbol{a}, \boldsymbol{b})$ heißt **gewöhnlich**, falls $\boldsymbol{b} = (1, \ldots, 1)$ und $\boldsymbol{a} = (u^i)_{1 \leq i \leq n}$ mit einer primitiven n-ten Einheitswurzel $u \in \mathbb{F}_q$ gelten.

Anmerkung 3.9. Gewöhnliche Reed-Solomon-Codes liefern auch Beispiele für die sogenannte *BCH - Codes*, die wir in Abschnitt 6.3 studieren.

Bemerkung 3.10. (Parameter und Erzeugermatrix von $RS_k(\boldsymbol{a}, \boldsymbol{b})$)
Für einen Reed-Solomon-Code $RS_k(\boldsymbol{a}, \boldsymbol{b})$ der Länge n über $\mathbb{F}_q$ gelten:

(a) *$RS_k(\boldsymbol{a}, \boldsymbol{b})$ ist pseudorational mit Dimension k, d.h. $RS_k(\boldsymbol{a}, \boldsymbol{b})$ bildet einen $[n, k, n-k+1]_q-$Code.*

(b) *Die Matrix $(b_i a_i^j)_{0 \leq j \leq k-1, 1 \leq i \leq n}$ ist eine Erzeugermatrix von $RS_k(\boldsymbol{a}, \boldsymbol{b})$.*

Beweis. (a) Der Raum $\mathcal{P}_k$ wird durch den Codierer C in $\mathbb{F}_q^n$ linear eingebettet, da das Bild eines Polynoms f unter C nur dann verschwindet, falls f für die Argumente $a_1, \ldots, a_n$ verschwindet. In diesen Fall hat f nämlich mindestens n Nullstellen und nach Voraussetzung höchstens Grad $k-1$. Wegen $n \geq k$ ist also $C(f) = 0$ nur im Fall $f = 0$ möglich, d.h. C ist injektiv. Über $\mathbb{F}_q$ besitzt $\mathcal{P}_k$ Dimension k, woraus $\dim(RS_k(\boldsymbol{a}, \boldsymbol{b})) = k$ folgt. Da $f \neq 0$ aus $\mathcal{P}_k$ höchstens $k-1$ Nullstellen hat, sind mindestens $n-(k-1)$ Einträge des Codewortes $C(f)$ ungleich 0. Es gilt also $d \geq n-k+1$. Aus der *Singleton-Schranke* erhält man die Gleichheit, was die Pseudorationalität von $RS_k(\boldsymbol{a}, \boldsymbol{b})$ beweist.
(b) Die Polynome $1, X, \ldots, X^{k-1}$ bilden eine Basis von $\mathcal{P}_k$ und somit sind auch ihre Bilder $C(x^j) = (b_1 a_1^j, \ldots, b_n a_n^j)$ unter C eine Basis von $RS_k(\boldsymbol{a}, \boldsymbol{b})$. □

Aus Bemerkung 3.4 wissen wir bereits, daß die Klasse der pseudorationalen Codes abgeschlossen bezüglich Dualisierung ist. Die Unterklasse der Reed-Solomon-Codes ist ebenfalls $(\,\cdot\,)^\perp$ - invariant und ihre Parameter sind sogar "uniform".

Satz 3.11. (Dualer Reed-Solomon-Code)
Es seien die Vektoren $\boldsymbol{a} = (a_1, \ldots, a_n)$ mit paarweise verschiedenen Einträgen a_i aus $\mathbb{F}_q$ und $\boldsymbol{b} \in (\mathbb{F}_q^\times)^n$ gegeben. Dann gibt es ein $\boldsymbol{c} \in (\mathbb{F}_q^\times)^n$, sodaß

$$RS_k(\boldsymbol{a}, \boldsymbol{b})^\perp = RS_{n-k}(\boldsymbol{a}, \boldsymbol{c})$$

für $0 \leq k \leq n-1$ gilt.

Beweis. Wir betrachten zunächst den Reed-Solomon-Code $C = RS_{n-1}(\boldsymbol{a}, \boldsymbol{b})$ der Dimension $n-1$. Dann ist sein dualer Code $C^\perp$ nach Bemerkung 3.4 ebenfalls pseudorational und besitzt die Parameter $[n, 1, n]_q$. Folglich wird $C^\perp$ erzeugt von einen einzigen Wort $\boldsymbol{c} = (c_1, \ldots, c_n)$ vom Gewicht n, das dann auch die Kontrollmatrix von $RS_{n-1}(\boldsymbol{a}, \boldsymbol{b})$ bildet. Mit der Kontrollgleichung für $RS_{n-1}(\boldsymbol{a}, \boldsymbol{b})$ erhalten wir also

$$\sum_{i=1}^{n} c_i b_i h(a_i) = 0 \qquad \text{für } h \in \mathcal{P}_{n-1}.$$

Für $k \in \mathbb{N}$ mit $0 \leq k \leq n-1$ wählen wir beliebige Polynome $f \in \mathcal{P}_k$ und $g \in \mathcal{P}_{n-k}$. Dann ist $h := f \cdot g$ Element von $\mathcal{P}_{n-1}$ und es gilt nach obigem die Orthogonalitätsrelation

$$\langle\ (b_1 f(a_1), \ldots, b_n f(a_n)), (c_1 g(a_1), \ldots, c_n g(a_n))\ \rangle = \sum_{i=1}^{n} c_i b_i h(a_i) = 0$$

zwischen den Worten $(b_1 f(a_1), \ldots, b_n f(a_n))$ aus $RS_k(\boldsymbol{a}, \boldsymbol{b})$ und $(c_1 g(a_1), \ldots, c_n g(a_n))$ aus $RS_{n-k}(\boldsymbol{a}, \boldsymbol{c})$. Da f und g beliebig wählbar sind, folgt $RS_k(\boldsymbol{a}, \boldsymbol{b})^\perp \leq RS_{n-k}(\boldsymbol{a}, \boldsymbol{c})$ und aus Dimensionsgründen schließlich die behauptete Gleichheit. □

3.3 Projektive Reed-Solomon-Codes

Reed-Solomon-Codes können unter Beibehaltung des Singleton-Defekts 0 um ein Symbol verlängert werden. Dies liefert unteren anderem pseudorationale Codes über $\mathbb{F}_q$ der Länge $q+1$.

Definition 3.12. (Projektiver Reed-Solomon-Code)
Es seien $RS_k(\boldsymbol{a}, \boldsymbol{b})$ ein Reed-Solomon-Code über $\mathbb{F}_q$ der Länge $n \leq q$ und $b_{n+1} \in \mathbb{F}_q^\times$. Dann heißt der durch die Matrix

$$\hat{G} := \left(\begin{array}{ccc|c} b_1 & \cdots & b_n & 0 \\ b_1a_1 & \cdots & b_na_n & 0 \\ \vdots & & \vdots & \vdots \\ b_1a_1^{k-1} & \cdots & b_na_n^{k-1} & 0 \\ \hline b_1a_1^k & \cdots & b_na_n^k & b_{n+1} \end{array}\right)$$

definierte $[n+1, k+1]_q-$Code **projektiver Reed-Solomon-Code** über $\mathbb{F}_q$.

Satz 3.13. *Projektive Reed-Solomon-Codes sind pseudorational.*

Beweis. In der Situation von Definition 3.12 seien $C = RS_k(\boldsymbol{a}, \boldsymbol{b})$ und $\hat{C}$ der durch C und b_{n+1} definierte projektive Reed-Solomon-Code der Länge $n+1$ und Dimension $k+1$. Für den Nachweis, daß $\hat{C}$ pseudorational ist, müssen wir gemäß der *Singleton-Schranke* nur $d(\hat{C}) \geq n-k+1$ zeigen. Sei dazu $\boldsymbol{c} = (c_1, \ldots, c_n)$ der Dualitätsvektor von C (aus Satz 3.11) mit $C^\perp = RS_{n-k}(\boldsymbol{a}, \boldsymbol{c})$. Es sei $c_{n+1} \in \mathbb{F}_q$ mit

$$\sum_{i=1}^{n} c_i b_i a_i^{n-1} + c_{n+1}b_{n+1} = 0.$$

Wir nehmen zunächst an, daß $c_{n+1} = 0$ ist. Es gilt dann $\sum_{i=1}^{n} c_i b_i a_i^{n-1} = 0$ und somit $\sum_{i=0}^{n-1} c_i b_i h(a_i) = 0$ für alle $h \in \mathcal{P}_n$ nach Konstruktion von $\boldsymbol{c}$. So aber ist $\boldsymbol{c}$ als nichtverschwindender Vektor orthogonal zu allen Vektoren aus $\mathbb{F}_q^n$. Aufgrund diesen Widerspruchs ist $c_{n+1} \in \mathbb{F}_q^\times$. Wir bilden die Matrix

$$\hat{H} := \left(\begin{array}{ccc|c} c_1 & \cdots & c_n & 0 \\ c_1a_1 & \cdots & c_na_n & 0 \\ \vdots & & \vdots & \vdots \\ c_1a_1^{n-k-2} & \cdots & c_na_n^{n-k-2} & 0 \\ \hline c_1a_1^{n-k-1} & \cdots & c_na_n^{n-k-1} & c_{n+1} \end{array}\right) = \left(\begin{array}{ccc|c} & & & \\ & H & & \boldsymbol{u} \\ & & & \\ \hline c_1a_1^{n-k-1} & \cdots & c_na_n^{n-k-1} & \end{array}\right),$$

die ebenfalls einen projektiven Reed-Solomon-Code erzeugt. Wegen $\hat{H}\hat{G}^T = 0$ ist dieser dual zu $\hat{C}$ und $\hat{H}$ wirkt als Kontrollmatrix auf $\hat{C}$. Wir zeigen nun, daß jeweils $n-k$ Spalten von $\hat{H}$ linear unabhängig sind und untersuchen dazu die quadratischen $n-k$ - Teilmatrizen M von $\hat{H}$.

1.Fall: Es ist $\boldsymbol{u}$ nicht in M enthalten. Dann hat M die Gestalt

$$M = V(a_{i_1}, \ldots, a_{i_{n-k}}) \cdot \mathrm{diag}(c_{i_1}, \ldots, c_{i_{n-k}}),$$

wobei $V(a_{i_1}, \ldots, a_{i_{n-k}})$ die Vandermonde-Matrix bedeutet. Da die a_{i_j} paarweise verschieden und die c_{i_j} invertierbar sind, ergibt sich $\det(M) \neq 0$.
2.Fall: Im zweiten Fall hat M die Spalten $\boldsymbol{s}_{i_1}, \ldots, \boldsymbol{s}_{i_{n-k-1}}, \boldsymbol{u}$. Dabei sind $\boldsymbol{s}_{i_1}, \ldots, \boldsymbol{s}_{i_{n-k-1}}$ linear unabhängig, da H Kontrollmatrix von C ist und somit nach Bemerkung 2.16 jeweils $d(C)-1 = n-k$ Spalten von H linear unabhängig sind. Das hat aber auch die lineare Unabhängigkeit von $\boldsymbol{u}$ zu $\boldsymbol{s}_{i_1}, \ldots, \boldsymbol{s}_{i_{n-k-1}}$ und damit die Regularität von M zur Folge. In beiden Fällen sind also jeweils $n-k$ Spalten von $\hat{H}$ linear unabhängig. Folglich gilt $d(\hat{C}) \geq n-k+1$. □

Der Beweis zeigt zusätzlich, daß die Kontrollmatrix eines projektiven Reed-Solomom-Code wieder einen projektiven Reed-Solomon-Code erzeugt. Dies impliziert

Korollar 3.14. *Die Klasse der projektiven Reed-Solomon-Codes ist abgeschlossen bezüglich der Dualisierung und enthält ausschließlich pseudorationale Codes.* □

3.4 Decodierung von Reed-Solomon-Codes

Im gesamten Abschnitt sei

$$C = RS_k(\boldsymbol{a}, \boldsymbol{b}) = RS_{n-k}(\boldsymbol{a}, \boldsymbol{c})^{\perp}$$

ein Reed-Solomon-Code über $\mathbb{F}_q$ mit Auswertungsvektor $\boldsymbol{a} = (a_1, \ldots, a_n)$. Desweiteren sei $e = \lfloor \frac{n-k+1}{2} \rfloor$ der Fehlerkorrekturparameter von C, d.h. die maximal mögliche Anzahl von korrigierbaren Fehlern bei der Decodierung von C. Gesucht wird für eine empfangene Nachricht $\boldsymbol{y}$ ein Codewort $\boldsymbol{x}$ mit Abstand $d(\boldsymbol{x}, \boldsymbol{y}) \leq e$.

Definition 3.15. (Fehlervektor, Fehlerpolynom)
Gibt es zu $\boldsymbol{y} \in \mathbb{F}_q^n$ ein Codewort $\boldsymbol{x} \in C$ mit $d(\boldsymbol{x}, \boldsymbol{y}) \leq e$, so nennen wir $\boldsymbol{x} - \boldsymbol{y} = (e_1, \ldots, e_n)$ **Fehlervektor**. Die Indexmenge $I_{\boldsymbol{y}} = \{i : e_i \neq 0\}$ heißt **Menge der Fehlerpositionen**. Das **Fehlerpolynom** ist definiert durch

$$\sigma(X) = \prod_{i \in I_{\boldsymbol{y}}} (X - a_i) = \sum_{s=0}^{e} z_s X^s.$$

Wir nennen σ auch **fehlerlokalisierende Funktion**.

Die **Syndrome** zu $\boldsymbol{y}$ sind die Elemente

$$s_j(\boldsymbol{y}) = \sum_{i=1}^{n} y_i c_i a_i^j \qquad (0 \leq j \leq n-k).$$

Offenbar gilt $s_j(\boldsymbol{y}_1 + \boldsymbol{y}_2) = s_j(\boldsymbol{y}_1) + s_j(\boldsymbol{y}_2)$ sowie $s_j(\boldsymbol{x}) = 0$ für Codewörter $\boldsymbol{x} \in C$. Folglich stimmen die Syndrome $s_j(\boldsymbol{y})$ mit $s_j(\boldsymbol{e})$ überein. Daraus folgt

Lemma 3.16. *Die Koeffizienten $z_0, \ldots, z_e$ des Fehlerpolynoms $\sigma(X)$ erfüllen das Gleichungssystem*

$$\sum_{l=0}^{e} z_l s_{j+l}(\boldsymbol{y}) = 0 \qquad (0 \le j \le e-1) \tag{3.17}$$

und es ist $(z_0, \ldots, z_e)$ durch (3.17) bis auf skalare Multiplikation eindeutig bestimmt.

Beweis. Wegen $e_i = 0$ für $i \notin I_{\boldsymbol{y}}$ und $\sigma(a_i) = 0$ für $i \in I_{\boldsymbol{y}}$ gilt

$$\begin{aligned}\sum_{l=0}^{e} z_l s_{j+l}(\boldsymbol{y}) &= \sum_{l=0}^{e} z_l \sum_{i=1}^{n} e_i c_i a_i^{j+l} = \sum_{i=1}^{n} e_i c_i a_i^j \sum_{l=0}^{e} z_l a_i^l \\ &= \sum_{i \in I_{\boldsymbol{y}}} e_i c_i a_i^j \sigma(a_i) \quad = \; 0.\end{aligned}$$

Ist $(\hat{z}_0, \ldots, \hat{z}_e)$ eine weitere Lösung von (3.17), so definieren wir

$$\hat{\sigma}(X) := \sum_{l=0}^{e} \hat{z}_l X^l \qquad \text{und} \qquad \sigma_j(X) := \prod_{\substack{i \in I \\ i \ne j}} (X - a_i) = \sum_{l=0}^{e-1} z_{l,j} X^l.$$

Dann gilt für eine beliebige Fehlerposition $j \in I_{\boldsymbol{y}}$

$$e_j c_j \sigma_j(a_j) \hat{\sigma}(a_j) = \sum_{i \in I_{\boldsymbol{y}}} e_i c_i \sigma_j(a_i) \hat{\sigma}(a_i),$$

da $\sigma_j(a_i)$ im Falle $i \ne j$ verschwindet. Diese Summe kann weiter umgeformt werden zu

$$\sum_{i \in I} \sum_{k=0}^{e-1} \sum_{l=0}^{e} e_i c_i z_{k,j} a_i^k \hat{z}_l a_i^l = \sum_{k=0}^{e-1} z_{k,j} \left(\sum_{l=0}^{e} \hat{z}_l s_{k+l}(\boldsymbol{y}) \right).$$

Als Lösung von (3.17) erfüllen $\hat{z}_0, \ldots, \hat{z}_e$ die Gleichungen $\sum_{l=0}^{e} \hat{z}_l s_{k+l}(\boldsymbol{y}) = 0$ für alle Indices $0 \le k \le e-1$. Das Produkt $e_j c_j \sigma_j(a_j) \hat{\sigma}(a_j)$ verschwindet also, und wegen $e_j c_j \sigma_j(a_j) \ne 0$ ist $\hat{\sigma}(a_j) = 0$ für alle Fehlerpositionen $j \in I_{\boldsymbol{y}}$. Folglich ist das Fehlerpolynom $\sigma(X)$ ein Teiler von $\hat{\sigma}(X)$. Da die Polynomgrade übereinstimmen folgt nun die Existenz eines Skalars $a \in \mathbb{F}_q$ mit $\sigma(X) = a \cdot \hat{\sigma}(X)$. □

Decodieralgorithmus 3.18. Es sei $\boldsymbol{y} \in \mathbb{F}_q^n$ gegeben.

(1) Bestimme für $0 \le j \le n-k$ die Syndrome $s_j(\boldsymbol{y}) = \sum_{i=1}^{n} y_i c_i a_i^j$ zu $\boldsymbol{y}$.

(2) Finde eine Lösung $\boldsymbol{z} = (z_0, \ldots, z_l)$ des Gleichungssystems (3.17).

(3) Faktorisiere das Polynom $\hat{\sigma}(X) := \sum_{l=0}^{e} z_l X^l$. Die Indexmenge der Fehlerpositionen ist dann $I = \{i : \hat{\sigma}(a_i) = 0\}$.

(4) Für $i \notin I$ setze $e_i := 0$. Bestimme die restliche Koeffizienten des Fehlervektors $\boldsymbol{e} = (e_1, \ldots, e_n)$ mit Hilfe des Gleichungssystem

$$\sum_{i \in I} e_i c_i a_i^j = s_j(\mathbf{y}) \qquad (0 \leq j \leq n-k). \tag{3.19}$$

(5) Das Codewort $\boldsymbol{x} = \boldsymbol{y} - \boldsymbol{e} \in C$ ist dann die decodierte Nachricht.

Bemerkung 3.20. *Der Decodieralgorithmus 3.18 mit dem Startvektor $\boldsymbol{y} \in \mathbb{F}_q^n$ terminiert, falls es ein Codewort $\boldsymbol{x} \in C$ mit Distanz $d(\boldsymbol{x}, \boldsymbol{y}) \leq e$ gibt.*

Beweis. Aus Lemma 3.16 folgt, daß $\hat{\sigma}$ aus Schritt 3 ein skalares Vielfaches der fehlerlokalisierenden Funktion σ von $\boldsymbol{y}$ ist. Somit ist I die tatsächliche Indexmenge $I_{\boldsymbol{y}}$ der Fehlerpositionen. Es ist nur noch zu zeigen, daß eine Lösung des Gleichungssystem (3.19) eindeutig bestimmt ist. Dazu sei $\boldsymbol{e}'$ mit $e_i' = 0$ für $i \notin I$ eine Lösung von (3.19). Dann verschwinden die Syndrome

$$s_j(\boldsymbol{e} - \boldsymbol{e}') = \sum_{i=1}^{n} (e_i - e_i') c_i a_i^j$$

für $0 \leq j \leq n-k$ und somit ist $\boldsymbol{e} - \boldsymbol{e}'$ ein Codewort aus C vom Gewicht

$$w(\boldsymbol{e} - \boldsymbol{e}') \leq 2e < d(C).$$

Das ist nur für $\boldsymbol{e} = \boldsymbol{e}'$ möglich. □

Kapitel 4

Variationen von Codes

4.1 Einige elementare lineare Konstruktionen

Bemerkung 4.1. (Erweiterung mit Paritätsbit)
Es sei C ein $[n,k,d]_q-$Code mit Erzeugermatrix G. Dann erzeugt

$$\hat{G} = (G|\boldsymbol{p}) = \left(\begin{array}{ccc|c} x_{11} & \cdots & x_{1n} & -\sum_{i=1}^{n} x_{1i} \\ \vdots & \ddots & \vdots & \vdots \\ x_{k1} & \cdots & x_{kn} & -\sum_{i=1}^{n} x_{ki} \end{array}\right)$$

einen $[n+1,k,\hat{d}]_q-$Code mit Minimaldistanz d oder $d+1$.

Bemerkung 4.2. (Punktierung)
Es sei C ein $[n,k,d]_q-$Code. Der durch Weglasssen des i-ten Symbols erzeugte Code

$$C^{\vee i} = \{(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n) : \boldsymbol{x} \in C\}$$

ist ein $[n-1,k^{\vee},d^{\vee}]_q-$Code mit Dimension $k^{\vee} \in \{k-1,k\}$ und Distanz $d^{\vee} \in \{d-1,d\}$.

Bemerkung 4.3. (Direkte Summe)
Es seien C_1 und C_2 lineare Codes mit den Paramtern $[n_i,k_i,d_i]_q$ für $i=1,2$. Dann gelten:

(a) *Der Code*

$$C_1 \oplus C_2 = \{(\boldsymbol{x}_1,\boldsymbol{x}_2) : \boldsymbol{x}_i \in C_i\}$$

ist ein $[n_1+n_2,k_1+k_2,d]_q-$Code mit Minimaldistanz $d = \min\{d_1,d_2\}$.

(b) *Im Fall $n_1 = n_2$ definiert*

$$C := \{(\boldsymbol{x}_1,\boldsymbol{x}_1+\boldsymbol{x}_2) : x_i \in C_i\}$$

einen $[2n_1,k_1+k_2,d]_q-$Code mit Distanz $d = \min\{2d_1,d_2\}$.

Bemerkung 4.4. (Verklebung)
Es seien $C_1 : \mathbb{F}_q^k \hookrightarrow \mathbb{F}_q^{n_1}$ *und* $C_2 : \mathbb{F}_q^k \hookrightarrow \mathbb{F}_q^{n_2}$ *Codierer von* $[n_1, k, d_1]_q-$ *bzw.* $[n_2, k, d_2]_q-$*Codes. Dann gelten:*

(a) *Der Codierer*

$$(C_1|C_2) : \begin{cases} \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^{n_1} \oplus \mathbb{F}_q^{n_2} \\ \boldsymbol{x} & \longmapsto & (C_1(\boldsymbol{x}), C_2(\boldsymbol{x})) \end{cases}$$

erzeugt einen $[n_1 + n_2, k, d]_q-$*Code mit Minimaldistanz* $d \geq d_1 + d_2$.

(b) $(C_1|\cdots|C_1) : \mathbb{F}_q^k \hookrightarrow \mathbb{F}_q^{ln}$ *ist ein* $[ln, k, ld]_q-$*Wiederholungscode.*

Bemerkung 4.5. (Tensorprodukt, Cross Interleaving)
Es seien C_1 *und* C_2 *lineare Codes mit den Parametern* $[n_i, k_i, d_i]_q$ *für* $i = 1, 2$. *Dann definiert*

$$C_1 \otimes C_2 = \left\{ \boldsymbol{x}^{(1)} \otimes \boldsymbol{x}^{(2)} : \boldsymbol{x}^{(i)} \in C_i \right\} \leq \mathbb{F}_q^{n_1 \cdot n_2} \cong \mathbb{F}_q^{n_1} \otimes \mathbb{F}_q^{n_2}$$

mit

$$\boldsymbol{x}^{(1)} \otimes \boldsymbol{x}^{(2)} = (x_1^{(1)}x_1^{(2)}, \ldots, x_{n_1}^{(1)}x_1^{(2)}, x_1^{(1)}x_2^{(2)}, \ldots, x_{n_1}^{(1)}x_2^{(2)}, \ldots\ldots, x_1^{(1)}x_{n_2}^{(2)}, \ldots, x_{n_1}^{(1)}x_{n_2}^{(2)})$$

einen $[n_1 \cdot n_2, k_1 \cdot k_2, d_1 \cdot d_2]_q-$*Code. Dabei heißen* C_1 **innerer** *und* C_2 **äußerer Code** *von* $C_1 \otimes C_2$.

Beweis. Offensichtlich hat $C_1 \otimes C_2$ die Länge $n_1 \cdot n_2$. Ein Codewort besitzt das Gewicht $w(\boldsymbol{x}^{(1)} \otimes \boldsymbol{x}^{(2)}) = w(\boldsymbol{x}^{(1)}) \cdot w(\boldsymbol{x}^{(2)})$. Daher sind die Produkte von Minimalwörtern je aus C_1 und C_2 Minimalwörter in $C_1 \otimes C_2$ und es folgt die Aussage über die Distanz von $C_1 \otimes C_2$. Für den Rest des Beweises zeigen wir, daß $C_1 \otimes C_2$ tatsächlich ein Tensorprodukt ist und als solches Dimension $k_1 \cdot k_2$ besitzt. Das (existierende) Tensorprodukt von C_1 und C_2 bezeichnen wir dabei mit V. Die Abbildung $(\boldsymbol{x}^{(1)}, \boldsymbol{x}^{(2)}) \mapsto \boldsymbol{x}^{(1)} \otimes \boldsymbol{x}^{(2)}$ von $C_1 \times C_2$ nach $C_1 \otimes C_2$ ist offensichtlich bilinear und surjektiv. Nach der universellen Abbildungseigenschaft von Tensorprodukten gibt es daher einen surjektiven Homomorphismus von V nach $C_1 \otimes C_2$ und es gilt $\dim(C_1 \otimes C_2) \leq \dim(V) = k_1 \cdot k_2$. Dieser Homomorphismus ist auch injektiv, da die Produkte $\boldsymbol{x}_{\boldsymbol{i}}^{(1)} \otimes \boldsymbol{x}_{\boldsymbol{j}}^{(2)}$ von Basen in C_1 und C_2 linear unabhängig sind. Eine Linearkombination $\sum a_{ij} \boldsymbol{x}_{\boldsymbol{i}}^{(1)} \otimes \boldsymbol{x}_{\boldsymbol{j}}^{(2)} = 0$ läßt sich auf $k_2 \cdot n_2$ Linearkombinationen $\sum_{i=1}^{k_1} a_{ij} x_{jl}^{(2)} \boldsymbol{x}_{\boldsymbol{i}}^{(1)} = 0$ mit $1 \leq j \leq k_2, 1 \leq l \leq n_2$ zurückführen. Diese liefern die Gleichungen $a_{ij} \boldsymbol{x}_{\boldsymbol{j}}^{(2)} = 0$ für $1 \leq i \leq k_1, 1 \leq j \leq k_2$ und somit schließlich $a_{ij} = 0$ für alle Doppelindizes ij. Das beweist unsere Aussage über die Dimension und zeigt, daß $C_1 \otimes C_2$ ein Tensorprodukt von C_1 und C_2 ist. □

Aufgabe 4.6. Führen Sie die Beweise der Bemerkungen 4.1 - 4.4 durch.

4.2 Spreizung und Verkettung

In der Praxis sind viele Kanäle anfällig für sogenannte "*burst errors*". Diese Fehler treten während der gesamten Nachrichtenübermittlung im Gegensatz zu den "*random errors*" nicht gleichverteilt sondern in Form von Fehlerpaketen auf. Zum Beispiel führen Kratzer auf Audio CDs oder Blitzeinschläge bei Funkübertragungen zum Verlust mehrerer aufeinanderfolgenden Bits. Um solche Fehlerpakete korrigieren zu können, verteilt man die Symbole von t Codewörter auf der Länge $n \cdot t$ und zieht somit die Informationen weit auseinander.

Definition 4.7. (Spreizung, Interleaving)
Für einen linearen $[n,k]_q-$Code heißt

$$C^t := \{(x_1^{(1)}, x_1^{(2)}, \ldots, x_1^{(t)}, x_2^{(1)}, \ldots, x_2^{(t)}, \ldots\ldots, x_n^{(1)}, \ldots, x_n^{(t)}) : \boldsymbol{x}^{(i)} \in C\}$$

der **zur Tiefe t gespreizte Code**.

Anmerkung 4.8. Der gespreizte Code C^t ist ein linearer $[nt,kt]_q-$Code mit Minimaldistanz $d(C^t) = d(C)$.

Bemerkung 4.9. *Ist C ein linearer Code, der jedes Fehlerpaket bis zur Länge b korrigieren kann, so ist C^t ein linearer Code, der jedes Fehlerpaket bis zur Länge $b \cdot t$ korrigieren kann.* □

Beispiel 4.10. (**C**ross **I**nterleaved **R**eed-Solomon **C**ode)
Für Audio CDs verwendet man einen Untercode von $C_1 \otimes C_2$ der Länge $28 \cdot 32$ über $\mathbb{F}_{2^8}$ mit einem $[28,24,5]_{2^8}-$Reed-Solomon-Code C_1 als inneren und einem $[32,28,5]_{2^8}-$Reed-Solomon-Code C_2 als äußeren Code. Die Amplitude der Schallwelle wird pro Kanal (also links und rechts) $44100-$mal in der Sekunde gemessen und einem Wert zwischen 0 und $2^{16}-1$ zugeordnet. Dieser Wert wird mit einem Punkt aus $\mathbb{F}_{2^8}^2 \cong \mathbb{F}_2^{16}$ identifiziert. Eine Abtastung der Schallwelle ergibt also ein Paar $(L,R) \in \mathbb{F}_{2^8}^4$. Es werden 6 aufeinanderfolgende Abtastungen (zu einen Vektor der Länge 24) zusammengefaßt und mit C_1 zu einem Spaltenvektor in $\mathbb{F}_{2^8}^{28}$ codiert. Mit $168 = 6 \cdot 28$ Abtastungen erhält man 28 Codewörter $\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(28)} \in C_1$, die dann als Spalten einer $28 \times 28-$Matrix aufgefaßt werden. Mit einer reduzierten Erzeugermatrix $(I_{28}|P_4)$ von C_2 codiert man $\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(28)}$. Mit 168 Abtastungen erhält man also die Matrix

$$M = (\boldsymbol{x}^{(1)} \ \cdots \ \boldsymbol{x}^{(28)}) \cdot (I_{28}|P_4) = (\boldsymbol{x}^{(1)} \ \cdots \ \boldsymbol{x}^{(28)}|\tilde{P}) \in \mathbb{F}_{2^8}^{28\times 32},$$

deren Spalten Wörter aus C_1 und deren Zeilen Wörter aus C_2 sind. Diese Matrix wird nun (zur Tiefe 28) gespreizt, d.h alle Zeilenvektoren werden hintereinandergelegt zu einen Zeilenvektor der Länge $28 \cdot 32$. Dies ist dann die Bitfolge, die auf der CD gespeichert wird. Zur Decodierung eines ausgelesenen Wortes macht man zunächst die Spreizung rückgängig und erhält somit eine Matrix $\tilde{M} \in \mathbb{F}_{2^8}^{28\times 32}$. War die

Auslesung korrekt, so sind die Zeilen wiederum Codewörter aus C_2 und die Spalten Wörter aus C_1. Die Audioinformationen, d.h. die Amplituden der Schallwellen im linken und rechten Kanal, werden dann durch Decodierung der Spalten von $\tilde{M}$ zurüchgewonnen. Ein ausführliches Beispiel zur Behebung eines burst errors mit dem *CIRC* - Code kann in [Lü03] Abschnitte 4.2 und 4.3 nachgelesen werden.

Definition 4.11. (Verkettung)
Es seien C_1 ein $[n_1, k_1, d_1]_q-$ und C_2 ein $[n_2, k_2, d_2]_r-$Code, wobei $q = r^{k_2}$ gelte. Desweiteren seien $\psi_1 : \mathbb{F}_r^{k_1 k_2} \to \mathbb{F}_q^{k_1}$ und $\psi_2 : \mathbb{F}_q^{n_1} \to \mathbb{F}_r^{n_1 k_2}$ Vektorraumisomorphismen über $\mathbb{F}_r$. Dann heißt der Code

$$C_1 * C_2 : \mathbb{F}_r^{k_1 k_2} \xrightarrow{\psi_1} \mathbb{F}_q^{k_1} \xrightarrow{C_1} \mathbb{F}_q^{n_1} \xrightarrow{\psi_2} \mathbb{F}_r^{n_1 k_2} \xrightarrow{C_2 \times \cdots \times C_2} \mathbb{F}_r^{n_1 n_2}$$

verketteter Code mit C_1 als **äußerem** und C_2 als **innerem** Code.

Bemerkung 4.12. (Parameter verketteter Codes)
In der Situation von Definition 4.11 ist $C_1 * C_2$ ein linearer $[n_1 \cdot n_2, k_1 \cdot k_2]_r-$Code mit Minimaldistanz $d(C_1 * C_2) \geq d_1 \cdot d_2$.

Beweis. Die Aussagen über Länge und Dimension von $C_1 * C_2$ folgen aus der Konstruktion, wobei man beachte, daß ψ_1, C_1, ψ_2 sowie $C_2 \times \cdots \times C_2$ und daher auch $C_1 * C_2$ injektive Homomorphismen sind. Ist nun $\boldsymbol{x} = (x_1, \ldots, x_{n_1}) \in C_1$ ein Wort des äußeren Codes, so wird jedem Symbol x_i durch die Abbildung $C_2 \circ \psi_2$ genau ein Codewort $\boldsymbol{y}_i$ des inneren Codes C_2 zugeordnet:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_{n_1} \end{pmatrix} \overset{\psi_2}{\longmapsto} \begin{pmatrix} \boldsymbol{x}_1 \\ \vdots \\ \boldsymbol{x}_{n_1} \end{pmatrix} = \begin{pmatrix} x_{11} & \cdots & x_{1k_2} \\ \vdots & \ddots & \vdots \\ x_{n_1 1} & \cdots & x_{n_1 k_2} \end{pmatrix} \overset{C_2}{\longmapsto} \begin{pmatrix} y_{11} & \cdots & y_{1n_2} \\ \vdots & \ddots & \vdots \\ y_{n_1 1} & \cdots & y_{n_1 n_2} \end{pmatrix} = \begin{pmatrix} \boldsymbol{y}_1 \\ \vdots \\ \boldsymbol{y}_{n_1} \end{pmatrix}$$

Es gibt also für jeden Eintrag $x_i \neq 0$ mindestens d_2 nichtverschwindende Einträge von $\boldsymbol{y}_i$. Das zeigt $d(C_1 * C_2) \geq d_1 \cdot d_2$. □

Korollar 4.13. (Körperabstieg)
Ist der innere Code C_2 bei $q = r^m$ ein linearer $[m, m, 1]_q-$Code, d.h. es gilt $C_2 \in \mathrm{Aut}(\mathbb{F}_r^m)$, so bildet der verkettete Code $C_1 * C_2$ einen $[n_1 m, k_1 m]_r-$Code mit Distanz $d(C_1 * C_2) \geq d(C_1)$. □

4.3 Teilkörpercodes

Beispiele für Teilkörpercodes traten schon bei der Konstruktion von verketteten Codes auf. In diesem Abschnitt wollen wir nun die Struktur von Teilkörpercodes systematisch untersuchen.

Definition 4.14. (Einschränkung auf Teilkörper, Spurcode)
Es seien q, r Primzahlpotenzen mit $q = r^m$. Der Frobeniusautomorphismus

$$\phi : \left\{ \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ a & \longmapsto & a^r \end{array} \right.$$

mit $\mathrm{Gal}(\mathbb{F}_q{:}\mathbb{F}_r) = \langle\phi\rangle$ operiere auf $\mathbb{F}_q^n$ durch komponentenweiser Operation, d.h. für $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ sei

$$\phi(\boldsymbol{x}) = (\phi(x_1), \ldots, \phi(x_n)).$$

Analog definieren wir die Spur eines Vektor $\boldsymbol{x} \in \mathbb{F}_q^n$ durch

$$\mathrm{Tr}_{\mathbb{F}_q:\mathbb{F}_r}(\boldsymbol{x}) = (\mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_r}(x_1), \ldots, \mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_r}(x_n)) = \sum_{j=0}^{m-1} \phi^j(\boldsymbol{x}).$$

Für einen linearen Code C aus $\mathbb{F}_q^n$ heißt

$$C|_{\mathbb{F}_r} := C \cap \mathbb{F}_r^n$$

die **Einschränkung** von C auf $\mathbb{F}_r$ und

$$\mathrm{Tr}(C) := \mathrm{Tr}_{\mathbb{F}_q:\mathbb{F}_r}(C) = \{\mathrm{Tr}_{\mathbb{F}_q:\mathbb{F}_r}(\boldsymbol{x}) : \boldsymbol{x} \in C\} \leq \mathbb{F}_r^n$$

der **Spurcode** von C. Man beachte, daß $C|_{\mathbb{F}_r}$ ein Teilcode von $\mathrm{Tr}(C)$ ist. Der Code C heißt $\phi-$**invariant** (oder $\phi-$**stabil**), falls $\phi(C) \leq C$ gilt.

Satz 4.15. (Delsarte)
Für einen linearen Code $C \leq \mathbb{F}_q^n$ gilt

$$(C|_{\mathbb{F}_r})^\perp = \mathrm{Tr}\left(C^\perp\right).$$

Beweis. Es seien $\boldsymbol{x} = (x_1, \ldots, x_n)$ ein Wort aus $C|_{\mathbb{F}_r}$ und $\boldsymbol{y} = (y_1, \ldots, y_n)$ Element des dualen Codes $C^\perp$. Dann gelten $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0$ und

$$\langle \boldsymbol{x}, \mathrm{Tr}(\boldsymbol{y}) \rangle = \sum_{i=1}^{n} x_i \,\mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_r}(y_i) = \mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_r}(\sum_{i=1}^{n} x_i y_i) = \mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_r}(\langle \boldsymbol{x}, \boldsymbol{y} \rangle) = 0$$

aufgrund der $\mathbb{F}_r$-Linearität der Spurabbildung. Das zeigt $\mathrm{Tr}\left(C^\perp\right) \leq (C|_{\mathbb{F}_r})^\perp$.
Es bleibt also noch die entgegengesetzte Inklusion zu zeigen. Diese folgt mit dem Nachweis von

$$\left(\mathrm{Tr}\left(C^\perp\right)\right)^\perp \leq C|_{\mathbb{F}_r}.$$

Dazu nehmen wir an, es gäbe ein Codewort $\boldsymbol{x} \in \left(\mathrm{Tr}\left(C^\perp\right)\right)^\perp$, das nicht in $C|_{\mathbb{F}_r}$ enthalten sei. Da $\boldsymbol{x}$ ein $\phi-$invarinates Wort ist, gilt daher auch $\boldsymbol{x} \notin C$. Folglich gibt

es ein $\boldsymbol{y} \in C^\perp$ mit $\langle \boldsymbol{x}, \boldsymbol{y} \rangle \neq 0$. Die Spurabbildung $\mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_r}$ ist nicht trivial. Somit gibt es ein $a \in \mathbb{F}_q$ mit

$$\mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_r}(\langle \boldsymbol{x}, a\boldsymbol{y} \rangle) = \mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_r}(a\langle \boldsymbol{x}, \boldsymbol{y} \rangle) \neq 0.$$

Andererseits gilt wie oben

$$\mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_r}(\langle \boldsymbol{x}, a\boldsymbol{y} \rangle) = \langle \boldsymbol{x}, \mathrm{Tr}(a\boldsymbol{y}) \rangle = 0,$$

da $\mathrm{Tr}(a\boldsymbol{y})$ Element von $\mathrm{Tr}\left(C^\perp\right)$ und $\boldsymbol{x}$ Element von $\left(\mathrm{Tr}\left(C^\perp\right)\right)^\perp$ ist. Dies führt zum Widerspruch unserer Annahme, was zu zeigen war. □

Korollar 4.16. *Für einen linearen Code $C \leq \mathbb{F}_q^n$ mit $q = r^m$ gelten:*

(a) *Die Dimension des Spurcodes von C ist beschränkt durch*

$$\dim_{\mathbb{F}_q}(C) \leq \dim_{\mathbb{F}_r}(\mathrm{Tr}(C)) \leq m \cdot \dim_{\mathbb{F}_q}(C).$$

(b) *Die Dimension der Einschränkung von C auf $\mathbb{F}_r$ ist beschränkt durch*

$$m \cdot \dim_{\mathbb{F}_q}(C) - (m-1) \cdot n \leq \dim_{\mathbb{F}_r}(C|_{\mathbb{F}_r}) \leq \dim_{\mathbb{F}_q}(C).$$

Beweis. Die Ungleichung in (b)

$$\dim_{\mathbb{F}_r}(C|_{\mathbb{F}_r}) \leq \dim_{\mathbb{F}_q}(C)$$

folgt aus der Tatsache, daß eine $\mathbb{F}_r-$Basis von $C|_{\mathbb{F}_r}$ auch linear unabhängig über $\mathbb{F}_q$ ist. Nach der Dimensionsformel erfüllt $\mathrm{Tr} : C \to \mathrm{Tr}(C)$ als $\mathbb{F}_r-$lineare Abbildung die Gleichung

$$\dim_{\mathbb{F}_r}(\mathrm{Tr}(C)) + \dim_{\mathbb{F}_r}(\mathrm{Kern}\ (\mathrm{Tr})) = \dim_{\mathbb{F}_r}(C) = m \cdot \dim_{\mathbb{F}_q}(C).$$

Das zeigt die zweite Ungleichung von (a). Es bleibt also noch der Nachweis der jeweils ersten Ungleichungen.
(a) Mit dem Satz von *Delsarte* und $\dim_{\mathbb{F}_r}(C^\perp|_{\mathbb{F}_r}) \leq \dim_{\mathbb{F}_q}(C^\perp)$ erhalten wir

$$\begin{aligned}\dim_{\mathbb{F}_r}(\mathrm{Tr}(C)) &= \dim_{\mathbb{F}_r}\left(\left(C^\perp|_{\mathbb{F}_r}\right)^\perp\right) \\ &= n - \dim_{\mathbb{F}_r}\left(C^\perp|_{\mathbb{F}_r}\right) \geq n - \dim_{\mathbb{F}_q}\left(C^\perp\right) = \dim_{\mathbb{F}_q}(C).\end{aligned}$$

(b) Analog erhält man nun mit (a)

$$\begin{aligned}\dim_{\mathbb{F}_r}(C|_{\mathbb{F}_r}) &= \dim_{\mathbb{F}_r}\left(\mathrm{Tr}\left(C^\perp\right)^\perp\right) = n - \dim_{\mathbb{F}_r}\mathrm{Tr}\left(C^\perp\right) \\ &\geq n - m \cdot \dim_{\mathbb{F}_q}\left(C^\perp\right) = n - m \cdot (n - \dim_{\mathbb{F}_q}(C)) \\ &= m \cdot \dim_{\mathbb{F}_q}(C) - (m-1) \cdot n.\end{aligned}$$

Das schließt den Beweis. □

Korollar 4.17. *Für einen linearen Code $C \leq \mathbb{F}_q^n$ sind äquivalent:*

(a) *C ist $\phi-$invariant.*

(b) *Die Dimension von C ist invariant unter der Spurabbildung, d.h. es gilt*

$$\dim_{\mathbb{F}_r}(\mathrm{Tr}(C)) = \dim_{\mathbb{F}_q}(C).$$

(c) *Die Dimension von C ist invariant unter Einschränkung auf $\mathbb{F}_r$, d.h. es gilt*

$$\dim_{\mathbb{F}_r}(C|_{\mathbb{F}_r}) = \dim_{\mathbb{F}_q}(C).$$

Beweis. (a) $\Rightarrow$ (b): Für einen $\phi-$invarianten Code C gilt insbesondere die Inklusion $\mathrm{Tr}(C) \leq C$ und somit folgt $\mathrm{Tr}(C) \leq C|_{\mathbb{F}_r}$. Mit Korollar 4.16 erhalten wir dann

$$\dim_{\mathbb{F}_q}(C) \leq \dim_{\mathbb{F}_r}(\mathrm{Tr}(C)) \leq \dim_{\mathbb{F}_r}(C|_{\mathbb{F}_r}) \leq \dim_{\mathbb{F}_q}(C).$$

(b) $\Rightarrow$ (c): Nach dem Satz von *Delsarte* gilt $\mathrm{Tr}(C) = \left(C^\perp|_{\mathbb{F}_r}\right)^\perp$. Also erhalten wir mit unserer Voraussetzung

$$\dim_{\mathbb{F}_q}(C) = \dim_{\mathbb{F}_r}(\mathrm{Tr}(C))) = \dim_{\mathbb{F}_r}(\left(C^\perp|_{\mathbb{F}_r}\right)^\perp) = n - \dim_{\mathbb{F}_r}\left(C^\perp|_{\mathbb{F}_r}\right)$$

und somit

$$\dim_{\mathbb{F}_r}\left(C^\perp|_{\mathbb{F}_r}\right) = n - \dim_{\mathbb{F}_q}(C) = \dim_{\mathbb{F}_q}\left(C^\perp\right).$$

Folglich besitzt $C^\perp$ eine Basis aus $\phi-$invarianten Elementen, und es gibt eine Kontrollmatrix zu C mit ausschließlich Einträgen aus $\mathbb{F}_r$. Das zeigt

$$\dim_{\mathbb{F}_r}(C|_{\mathbb{F}_r}) = \dim_{\mathbb{F}_q}(C).$$

(c) $\Rightarrow$ (a): Im Fall $\dim_{\mathbb{F}_r}(C|_{\mathbb{F}_r}) = \dim_{\mathbb{F}_q}(C)$ besitzt C eine Basis von $\phi-$invarianten Elementen, was die die $\phi-$Invarianz des gesamten Codes C zur Folge hat. □

Aufgabe 4.18. Es seien $C \leq \mathbb{F}_q^n$ ein linearer Code und $q = r^m$. Zeigen Sie:

(a) Enthält C einen $\phi-$invarianten Teilcode B, so gilt die Ungleichung

$$\dim_{\mathbb{F}_r}(\mathrm{Tr}(C)) \leq m \cdot (\dim_{\mathbb{F}_q}(C) - \dim_{\mathbb{F}_q}(B)) + \dim_{\mathbb{F}_r}(B|_{\mathbb{F}_r}).$$

(b) Es sei B ein $\phi-$invarianter Teilcode des dualen Codes $C^\perp$. Dann gelten:

$$\begin{aligned}
&\dim_{\mathbb{F}_r}(C|_{\mathbb{F}_r}) \\
&\quad \geq m \cdot (\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(B)) - \dim_{\mathbb{F}_r}(B|_{\mathbb{F}_r}) - (m-1) \cdot n \\
&\quad \geq m \cdot \dim_{\mathbb{F}_q}(C) + (m-1) \cdot \dim_{\mathbb{F}_q}(B) - (m-1) \cdot n.
\end{aligned}$$

Kapitel 5

Perfekte Codes

5.1 Hamming-Codes

Definition 5.1. (Perfekter Code)
Ein Code $C \subset \mathbb{F}_q^n$ mit ungerader Minimaldistanz $d(C) = 2e(C) + 1$ heißt **perfekt**, falls es zu jedem Element $\boldsymbol{y} \in \mathbb{F}_q^n$ genau ein Codewort $\boldsymbol{x} \in C$ mit Abstand $d(\boldsymbol{x}, \boldsymbol{y}) \leq e(C)$ gibt. Für $\boldsymbol{y} \in \mathbb{F}_q^n$ definiert

$$\mathbb{B}_r^n(\boldsymbol{y}) := \{\boldsymbol{z} \in \mathbb{F}_q^n : d(\boldsymbol{y}, \boldsymbol{z}) \leq r\}$$

eine Kugel vom Radius r um $\boldsymbol{y}$.

Einfache Beispiele perfekter Codes liefern die binären n-fachen Wiederholungscodes mit ungerader Länge $n = 2m + 1$. Solche $[n, 1, n]_2-$Codes besitzen den Fehlerkorrekturparameter m.

Bemerkung 5.2. (Kugelpackungsbedingung)
Für einen perfekten Code $C \leq \mathbb{F}_q^n$ gilt

$$q^n = \#C \cdot \sum_{i=0}^{e(C)} \binom{n}{i} (q-1)^i.$$

Beweis. Die Anzahl der Gitterpunkte in der Kugel $\mathbb{B}_e^n(\boldsymbol{x})$ vom Radius $e = e(C)$ beträgt

$$\#\mathbb{B}_e^n(\boldsymbol{x}) = \sum_{i=0}^{e} \binom{n}{i} (q-1)^i.$$

Da C perfekt ist, bilden die zu den Codewörtern $\boldsymbol{x} \in C$ gehörigen Kugeln $\mathbb{B}_e^n(\boldsymbol{x})$ eine disjunkte Vereinigung von $\mathbb{F}_q^n$. Hieraus folgt die Behauptung. □

Definition 5.3. (Hamming-Code)
Es seien $k > 1$ eine natürliche Zahl und $n := \frac{q^k-1}{q-1}$. Ein linearer $[n, n-k]_q-$Code C heißt **Hamming-Code** $\mathrm{Ham}[n, n-k]_q$, falls die Spalten der Kontrollmatrix zu C paarweise linear unabhängig sind.

Anmerkung 5.4. Nach Bemerkung 2.16 ist die Minimaldistanz eines Hamming-Codes $\mathrm{Ham}[n, n-k]_q$ mindestens 3. Umgekehrt ist auch jeder $[n, n-k, d]_q-$Code mit Länge $n = \frac{q^k-1}{q-1}$ und Minimaldistanz $d \geq 3$ ein Hamming-Code. Die Anzahl korrigierbarer Fehler eines Hamming-Codes $C = \mathrm{Ham}[n, n-k]_q$ beträgt

$$e(C) \geq 1.$$

Hammingscodes sind Codes mit guter Informationsrate vermöge

$$r(C) = \tfrac{n-k}{n} \xrightarrow[n\to\infty]{} 1.$$

Bemerkung 5.5. *Hamming-Codes sind perfekte Codes C mit Fehlerkorrekturparameter $e(C) = 1$.*

Beweis. Es sei $C := \mathrm{Ham}[n, n-k]_q$ ein Hamming-Code der Länge $n = \frac{q^k-1}{q-1}$. Eine Kugel in $\mathbb{F}_q^n$ vom Radius 1 enthält genau $1 + (q-1)n = q^k$ Elemente. Desweiteren sind die Kugeln $\mathbb{B}_1^n(\boldsymbol{x})$, $\mathbb{B}_1^n(\tilde{\boldsymbol{x}})$ um verschiedene Codewörter $\boldsymbol{x}, \tilde{\boldsymbol{x}} \in C$ disjunkt. Somit folgt

$$\sum_{\boldsymbol{x}\in C} \#\mathbb{B}_1^n(\boldsymbol{x}) = \#C \cdot q^k = q^n.$$

Also gibt es zu jedem $\boldsymbol{y} \in \mathbb{F}_q^n$ genau ein Codewort $\boldsymbol{x} \in C$ mit $d(\boldsymbol{x}, \boldsymbol{y}) \leq 1$. □

Satz 5.6. (Existenz von Hamming-Codes)

(a) *Zu jeder natürliche Zahl $k > 1$ gibt es einen Hamming-Code über $\mathbb{F}_q$ der Länge $\frac{q^k-1}{q-1}$.*

(b) *Im Fall $q = 2$ gibt es eine Kontrollmatrix zu $\mathrm{Ham}[n, n-k]_2$, deren Spalten aus den Koeffizienten der Binärdarstellung von $1, \ldots, 2^k - 1$ bestehen.*

Beweis. Man wähle aus allen 1-dimensionalen Unterräumen in $\mathbb{F}_q^k$ jeweils einen nichtverschwindenden Vektor als Spaltenvektor der Matrix H. Dann besteht H aus $n = \frac{q^k-1}{q-1}$ Spalten und ist somit als Element von $\mathbb{F}_q^{k\times n}$ Kontrollmatrix eines $[n, n-k]_q-$Codes C. Da zwei verschiedene 1-dimensionale Unterräume in $\mathbb{F}_q^k$ einen 2-dimensionalen Unterraum aufspannen, sind die Spalten von H paarweise linear unabhängig. Das beweist Aussage (a).
Die Behauptung für $q = 2$ in (b) folgt aus der Tatsache, daß die Binärdarstellungen je zwei verschiedener ganzer Zahlen über $\mathbb{F}_2$ linear unabhängig sind. □

Beispiel 5.7. Es gibt also Codes mit Minimaldistanz 3 zu den Parametern

	$q=2$	$q=3$	$q=4$	$q=5$
$k=2$	$[3,1]_2$	$[4,2]_3$	$[5,3]_4$	$\cdots$
$k=3$	$[7,4]_2$	$[13,10]_3$	$[21,18]_4$	
$k=4$	$[15,11]_2$	$[40,36]_3$	$[85,81]_4$	
$k=5$	$[31,26]_2$			
$\vdots$	$\cdots$			

Der Hamming-Code $\mathrm{Ham}[7,4]_2$ ist ein besonders wichtiges Beispiel und wird zur Konstruktion der Golay-Codes verwendet. Wir geben daher seine Kontroll- und Erzeugermatrix konkret an:

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \qquad G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

5.2 Konstruktion binärer Golay-Codes

Ziel dieses Abschnittes ist die Konstruktion nichttrivialer perfekter Codes mit Fehlerkorrekturparameter $e > 1$. Für diese muß notwendigerweise die Kugelpackungsgleichung

$$q^k \cdot \#\mathbb{B}_e^n = q^n$$

erfüllt sein. Hierzu findet man zum Beispiel im Fall $q = 2$ oder 3 die Relationen

$$2^{11} = 1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = \#\mathbb{B}_3^{23}$$

und

$$3^5 = 1 + \binom{11}{1} \cdot 2 + \binom{11}{2} \cdot 4 = \#\mathbb{B}_2^{11}.$$

Diese "kombinatorischen Glücksfälle" führen tatsächlich auf perfekte Codes mit Parametern $[23, 12, 7]_2$ und $[11, 6, 5]_3$, die sogenannten Golay-Codes.
Zur Realisierung des binären Golay-Codes betrachten wir den aus $\mathcal{H} := \mathrm{Ham}[7,4]_2$ durch ein Paritätsbit erweiterten $[8,4]_2-$Code $\hat{\mathcal{H}}$ (vgl. 4.1). Es ist dann

$$\hat{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

eine Generatormatrix zu $\hat{\mathcal{H}}$. Desweiteren seien $\mathcal{H}^*$ und $\hat{\mathcal{H}}^*$ die vermöge der Permutation $\sigma = (1\ 7)(2\ 6)(3\ 5)$ zu $\mathcal{H}$ bzw. $\hat{\mathcal{H}}$ äquivalenten Codes. Die Matrizen

$$G^* = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \quad \text{und} \quad \hat{G}^* = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

erzeugen dann $\mathcal{H}^*$ beziehungsweise $\hat{\mathcal{H}}^*$.

Bemerkung 5.8. *Die erweiterten Hamming-Codes $\hat{\mathcal{H}}$ und $\hat{\mathcal{H}}^*$ sind selbstduale $[8,4,4]_2-$Codes. Desweiteren sind diese Codes 4-dividierbar, d.h. jedes ihrer Wörter besitzt ein durch 4 teilbares Gewicht.*

Beweis. Nach Bemerkung 4.1 besitzen $\hat{\mathcal{H}}$ und $\hat{\mathcal{H}}^*$ Dimension 4 und Minimaldistanz 3 oder 4. Aufgrund des zugefügten Paritätsbits gilt $w(\boldsymbol{x}) \equiv 0 \pmod 2$ für sämtliche Wörter $\boldsymbol{x} \in \hat{\mathcal{H}}$ und somit $d(\hat{\mathcal{H}}) = d(\hat{\mathcal{H}}^*) = 4$. Die Selbstdualität folgt aus Dimensionsgründen und $\hat{G} \cdot \hat{G}^T = 0$ sowie $\hat{G}^* \cdot (\hat{G}^*)^T = 0$. Aufgrund ihrer Minimaldistanz und $\mathbf{1} \in \hat{\mathcal{H}}, \hat{\mathcal{H}}^*$ enthalten die erweiterten Hamming-Codes keine Wörter vom Gewicht 2 oder 6. Somit sind sie 4-dividierbar. □

Definition 5.9. (Binäre Golay-Codes)
Der aus den erweiterten Hamming-Codes $\hat{\mathcal{H}}$ und $\hat{\mathcal{H}}^*$ konstruierte binäre Code

$$\mathrm{Gol}_{24} := \{(\boldsymbol{x}+\boldsymbol{z}, \boldsymbol{y}+\boldsymbol{z}, \boldsymbol{x}+\boldsymbol{y}+\boldsymbol{z}) : \boldsymbol{x}, \boldsymbol{y} \in \hat{\mathcal{H}}, \boldsymbol{z} \in \hat{\mathcal{H}}^*\}$$

heißt **binärer Golay-Code** Gol_{24}. Der hieraus durch Streichen des letzten Symbols (Punktierung) verkürzte Code

$$\mathrm{Gol}_{23} := \mathrm{Gol}_{24}^{\vee 24}$$

heißt **binärer Golay-Code** Gol_{23}.

Satz 5.10. (Parameter und Gewichtspolynom zu Gol_{24})
Der Golay-Code Gol_{24} *ist ein selbstdualer* $[24, 12, 8]_2-$*Code mit erzeugender Funktion*

$$W_{\mathrm{Gol}_{24}}(X) = 1 + 759X^8 + 2576X^{12} + 759^{16} + X^{24}.$$

Beweis. Behauptung 1: Gol_{24} *ist ein* $[24, 12]_2-$*Code.*
Per Konstruktion besitzt Gol_{24} Länge 24 und Dimension $k \leq 12$, da $\hat{\mathcal{H}}$ 4-dimensional ist. Aus Ordnungsgründen reicht es zu zeigen, daß für jedes Wort $\boldsymbol{g} \in \mathrm{Gol}_{24}$ nur ein Tripel $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \in \hat{\mathcal{H}}^2 \times \hat{\mathcal{H}}^*$ mit $\boldsymbol{g} = (\boldsymbol{x}+\boldsymbol{z}, \boldsymbol{y}+\boldsymbol{z}, \boldsymbol{x}+\boldsymbol{y}+\boldsymbol{z})$ existiert. Zunächst betrachten wir den Schnitt $\hat{\mathcal{H}} \cap \hat{\mathcal{H}}^*$. Ein Wort $\boldsymbol{a} \in \hat{\mathcal{H}} \cap \hat{\mathcal{H}}^*$ hat die Gestalt

$$\begin{aligned}&(\quad a \quad , \quad b \quad , \quad c \quad , d, a+c+d, a+b+c, b+c+d, a+b+d) = \\ &(b'+c'+d', a'+b'+c', a'+c'+d', d', \quad c' \quad , \quad b' \quad , \quad a' \quad , a'+b'+d'),\end{aligned}$$

was man anhand der Erzeugermatrizen nachprüft. Durch einen Koordinatenvergleich bekommt man $d = d'$ und die Gleichungen

$$a = b'+c'+d' = (a+b+c)+(a+c+d)+d = b,$$

$$b = a'+b'+c' = (b+c+d)+(a+b+c)+(a+c+d) = c$$

sowie

$$c = a'+c'+d' = (b+c+d)+(a+c+d)+d = a+b+d = d.$$

Folglich sind die Symbole von $\boldsymbol{a}$ alle gleich, d.h. es ist

$$\hat{\mathcal{H}} \cap \hat{\mathcal{H}}^* = \{\mathbf{0}, \mathbf{1}\}.$$

Für zwei Tripel $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}), (\tilde{\boldsymbol{x}}, \tilde{\boldsymbol{y}}, \tilde{\boldsymbol{z}}) \in \hat{\mathcal{H}}^2 \times \hat{\mathcal{H}}^*$ mit

$$(\boldsymbol{x}+\boldsymbol{z}, \boldsymbol{y}+\boldsymbol{z}, \boldsymbol{x}+\boldsymbol{y}+\boldsymbol{z}) = (\tilde{\boldsymbol{x}}+\tilde{\boldsymbol{z}}, \tilde{\boldsymbol{y}}+\tilde{\boldsymbol{z}}, \tilde{\boldsymbol{x}}+\tilde{\boldsymbol{y}}+\tilde{\boldsymbol{z}}) \in \mathrm{Gol}_{24}$$

gilt notwendigerweise

$$\boldsymbol{x}+\tilde{\boldsymbol{x}} = \boldsymbol{z}+\tilde{\boldsymbol{z}}.$$

Folglich ist $\boldsymbol{x}+\tilde{\boldsymbol{x}}$ Element von $\hat{\mathcal{H}} \cap \hat{\mathcal{H}}^*$. Der Fall $\boldsymbol{x}+\tilde{\boldsymbol{x}} = \mathbf{1}$ kann nicht auftreten, denn dann wären $\boldsymbol{z} = \tilde{\boldsymbol{z}} + \mathbf{1}$ und $\boldsymbol{y} = \tilde{\boldsymbol{y}} + \mathbf{1}$, woraus aber

$$\tilde{\boldsymbol{x}} + \tilde{\boldsymbol{y}} + \tilde{\boldsymbol{z}} = \boldsymbol{x} + \boldsymbol{y} + \boldsymbol{z} + \mathbf{1}$$

folgte im Widerspruch zur Annahme. Also bleibt nur der Fall $\boldsymbol{x}+\tilde{\boldsymbol{x}} = \boldsymbol{z}+\tilde{\boldsymbol{z}} = \mathbf{0}$ übrig. Das zieht aber $\boldsymbol{y} = \tilde{\boldsymbol{y}}$ nach sich. Somit gehört zu jedem Wort aus Gol_{24} genau ein Tripel $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \in \hat{\mathcal{H}}^2 \times \hat{\mathcal{H}}^*$.

Behauptung 2: Gol_{24} *ist selbstdual.*

Konstruktionsgemäß gilt

$$\mathrm{Gol}_{24} = \langle (\boldsymbol{x}, \mathbf{0}, \boldsymbol{x}), (\mathbf{0}, \boldsymbol{y}, \boldsymbol{y}), (\boldsymbol{z}, \boldsymbol{z}, \boldsymbol{z}) : \boldsymbol{x}, \boldsymbol{y} \in \hat{\mathcal{H}}, \boldsymbol{z} \in \hat{\mathcal{H}}^* \rangle.$$

Da $\hat{\mathcal{H}}$ und $\hat{\mathcal{H}}^*$ nach Bemerkung 5.8 selbstdual sind, gelten

$$\langle (\boldsymbol{x}, \mathbf{0}, \boldsymbol{x}), (\boldsymbol{z}, \boldsymbol{z}, \boldsymbol{z}) \rangle = 2 \cdot \langle \boldsymbol{x}, \boldsymbol{z} \rangle = 0$$

sowie

$$\langle (\mathbf{0}, \boldsymbol{y}, \boldsymbol{y}), (\boldsymbol{z}, \boldsymbol{z}, \boldsymbol{z}) \rangle = 2 \cdot \langle \boldsymbol{y}, \boldsymbol{z} \rangle = 0.$$

Hieraus folgt die Selbstdualität von Gol_{24} aus Dimensionsgründen.

Behauptung 3: Gol_{24} *ist* 4*-dividierbar.*

Das oben angegebene Erzeugersystem von Gol_{24} ist nach Bemerkung 5.8 4-dividierbar. Wir zeigen, daß die Summe zweier 4-dividierbarer Wörter $\boldsymbol{g}, \boldsymbol{h} \in \mathrm{Gol}_{24}$ ebenfalls Gewicht $w(\boldsymbol{g}+\boldsymbol{h}) \equiv 0 \pmod 4$ besitzt. Daraus folgt dann die Behauptung.
Wir defineren $\boldsymbol{g} \cap \boldsymbol{h}$ durch

$$(\boldsymbol{g} \cap \boldsymbol{h})_i = \begin{cases} 1 & : \quad g_i = h_i = 1 \\ 0 & : \quad \text{sonst.} \end{cases}$$

Man beachte, daß $\langle \boldsymbol{g}, \boldsymbol{h} \rangle \equiv w(\boldsymbol{g} \cap \boldsymbol{h}) \pmod 2$ gilt. Da Gol_{24} selbstdual ist, folgt dementsprechend $w(\boldsymbol{g} \cap \boldsymbol{h}) \equiv 0 \pmod 2$. Das Gewicht der Summe $\boldsymbol{g}+\boldsymbol{h}$ erfüllt also die Kongruenz

$$w(\boldsymbol{g}+\boldsymbol{h}) = w(\boldsymbol{g}) + w(\boldsymbol{h}) - 2 \cdot w(\boldsymbol{g} \cap \boldsymbol{h}) \equiv 0 \pmod 4.$$

Behauptung 4: Gol_{24} *besitzt Distanz* 8*.*

Für ein Wort $\boldsymbol{x} \in \hat{\mathcal{H}}$ mit Minimalgewicht $w(\boldsymbol{x}) = 4$ ist $(\boldsymbol{x}, \mathbf{0}, \boldsymbol{x})$ ein Wort in Gol_{24} vom Gewicht 8. Es gilt daher $d(\mathrm{Gol}_{24}) \leq 8$. Aufgrund der 4-Dividierbarkeit von Gol_{24} müssen wir nur $d(\mathrm{Gol}_{24}) = 4$ ausschließen.

Wir nehmen also an, es gäbe ein Wort

$$\boldsymbol{g} = (\boldsymbol{x} + \boldsymbol{z}, \boldsymbol{y} + \boldsymbol{z}, \boldsymbol{x} + \boldsymbol{y} + \boldsymbol{z}) \in \mathrm{Gol}_{24}$$

mit Gewicht 4. Entsprechend der obigen Vorgehensweise erhält man

$$w(\boldsymbol{x} + \boldsymbol{z}) = w(\boldsymbol{x}) + w(\boldsymbol{z}) - 2w(\boldsymbol{x} \cap \boldsymbol{z}) \equiv 0 \pmod 2$$

und analog $w(\boldsymbol{x} + \boldsymbol{z}) \equiv w(\boldsymbol{x} + \boldsymbol{y} + \boldsymbol{z}) \equiv 0 \pmod 2$. Eine der drei Komponenten $\boldsymbol{x} + \boldsymbol{z}, \boldsymbol{y} + \boldsymbol{z}, \boldsymbol{x} + \boldsymbol{y} + \boldsymbol{z}$ von $\boldsymbol{g}$ ist also trivial. Ohne Einschränkung können wir $\boldsymbol{x} + \boldsymbol{z} = \boldsymbol{0}$ annehmen, d.h. es ist $\boldsymbol{x} = \boldsymbol{z} \in \hat{\mathcal{H}} \cap \hat{\mathcal{H}}^* = \{\boldsymbol{0}, \boldsymbol{1}\}$. Im Fall $\boldsymbol{x} = \boldsymbol{0}$ gilt

$$w(\boldsymbol{g}) = w(\boldsymbol{0}, \boldsymbol{y}, \boldsymbol{y}) = 2w(\boldsymbol{y}) \geq 8,$$

und im Fall $\boldsymbol{x} = \boldsymbol{1}$ entsprechend

$$w(\boldsymbol{g}) = w(\boldsymbol{0}, \boldsymbol{y} + \boldsymbol{1}, \boldsymbol{y}) = w(\boldsymbol{y} + \boldsymbol{1}) + w(\boldsymbol{y}) \geq 8.$$

Somit führt die Annahme $w(\boldsymbol{g}) = 4$ zum Widerspruch.
Berechnung des Gewichtspolynoms. Mit den Behauptungen 2, 3 und 4 gilt

$$W(X, Y) := W_{\mathrm{Gol}_{24}}(X, Y) = Y^{24} + aX^8Y^{16} + bX^{12}Y^{12} + aX^{16}Y^8 + X^{24}.$$

Dies führt auf die Gleichung $2 + 2a + b = W(1, 1) = \#C = 2^{12}$ bzw. $2a + b = 4094$. Desweiteren gewinnen wir aus der *MacWilliams - Identität* 2.21

$$W_{\mathrm{Gol}_{24}}(X, Y) = W_{\mathrm{Gol}_{24}^{\perp}}(X, Y) = \frac{1}{2^{12}}\, W_{\mathrm{Gol}_{24}}(X + Y, X - Y).$$

Es gilt also

$$\begin{aligned} &2^{12} \cdot W(X, Y) = \\ &(X - Y)^{24} + a(X + Y)^8(X - Y)^{16} + bX^{12}Y^{12} + a(X + Y)^{16}(X - Y)^8 + (X + Y)^{24} \\ &= (X - Y)^{24} + (X + Y)^{24} + a(X^2 - Y^2)^8[(X - Y)^8 + (X + Y)^8] + b(X^2 - Y^2)^{12}. \end{aligned}$$

Koeffizientenvergleich bei X^8Y^{16} liefert

$$2^{12}a = 2\binom{24}{8} + 2a\left[\binom{8}{0}\binom{8}{8} - \binom{8}{1}\binom{8}{6} + \binom{8}{2}\binom{8}{4} - \binom{8}{3}\binom{8}{2} + \binom{8}{4}\binom{8}{0}\right] + b\binom{12}{4}.$$

Daraus folgen $a = 759$ und $b = 2576$. □

Korollar 5.11. *Der Golay-Code* Gol_{23} *ist ein perfekter* $[23, 12, 7]_2-$*Code.*

Beweis. Da die Minimaldistanz von Gol_{24} mindestens 2 beträgt, bleibt die Dimension beim Streichen eines Symbols erhalten. Desweiteren folgen aus Satz 5.10 $d(\mathrm{Gol}_{23}) \geq 7$ und $e(\mathrm{Gol}_{23}) \geq 3$. Wir zeigen nun allgemeiner, daß jeder $(23, 2^{12}, d)_2-$ Code C

mit Minimaldistanz $d \geq 7$ perfekt ist. Aufgrund $d \geq 7$ sind je zwei Kugeln $\mathbb{B}_3^{23}(\boldsymbol{x})$, $\mathbb{B}_3^{23}(\tilde{\boldsymbol{x}})$ zu verschiedenen Codewörter $\boldsymbol{x}, \tilde{\boldsymbol{x}}$ aus C disjunkt. Aus

$$\#\mathbb{B}_3^{23}(\mathbf{0}) = 1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2^{11}$$

folgen dann

$$\#C \cdot \#\mathbb{B}_3^{23}(\mathbf{0}) = 2^{12} \cdot 2^{11} = 2^{23} = \#\mathbb{F}_2^{23}$$

und somit

$$\bigcup_{\boldsymbol{x} \in C} \mathbb{B}_3^{23}(\boldsymbol{x}) = \mathbb{F}_2^{23},$$

Daher ist C perfekt mit Minimaldistanz 7. □

Das Gewichtspolynom für Gol_{23} erhalten wir aus der folgenden in Hinblick auf Abschnitt 5.3 etwas allgemeiner gehaltenen

Bemerkung 5.12. *Ein beliebiger $(23, 2^{12}, 7)_2-$Code C mit $\mathbf{0} \in C$ besitzt die erzeugende Funktion*

$$W_C(X) = 1 + 253X^7 + 506X^8 + 1288X^{11} + 1288X^{12} + 506X^{15} + 253X^{16} + X^{23}.$$

Beweis. Es seien

$$C_i := \{\boldsymbol{x} \in C : w(\boldsymbol{x}) = i\}, \qquad M_j := \{\boldsymbol{y} \in \mathbb{F}_2^{23} : w(\boldsymbol{y}) = j\}$$

sowie

$$w_i := w_i(C) = \#C_i \quad \text{und} \quad m_j := \#M_j = \binom{23}{j}.$$

Wegen $d(C) = 7$ und $\mathbf{0} \in C$ gelten $w_0 = 1$ und $w_i = 0$ für $1 \leq i \leq 6$. Nach dem Beweis zu Korollar 5.11 ist C perfekt. Somit wird M_4 disjunkt überdeckt von den Kugeln $\mathbb{B}_3^{23}(\boldsymbol{x})$ aller Codewörter $\boldsymbol{x} \in C_1 \cup \cdots \cup C_7 = C_7$, d.h. es gilt

$$M_4 = \dot{\bigcup_{\boldsymbol{x} \in C_7}} \mathbb{B}_3^{23}(\boldsymbol{x}) \cap M_4$$

Das zeigt

$$m_4 = \sum_{\boldsymbol{x} \in C_7} \#(\mathbb{B}_3^{23}(\boldsymbol{x}) \cap M_4) = w_7 \cdot \tbinom{7}{4} \qquad \text{und} \qquad w_7 = \frac{\binom{23}{4}}{\binom{7}{4}} = 253.$$

Nun geht man unter Beachtung der Perfektheit von C induktiv vor: Die Menge M_5 der 5-gewichtigen Wörter ist disjunkt überdeckt von den Kugeln $\mathbb{B}_3^{23}(\boldsymbol{x})$ um $\boldsymbol{x} \in C$ mit $w(\boldsymbol{x}) = 7, 8$. Das hat

$$m_5 = w_7 \cdot \tbinom{7}{5} + w_8 \cdot \tbinom{8}{5} \qquad \text{und} \qquad w_8 = \frac{\binom{23}{5} - w_7 \cdot \binom{7}{5}}{\binom{8}{5}} = 506$$

zur Folge. Die Menge M_6 wird überdeckt von

$$M_6 = \dot{\bigcup_{i=7,8,9}} \dot{\bigcup_{\boldsymbol{x}_i \in C_i}} \mathbb{B}_3^{23}(\boldsymbol{x}_i) \cap M_6.$$

Dabei gelten

$$\#(\mathbb{B}_3^{23}(\boldsymbol{x}_7) \cap M_6) =$$
$$\#\{\boldsymbol{y} \in M_6 : d(\boldsymbol{x}, \boldsymbol{y}) = 1\} + \#\{\boldsymbol{y} \in M_6 : d(\boldsymbol{x}, \boldsymbol{y}) = 3\} = \binom{7}{6} + \binom{7}{5}\binom{16}{1}$$

und

$$\#(\mathbb{B}_3^{23}(\boldsymbol{x}_8) \cap M_6) = \#\{\boldsymbol{y} \in M_6 : d(\boldsymbol{x}, \boldsymbol{y}) = 2\} = \binom{8}{6}.$$

Wegen

$$m_6 = \binom{23}{6} = w_7 \cdot \#(\mathbb{B}_3^{23}(\boldsymbol{x}_7) \cap M_6) + w_8 \cdot (\mathbb{B}_3^{23}(\boldsymbol{x}_8) \cap M_6)$$

folgt hieraus $w_9 = 0$. Analog erhält man $w_{10} = 0$ aufgrund

$$\begin{aligned} m_7 = \binom{23}{7} &= w_7 \cdot \#(\mathbb{B}_3^{23}(\boldsymbol{x}_7) \cap M_7) + w_8 \cdot (\mathbb{B}_3^{23}(\boldsymbol{x}_8) \cap M_7) \\ &= w_7 \cdot \left(1 + \binom{7}{6}\binom{16}{1}\right) + w_8 \cdot \left(\binom{8}{7} + \binom{8}{6}\binom{15}{1}\right). \end{aligned}$$

Die Zahl w_{11} ist bestimmt durch die Anzahl der Elemente aus M_8, die nicht in den Kugeln $\mathbb{B}_3^{23}(\boldsymbol{x})$ der Codewörter $\boldsymbol{x}$ mit Gewicht 7 oder 8 enthalten sind, da M_8 disjunkt überdeckt wird von

$$M_8 = \dot{\bigcup_{i=7,8,11}} \dot{\bigcup_{\boldsymbol{x}_i \in C_i}} \mathbb{B}_3^{23}(\boldsymbol{x}_i) \cap M_8.$$

Das zeigt

$$w_{11} = \frac{\binom{23}{8} - w_7 \cdot \left(16 + \binom{7}{6}\binom{16}{2}\right) - w_8 \cdot \left(1 + \binom{8}{7}\binom{15}{1}\right)}{\binom{11}{8}} = 1288.$$

Wir überlassen es den Leser, diese Rechnung fortzusetzen. □

5.3 Charakterisierung binärer Golay-Codes

Definition 5.13. (Steinersystem)
Es sei M eine endliche Menge mit m Elementen. Eine Teilmenge $\mathcal{B} \subset \mathcal{P}(M)$ der Potenzmenge von M heißt $(t, b, m)-$**Steinersystem**, falls es die folgenden Eigenschaften hat:

(1) Jede Menge $B \in \mathcal{B}$ besitzt b Elemente.

(2) Jede Teilmenge $T \subset M$ mit t Elementen ist in genau einem $B \in \mathcal{B}$ enthalten.

Beispiel 5.14. (1) Die Geraden der affine Ebene $\mathbb{A}^2(\mathbb{F}_q)$ bilden ein $(2, q, q^2)-$Steinersystem, da zwei Punkte in $\mathbb{A}^2(\mathbb{F}_q)$ genau eine Gerade erzeugen.
(2) Die Geraden der projektiven Ebene $\mathbb{P}^2(\mathbb{F}_q)$ bilden ein $(2, q+1, q^2+q+1)-$ Steinersystem.

Binäre Worte $\boldsymbol{x} \in \mathbb{F}_2^n$ können mit ihren Träger $I_{\boldsymbol{x}} := \{1 \leq i \leq n : x_i \neq 0\}$ identifiziert werden. Damit übertragen wir das Inklusionssymbol von $\{1, \ldots, n\}$ auf $\mathbb{F}_2^n$, d.h. wir schreiben $\boldsymbol{x} \subset \boldsymbol{y}$ im Fall $I_{\boldsymbol{x}} \subset I_{\boldsymbol{y}}$.

Aufgabe 5.15. Es sei $\hat{\mathcal{H}} := \hat{\text{Ham}}[2^m - 1, 2^m - 1 - m]_2$ der durch ein Paritätsbit erweiterte Hamming-Code. Zeigen Sie, daß die Codewörter in $\hat{\mathcal{H}}$ vom Gewicht 4 ein $(3, 4, 2^m)-$ Steinersystem bilden.

Bemerkung 5.16. *Die Codewörter des Golay-Codes* Gol_{24} *vom Gewicht* 8 *bilden ein* $(5, 8, 24)-$*Steinersystem.*

Beweis. Es sei $\boldsymbol{x} \in \mathbb{F}_2^{24}$ ein Wort vom Gewicht $w(\boldsymbol{x}) = 5$. Gemäß unserer Behauptung reicht zu zeigen, daß die Kugel $\mathbb{B}_3^{24}(\boldsymbol{x})$ mit Radius 3 genau ein Codewort $\boldsymbol{g} \in \text{Gol}_{24}$ enthält, da hieraus automatisch $w(\boldsymbol{g}) = 8$ und $\boldsymbol{x} \subset \boldsymbol{g}$ folgen.
Für zwei Codewörter $\boldsymbol{g}, \boldsymbol{h} \in \mathbb{B}_3^{24}(\boldsymbol{x})$ gilt nach der Dreiecksungleichung

$$d(\boldsymbol{g}, \boldsymbol{h}) \leq d(\boldsymbol{g}, \boldsymbol{x}) + d(\boldsymbol{x}, \boldsymbol{h}) \leq 6.$$

Da Gol_{24} Minimaldistanz 8 besitzt, folgt hieraus $\boldsymbol{g} = \boldsymbol{h}$. Die Kugel $\mathbb{B}_3^{24}(\boldsymbol{x})$ enthält also höchstens ein Codewort von Gewicht 8.
Desweiteren ist $\mathbb{B}_3^{24}(\boldsymbol{x}) \cap \text{Gol}_{24}$ nicht leer. Denn zu jedem Codewort $\boldsymbol{g} \in \text{Gol}_{24}$ vom Gewicht 8 gibt es genau $\binom{8}{5}$ Elemente $\boldsymbol{y} \in \mathbb{F}_2^{24}$ mit $w(\boldsymbol{y}) = 5$ und $\boldsymbol{y} \subset \boldsymbol{g}$. Die Anzahl aller $\boldsymbol{y} \in \mathbb{F}_2^{24}$ mit $w(\boldsymbol{y}) = 5$ und $\mathbb{B}_3^{24}(\boldsymbol{y}) \cap \text{Gol}_{24} \neq \emptyset$ beträgt also

$$w_8(\text{Gol}_{24}) \cdot \binom{8}{5} = 759 \cdot \binom{8}{5} = \binom{24}{5} = \#\{\boldsymbol{y} \in \mathbb{F}_2^{24} : w(\boldsymbol{y}) = 5\}$$

und stimmt daher mit der Anzahl sämtlicher Wörter in $\mathbb{F}_2^{24}$ vom Gewicht 5 überein. Das zeigt $\mathbb{B}_3^{24}(\boldsymbol{x}) \cap \text{Gol}_{24} \neq \emptyset$. □

Satz 5.17. (Witt, 1938)
Das $(5, 8, 24)-$*Steinersystem ist bis auf Äquivalenz eindeutig bestimmt.*

Ohne Beweis. (siehe [Lü89, §12] und [MS77, Ch.20 §5])

Satz 5.18. *Jeder* $(24, 2^{12}, 8)_2-$*Code* C *mit* $\mathbf{0} \in C$ *ist äquivalent zum binären Golay-Code* Gol_{24}.

Beweis. Es sei C ein binärer $(24, 2^{12}, 8)_2-$Code mit $\mathbf{0} \in C$. Die um ein Symbol verkürzten Codes $C^{\vee 1}, \ldots, C^{\vee 24}$ behalten aufgrund $d(C) \geq 2$ die Elementanzahl 2^{12}

und sind daher nach dem Beweis zu Korollar 5.11 und Lemma 5.12 perfekte Codes mit Gewichtsspektrum

$$\text{Gewichte}(C^{\vee i}) = \{0, 7, 8, 11, 12, 15, 16, 23\}.$$

Da dies unabhängig von der Wahl des zu streichenden Symbols in C ist, folgt hieraus

$$\text{Gewichte}(C) = \{0, 8, 12, 16, 24\}.$$

Der Abstand $d(\boldsymbol{x}, \boldsymbol{y})$ zweier Codewörter $\boldsymbol{x}, \boldsymbol{y} \in C$ ist also stets durch 4 teilbar, was $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0$ zur Folge hat. Daher sind C wie auch der von C erzeugte lineare Code $\langle C \rangle$ selbstdual mit $\dim\langle C \rangle = 12$, woraus $C = \langle C \rangle$ folgt. Wir haben also gezeigt, daß jeder $\mathbf{0}$ enthaltende $(24, 2^{12}, 8)_2-$Code linear ist. Der Beweis zu Bemerkung 5.16 ist für beliebige $[24, 12, 8]_2-$Codes gültig, also bilden die Codewörter in C vom Gewicht 8 ein $(5, 8, 24)-$Steinersystem. Da dieses $(5, 8, 24)-$Steinersystem nach dem Satz von *Witt* bis auf Äquivalenz eindeutig ist und Gol_{24} von Codewörter des Gewichtes 8 erzeugt wird, folgt hieraus die Äquivalenz von C und Gol_{24}. □

Wir werden im Abschnitt 7.3 eine andere Konstruktion des Golay-Codes Gol_{24} kennenlernen. Nach dem obigen Satz 5.18 ist der in Beispiel 7.12 vorgestellte erweiterte quadratische Reste-Code $\hat{\mathcal{Q}}_{23}$ äquivalent zu Gol_{24}. Da die Symmtriegruppe von $\hat{\mathcal{Q}}_{23}$ transitiv ist (Satz 7.9), hat auch Gol_{24} eine transitive Symmetriegruppe. Hieraus folgt

Korollar 5.19. *Jeder $(23, 2^{12}, 7)_2-$Code C mit $\mathbf{0} \in C$ ist äquivalent zu* Gol_{23}.

Beweis. Es seien $\boldsymbol{x}, \boldsymbol{y} \in C$ zwei Codewörter mit Minimalabstand $d(\boldsymbol{x}, \boldsymbol{y}) = 7$. Dann gilt

$$w(\boldsymbol{x} \cap \boldsymbol{y}) \equiv \langle \boldsymbol{x}, \boldsymbol{y} \rangle \equiv d(\boldsymbol{x}, \boldsymbol{y}) \equiv 1 \pmod 2,$$

wobei $\boldsymbol{x} \cap \boldsymbol{y}$ wie im Beweis zu Satz 5.10 definiert ist. Die Quersummen beider Wörter können also nicht gleichzeitig gerade sein. Der durch ein Paritätsbit erweiterte Code $\hat{C}$ ist also ein $(24, 2^{12}, 8)_2-$Code und damit äquivalent zu Gol_{24}. Somit entsteht C durch Streichen eines Symbols in Gol_{24}, etwa das i-te Symbol. Da die Symmetriegruppe zu Gol_{24} transitiv ist, ergibt sich

$$C \cong \text{Gol}_{24}^{\vee i} \cong (\sigma(\text{Gol}_{24}))^{\vee 24} = \text{Gol}_{24}^{\vee 24} = \text{Gol}_{23}$$

für ein $\sigma \in \text{Sym}(\text{Gol}_{24})$ mit $\sigma(i) = 24$. □

Zusatz 5.20. *Die Symmetriegruppen der binären Golay-Codes sind die Mathieu-Gruppen* $\mathbf{M}_{24}$ *und* $\mathbf{M}_{23}$. *Genauer gelten:*

$$\text{Sym}(\text{Gol}_{24}) \cong \mathbf{M}_{24} \qquad \textit{und} \qquad \text{Sym}(\text{Gol}_{23}) \cong \mathbf{M}_{23},$$

mit $\#\mathbf{M}_{24} = 244.823.040$ *und* $\#\mathbf{M}_{23} = 10.200.960$.

Ohne Beweis.(siehe [Lin99, 4.2.3])

5.4 Ternäre Golay-Codes

Satz 5.21. (Ternäre Golay-Codes Gol_{12} und Gol_{11})

(a) *Es gibt einen bis auf Äquivalenz eindeutig bestimmten* $[12, 6, 6]_3-$*Code* Gol_{12} *zum* $(5, 6, 12)-$ *Steinersystem mit* $\mathrm{Sym}(\mathrm{Gol}_{12}) \cong \mathbf{M}_{12}$ *und* $\#\mathbf{M}_{12} = 95040$.

(b) *Es gibt einen bis auf Äquivalenz eindeutig bestimmten perfekten* $[11, 6, 5]_3-$*Code* Gol_{11} *zum* $(4, 5, 11)-$*Steinersystem mit* $\mathrm{Sym}(\mathrm{Gol}_{11}) \cong \mathbf{M}_{11}$ *und* $\#\mathbf{M}_{11} = 7920$.

Ohne Beweis.(siehe [Lü89, §7] und [MS77, Ch.20])

Die perfekten Code mit Fehlerkorrekturparameter $e > 1$ sind vollständig bekannt:

Zusatz 5.22. *Ein perfekter Code mit Fehlerkorrekturparameter* $e > 1$ *ist äquivalent zu einem der Golay-Codes* Gol_{23} *bzw.* Gol_{11} *oder zum* $[2e + 1, 1, 2e + 1]_2-$*Wiederholungscode. Insbesondere gibt es keine perfekten Codes über* $\mathbb{F}_q$ *mit* $q \neq 2, 3$.

Ohne Beweis.(siehe [Lin99, Ch.7])

Kapitel 6

Zyklische Codes

6.1 Polynomdarstellung zyklischer Codes

Definition 6.1. (Zyklischer Code)
Ein linearer Code C der Länge n mit der Eigenschaft

$$(x_1, \ldots, x_n) \in C \Longleftrightarrow (x_n, x_1, \ldots, x_{n-1}) \in C$$

heißt **zyklischer Code**.

Die Symmetriegruppe $\mathrm{Sym}(C)$ eines zyklischen Codes der Länge n umfaßt also per Definition die zyklische Gruppe $\mathbf{Z}_n$. Mit dem Vektorraumisomorphismus

$$\rho : \begin{cases} \mathbb{F}_q^{\,n} & \longrightarrow & \mathbb{F}_q[X]/(X^n-1) \\ (x_0, \ldots, x_{n-1}) & \longmapsto & \sum_{i=0}^{n-1} x_i X^i \end{cases}$$

zwischen $\mathbb{F}_q^{\,n}$ und $R_n := \mathbb{F}_q[X]/(X^n-1)$ erhält man ein notwendiges und hinreichendes Kriterium für die Zyklizität eines linearen Codes $C \leq \mathbb{F}_q^{\,n}$.

Bemerkung 6.2. *Ein linearer Code $C \leq \mathbb{F}_q^{\,n}$ ist genau dann zyklisch, falls sein Bild $\rho(C) \leq R_n$ unter ρ ein Ideal in R_n ist.*

Beweis. Nach Konstruktion des Isomorphismus ρ ist für einen zyklischen Code C notwendig und hinreichend, daß $X \cdot \rho(C) \leq \rho(C)$ gilt. Dies ist aber genau dann der Fall, wenn $\rho(C)$ ein Ideal in R_n íst. □

Wir können also einen zyklischen Code C als Ideal in $R_n = \mathbb{F}_q[X]/(X^n-1)$ betrachten. Dies werden wir im folgenden auch stets tun.

Bemerkung 6.3. (Ideale in $\mathbb{F}_q[X]/(X^n-1)$)

(a) *Jedes Ideal in R_n ist ein Hauptideal und wird von einem Teiler des Polynoms X^n-1 erzeugt.*

(b) *Sind n und q teilerfremd, so ist $X^n - 1$ separabel. Bezeichnet in diesem Fall t die Anzahl der irreduziblen normierten Teiler von $X^n - 1$, so gibt es genau 2^t zyklische Codes über $\mathbb{F}_q$ der Länge n.*

Beweis. (a) Es sei π der kanonische Epimorphismus von $\mathbb{F}_q[X]$ auf $R_n = \mathbb{F}_q[X]/(X^n - 1)$. Für ein Ideal I in R_n ist dann $\pi^{-1}(I)$ ein Ideal in $\mathbb{F}_q[X]$. Da $\mathbb{F}_q[X]$ ein Hauptidealring ist, wird $\pi^{-1}(I)$ von einen Polynom $g(X) \in \mathbb{F}_q[X]$ erzeugt. Wegen $\pi(X^n - 1) = 0$ gilt dann

$$(X^n - 1) \subseteq \pi^{-1}(I) = (g(X)).$$

Also ist $g(X)$ ein Teiler von $X^n - 1$.
(b) Sind n und q teilerfremd, so sind es auch $X^n - 1$ und nX^{n-1}. Daher ist $X^n - 1$ separabel und besitzt $\binom{t}{1} + \binom{t}{2} + \cdots + \binom{t}{t} = (1+1)^t = 2^t$ normierte Teiler. □

Definition 6.4. (Erzeuger- und Kontrollpolynom zyklischer Codes)
Es seien $C \trianglelefteq R_n = \mathbb{F}_q[X]/(X^n - 1)$ ein zyklischer Code und $g(X) \in \mathbb{F}_q[X]$ das normierte Polynom mit $C = (g(X))_{R_n}$. Dann heißt $g(X)$ **Erzeugerpolynom** und

$$h(X) := (X^n - 1)g(X)^{-1}$$

Kontrollpolynom von C. Wir nennen C einen **maximalen** (**minimalen**) **zyklischen Code**, falls $g(X)$ (bzw. $h(X)$) irreduzibel ist.

Vorsicht! Das Erzeugerpolynom ist nicht zu verwechseln mit der erzeugenden Funktion $W_C(X)$ aus Definition 2.18.

Notiz 6.5. Der Grad des Erzeugerpolynoms $g(X)$ eines zyklischen $[n,k]_q-$Codes beträgt $n - k$ wegen

$$C = \langle g(X), Xg(X), \ldots, X^{k-1}g(X) \rangle.$$

Sind $g(X) = \sum_{i=0}^{n-k} g_i X^i$ und dazu $h(X) = \sum_{i=0}^{k} h_i X^i$, so ist

$$G = \begin{pmatrix} g_0 & \cdots & g_{n-k} & & 0 \\ & \ddots & & \ddots & \\ 0 & & g_0 & \cdots & g_{n-k} \end{pmatrix} \in \mathbb{F}_q^{k \times n}$$

eine Erzeugermatrix und

$$H = \begin{pmatrix} 0 & & h_k & \cdots & h_0 \\ & \ddots & & \ddots & \\ h_k & \cdots & h_0 & & 0 \end{pmatrix} \in \mathbb{F}_q^{(n-k) \times n}$$

eine Kontrollmatrix zu C.

Bemerkung 6.6. (Kontrollgleichung für zyklische Codes)
Für einen zyklischen Code $C \trianglelefteq R_n$ mit Kontrollpolynom $h(X)$ gilt

$$C = \{f(X) \in R_n : f(X) \cdot h(X) = 0\}.$$

Beweis. Ein Polynom $f(X)$ aus C ist ein Vielfaches des Erzeugerpolynoms $g(X)$, d.h. es gilt $f(X) = a(X)g(X)$ für ein geeignetes Polynom $a(X)$. Da $g(X)h(X) = X^n - 1 = 0$ in R_n gilt, erfüllt $f(X)$ die Kontrollgleichung $f(X)h(X) = 0$. Umgekehrt gilt für jedes $f(X)$ mit $f(X)h(X) = 0$ die Teilerbedingung $g(X)|f(X)$, d.h. $f(X)$ ist ein Element des Codes C. □

Satz 6.7. *Die Klasse der zyklischen Codes ist abgeschlossen bezüglich Dualisierung. Genauer gilt: Ist $g(X)$ das Erzeugerpolynom eines zyklischen Codes $C \trianglelefteq R_n$ und $h(X)$ das zugehörige Kontrollpolynom, so sind*

$$g^{\perp}(X) = h(0)^{-1}h(X^{-1})X^k \qquad \textit{und} \qquad h^{\perp}(X) = g(0)^{-1}g(X^{-1})X^{n-k}$$

Erzeuger- und Kontrollpolynom des dualen Codes $C^{\perp}$.

Beweis. Die in Notiz 6.5 beschriebene Kontrollmatrix H eines zyklischen Codes C ist gleichzeitig auch eine Erzeugermatrix des dualen Codes $C^{\perp}$. Somit ergibt sich aus der Gestalt von H, daß das Ideal $C^{\perp} \trianglelefteq R_n$ vom Polynom

$$h_k + h_{k-1}X + \cdots + h_0X^k = h(X^{-1})X^k$$

erzeugt wird. Hieraus erhält man durch Normierung das Erzeugerpolynom von $C^{\perp}$. Auf dieselbe Weise gewinnt man das Kontrollpolynom zu $h^{\perp}(X)$ aus $g(X)$. □

Aufgabe 6.8. (a) Es sei C ein zyklischer Code über $\mathbb{F}_{q^m}$. Zeigen Sie, daß der Teilkörpercode $C|_{\mathbb{F}_q}$ ebenfalls zyklisch ist.
(b) Es seien C_1 und C_2 zwei zyklische Codes über $\mathbb{F}_q$ der Länge n_1 respektive n_2. Zeigen Sie, daß auch das Tensorprodukt $C_1 \otimes C_2$ dieser Codes zyklisch ist.

Satz 6.9. *Sind n und q teilerfremd, so wird jeder zyklische Code $C \trianglelefteq R_n$ von genau einem Idempotent in R_n erzeugt.*

Beweis. Existenz: Gemäß der Voraussetzung $\mathrm{ggT}(n, q) = 1$ ist $X^n - 1 = g(X)h(X)$ separabel (vgl. Bem. 6.3), und somit sind Erzeugerpolynom $g(X)$ und Kontrollpolynom $h(X)$ von C teilerfremd. Es gibt also Polynome $a(X), b(X) \in \mathbb{F}_q[X]$ mit

$$1 = a(X)g(X) + b(X)h(X).$$

Dann ist

$$e(X) := a(X)g(X) = 1 - b(X)h(X)$$

als Vielfaches von $g(X)$ ein Element des Codes C und idempotent, da es im Restklassenring R_n die Gleichung

$$e(X)^2 = a(X)g(X)(1 - b(X)h(X)) = a(X)g(X) - a(X)b(X)(X^n - 1) = e(X)$$

erfüllt. Weil jedes Codewort $c(X) \in C$ ein Vielfaches von $g(X)$ ist, wirkt $e(X) = 1 - b(X)h(X)$ als Identität auf C. Das zeigt schließlich

$$R_n \cdot e(X) \leq C = C \cdot e(X) \leq R_n \cdot e(X).$$

Eindeutigkeit: Für ein Idempotent $\tilde{e}(X) \in C$ mit $C = R_n \cdot \tilde{e}(X)$ gilt ebenfalls $\tilde{e}(X)c(X) = c(X)$ für alle Wörter $c(X) \in C$ und somit

$$\tilde{e}(X) = \tilde{e}(X)e(X) = e(X).$$

Das zeigt die Eindeutigkeit des erzeugenden Idempotents von C. □

Korollar 6.10. *Es sei $C \trianglelefteq R_n$ ein zyklischer Code mit erzeugenden Idempotent $e(X) = \sum_{i=0}^{n-1} e_i X^i$. Dann ist*

$$G = \begin{pmatrix} e_0 & e_1 & \cdots & e_{n-2} & e_{n-1} \\ e_{n-1} & e_0 & & e_{n-3} & e_{n-2} \\ \vdots & & & \vdots & \\ e_{n-k+1} & e_{n-k+2} & \cdots & e_{n-k-1} & e_{n-k} \end{pmatrix}$$

eine Erzeugermatrix von C.

Beweis. Die Behauptung dieses Korollars ist äquivalent zu

$$C = \langle e(X), Xe(X), \ldots, X^{k-1}e(X) \rangle.$$

Daher reicht es zu zeigen, daß aus

$$\sum_{i=0}^{k-1} a_i X^i e(X) = a(X)e(X) = 0$$

für ein Polynom $a(X) = \sum_{i=0}^{k-1} a_i X^i \in R_n$ stets $a(X) = 0$ folgt. Es sei also $a(X)$ ein Polynom vom Grad $\deg(a(X)) < k$ mit $a(X)e(X) = 0$ in R_n. Es gilt dann

$$0 = a(X)e(X)g(X) = a(X)g(X) = \sum_{i=0}^{k-1} a_i X^i g(X),$$

da $e(X)$ als Identität auf C wirkt. Weil aber $\{g(X), Xg(X), \ldots, X^{k-1}g(X)\}$ eine Basis von C ist, folgt hieraus $a(X) = 0$. □

6.2 Nullstellen zyklischer Codes

Für den Rest des Kapitels setzen wir stets voraus, daß die Alphabetgröße q und die Länge n der Codes teilerfremd zueinander sind.

Bemerkung 6.11. (Nullstellenmenge eines zyklischen Codes)
Es sei $C \trianglelefteq R_n$ ein zyklischer Code über $\mathbb{F}_q$. Dann gibt es eine Menge $U(C)$ von n-ten Einheitswurzeln aus $\overline{\mathbb{F}}_q$ mit

$$C = \{f(X) \in R_n : f(u) = 0 \text{ für alle } u \in U(C)\}.$$

Beweis. Als Teiler von $X^n - 1$ besitzt das Erzeugerpolynom $g(X)$ von C lediglich n-te Einheitswurzeln aus dem algebraischen Abschluß $\overline{\mathbb{F}}_q$ von $\mathbb{F}_q$ als Nullstellen. Da alle Codewörter aus C Vielfache von $g(X)$ sind, folgt die Behauptung mit

$$U(C) = \{u \in \overline{\mathbb{F}}_q : g(u) = 0\}. \qquad \square$$

Korollar 6.12. (Kontrollgleichung via Nullstellenmenge)
Es sei $C \trianglelefteq R_n$ ein zyklischer $[n,k]_q-$Code mit Nullstellenmenge $U(C) = \{u_1, \ldots, u_{n-k}\}$. Mit

$$L := \begin{pmatrix} 1 & u_1 & \cdots & u_1^{n-1} \\ \vdots & & & \vdots \\ 1 & u_{n-k} & \cdots & u_{n-k}^{n-1} \end{pmatrix}$$

gilt dann

$$C = \left\{ \sum_{i=0}^{n-1} x_i X^i \in R_n : L \cdot (x_0, \ldots, x_{n-1})^T = 0 \right\}. \qquad \square$$

Korollar 6.13. *Es seien $U_n := \{u \in \overline{\mathbb{F}}_q : u^n = 1\}$ die Menge aller n-ten Einheitswurzeln in $\overline{\mathbb{F}}_q$, C ein zyklischer Code über $\mathbb{F}_q$ und $U(C)$ sowie $U(C^\perp)$ die zugehörigen Nullstellenmengen von C und $C^\perp$. Dann sind $U(C)^{-1}$ und $U(C^\perp)$ komplementär in U_n, d.h. es gilt*

$$U(C^\perp) = U_n \backslash \{u^{-1} : u \in U(C)\}.$$

Beweis. Nach Satz 6.7 gilt für das Erzeugerpolynom $g^\perp(X)$ zu $C^\perp$

$$g^\perp(u^{-1}) = h(0)^{-1} h(u) u^{-k}.$$

Da $h(X)$ die Nullstellenmenge $U_n \backslash U(C)$ besitzt, folgt hieraus die Behauptung. $\square$

Aufgabe 6.14. Es seien n und q teilerfremd, $n = \frac{q^k-1}{q-1}$ und $u \in \mathbb{F}_{q^k}$ eine primitive n-te Einheitswurzel. Zeigen Sie, daß

$$C = \{f(X) \in \mathbb{F}_q[X]/(X^n - 1) : f(u) = 0\}$$

der Hamming-Code $\mathrm{Ham}[n, n-k]_q$ ist.

Satz 6.15. (BCH - Schranke)
Es seien $C \trianglelefteq R_n$ ein zyklischer $[n,k]_q-$Code mit Nullstellenmenge $U(C)$ und u eine primitive n-te Einheitswurzel. Es gebe natürliche Zahlen b und $2 \leq d \leq n+1$, sodaß die Elemente $u^b, \ldots, u^{b+d-2}$ in $U(C)$ enthalten sind. Dann besitzt C mindestens die Minimaldistanz d.

Beweis. Angenommen, es gäbe ein Codewort $c(X) = \sum_{i=0}^{n-1} x_i X^i = \sum_{j=1}^{r} x_{i_j} X^{i_j}$ aus C vom Gewicht $0 < r < d$. Dann ist nach Voraussetzung $\{u^b, \ldots, u^{b+r-1}\}$ in der Nullstellenmenge $U(C)$ enthalten und $(x_{i_1}, \ldots, x_{i_r})$ ist eine nichtriviale Lösung des homogenen linearen Gleichungssystems

$$\begin{array}{ccccccc} x_{i_1}(u^b)^{i_1} & + & \cdots & + & x_{i_r}(u^b)^{i_r} & = & 0 \\ \vdots & & & & \vdots & & \vdots \\ x_{i_1}(u^{b+r-1})^{i_1} & + & \cdots & + & x_{i_r}(u^{b+r-1})^{i_r} & = & 0. \end{array}$$

Somit verschwindet die Determinante von

$$L := \begin{pmatrix} u^{bi_1} & \cdots & u^{bi_r} \\ \vdots & & \vdots \\ u^{(b+r-1)i_1} & \cdots & u^{(b+r-1)i_r} \end{pmatrix}.$$

Andererseits gilt nach dem Satz über Vandermondesche Matrizen

$$\begin{aligned} \det(L) &= \left(\prod_{j=1}^{r} u^{bi_j}\right) \cdot \begin{vmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ (u^{i_1})^{r-1} & \cdots & (u^{i_r})^{r-1} \end{vmatrix} \\ &= \left(\prod_{j=1}^{r} u^{bi_j}\right) \cdot \left(\prod_{j<k} (u^{i_k} - u^{i_j})\right) \neq 0, \end{aligned}$$

was zum Widerspruch führt. □

Korollar 6.16. *Es sei r eine zu n teilerfremde Zahl. Dann ist $d(C) \geq d$ auch im Fall $u^b, u^{b+r}, \ldots, u^{b+r(d-2)} \in U(C)$ gültig.*

Beweis. Mit u ist $w := u^r$ aufgrund von $\mathrm{ggT}(r, n) = 1$ ebenfalls eine primitive $n-$te Einheitswurzel. Somit gibt es eine ganze Zahl $\tilde{b}$ mit $u^b = w^{\tilde{b}}$. Daher folgt unsere Behauptung aus der *BCH-Schranke* vermöge $w^{\tilde{b}}, w^{\tilde{b}+1}, \ldots, w^{\tilde{b}+d-2} \in U(C)$. □

6.3 BCH - Codes

Definition 6.17. (BCH - Code)
Es seien u ein Erzeuger der multiplikativen Gruppe $(\mathbb{F}_{q^m})^\times = \langle u \rangle$ sowie $U_{b,d} := \{u^b, \ldots, u^{b+d-2}\}$ mit $d \leq q^m + 1$. Weiter sei $g(X)$ das Produkt aller verschiedenen Minimalpolynome der $u^j \in U_{b,d}$ über $\mathbb{F}_q$. Dann heißt der durch $g(X)$ erzeugte zyklische Code C über $\mathbb{F}_q$ **BCH - Code mit garantierter Minimaldistanz** d. Diese sind benannt nach *R.C. Bose, D.K. Ray-Chandhuri* und *A. Hocquengham*. Desweiteren nennen wir einen BCH-Code C **primitiv (im engeren Sinne)**, falls C Länge $q^m - 1$ besitzt und u^b ebenfalls ein Erzeuger von $\mathbb{F}_{q^m}^\times$ ist. Für primitive BCH-Codes kann man also o.E. $b = 1$ annehmen.

Die Namensgebung der BCH-Codes ist gerechtfertigt, da BCH-Codes aufgrund der *BCH-Schranke* wenigstens Minimalabstand d besitzen.

Anmerkung 6.18. (BCH- und Reed-Solomon Codes)
(a) Die primitiven BCH-Codes über $\mathbb{F}_q$ der Länge $n = q-1$ sind genau die gewöhnlichen Reed-Solomon Codes $RS_k(\boldsymbol{u}, \mathbf{1})$ mit $\boldsymbol{u} = (1, u, \ldots, u^{q-2})$ (vgl. Definition 3.8). Ein primitiver BCH-Code C mit garantierter Minimaldistanz d besitzt die Kontrollmatrix

$$H := \begin{pmatrix} 1 & u & \cdots & u^{q-2} \\ 1 & u^2 & & u^{2(q-2)} \\ \vdots & & & \vdots \\ 1 & u^{d-1} & \cdots & u^{(d-1)(q-2)} \end{pmatrix},$$

die nach Bemerkung 3.10 auch eine Erzeugermatrix des gewöhnlichen Reed-Solomon Code $RS_{d-1}(\boldsymbol{u}, \boldsymbol{u})$ bildet. Aufgrund $\sum_{i=0}^{n-1} u^{ij} = \frac{u^{jn}-1}{u^j-1} = 0$ für $1 \leq j \leq n-1$ gilt $\mathbf{1} \perp RS_{n-1}(\boldsymbol{u}, \boldsymbol{u})$. Es folgt dann nach Satz 3.11

$$C = RS_{d-1}(\boldsymbol{u}, \boldsymbol{u})^{\perp} = RS_{q-d}(\boldsymbol{u}, \mathbf{1}).$$

Insbesondere ist C pseudorational. Umgekehrt ist $RS_k(\boldsymbol{u}, \mathbf{1})$ ein primitiver BCH-Code mit garantierter Minimaldistanz $q-k$.
(b) Allgemein tritt ein BCH-Code C mit garantierter Minimaldistanz d als Teilkörpercode des Reed-Solomon-Code $RS_{d-1}(\boldsymbol{u}, \boldsymbol{b})^{\perp}$ mit $\boldsymbol{u} = (1, u, \ldots, u^{n-1})$ und $\boldsymbol{b} = (1, u^b, \ldots, u^{b(n-1)})$ auf, d.h. es gilt

$$C = RS_{d-1}(\boldsymbol{u}, \boldsymbol{b})^{\perp}|_{\mathbb{F}_q}.$$

Satz 6.19. *Es sei C ein BCH-Code mit garantierter Minimaldistanz d der Länge n. Dann gelten:*

(a) *C besitzt mindestens Dimension $n - m(d-1)$.*

(b) *Im Fall $q = 2$ und $b = 1$ gilt* $\dim(C) \geq n - m \cdot \lfloor \frac{d}{2} \rfloor$.

Beweis. Per Konstruktion besitzt ein BCH-Code C mit garantiertem Minimalabstand d das Erzeugerpolynom

$$g(X) = \mathrm{kgV}\{g_j(X) : u^j \in U_{b,d}\},$$

wobei $g_j(X)$ jeweils das Minimalpolynom über $\mathbb{F}_q$ zu u^j bezeichne. Aufgrund von $[\mathbb{F}_q(u){:}\mathbb{F}_q] = m$ ist der Polynomgrad der $g_j(X)$ nicht größer als m und es folgt

$$\deg(g(X)) \leq m(d-1).$$

Im Fall $q = 2$ stimmen die Minimalpolynome $g_j(X)$ und $g_{2j}(X)$ überein vermöge

$$g_j(u^{2j}) = (g_j(u^j))^2 = 0.$$

Somit hat das Erzeugerpolynom $g(X)$ eines binären BCH-Code C mit $U_{1,d} \subseteq U(C)$ die Gestalt

$$g(X) = \mathrm{kgV}\{g_j(X) : j = 1, 3, \ldots, 2\lfloor \tfrac{d}{2} \rfloor - 1\}$$

und höchstens Grad $m \cdot \lfloor \frac{d}{2} \rfloor$. Die Behauptungen (a) und (b) folgen nun aus

$$\dim(C) = n - \deg(g(X)). \qquad \square$$

Korollar 6.20. *Für $q = 2$, $n = 2^m - 1$ und $t < 2^{m-1}$ existiert ein t-fehlerkorrigierender BCH-Code der Länge n und Dimension $k \geq n - mt$.*

Beweis. Es sei C ein binärer BCH-Code mit $U_{1,2t} \subseteq U(C)$. Aufgrund von $g_t(u^{2t}) = 0$ und $g_t(X) | g(X)$ ist u^{2t} eine weitere Nullstelle von C. Daher gilt sogar $U_{1,2t+1} \subseteq U(C)$ und somit besitzt C die garantierte Minimaldistanz $2t + 1$. $\square$

Satz 6.21. (Symmetriegruppe von BCH-Codes)
Es sei $\hat{C}$ ein durch ein Paritätssymbol erweiterter primitiver BCH-Code über $\mathbb{F}_q$ der Länge q^m. Dann operiert $\mathbf{AGL}_1(\mathbb{F}_{q^m})$ auf $\hat{C}$, d.h. es gilt

$$\mathbf{AGL}_1(\mathbb{F}_{q^m}) \leq \mathrm{Sym}(\hat{C}).$$

Beweis. Wir identifizieren die Positionen $0, 1, \ldots, n = q^m - 1$ von $\mathbb{F}_q^{n+1}$ mit den Elementen von $\mathbb{F}_{q^m} = \{0, 1, u, \ldots, u^{n-1}\}$ via $n \mapsto 0$ und $i \mapsto u^i$. Dann operiert $\mathbf{AGL}_1(\mathbb{F}_{q^m}) = \{\gamma_{a,b} : a \in \mathbb{F}_{q^m}^\times, b \in \mathbb{F}_{q^m}\}$ mit $\gamma_{a,b}(c) = ac + b$ auf $\mathbb{F}_q^{n+1}$ durch Permutation der Einträge vermöge

$$(y_0, y_1, \ldots, y_n)^{\gamma_{a,b}} = (y_{\gamma_{a,b}^{-1}(0)}, \ldots, y_{\gamma_{a,b}^{-1}(n)}).$$

Wegen der Relationen

$$\gamma_{a,b} = \gamma_{1,b}\gamma_{a,0}, \quad \gamma_{1,b} = \gamma_{b,0}\gamma_{1,1}\gamma_{b^{-1},0} \quad \text{sowie} \quad \gamma_{a,0}\gamma_{b,0} = \gamma_{ab,0}$$

wird $\mathbf{AGL}_1(\mathbb{F}_{q^m})$ von $\gamma_{u,0}$ und $\gamma_{1,1}$ erzeugt. Da C zyklisch ist, erfüllen die Codewörter $(x_0, \ldots, x_n)$ von $\hat{C}$

$$(x_0, \ldots, x_n)^{\gamma_{u,0}} = (x_{n-1}, x_0, \ldots, x_{n-2}, x_n) \in \hat{C},$$

d.h. $\hat{C}$ ist invariant unter $\gamma_{u,0}$. Es verbleibt also nur noch der Nachweis von $\gamma_{1,1} \in \mathrm{Sym}(\hat{C})$. Bezeichnet d die garantierte Minimaldistanz des primitiven BCH-Codes C, so sind $u, \ldots, u^{d-1}$ designierte Nullstellen von C. Es ist zu zeigen, daß die $\gamma_{1,1}$–Konjugierten Codewörter $\boldsymbol{x}^{\gamma_{1,1}} = (x_{\gamma_{1,1}^{-1}(0)}, \ldots, x_{\gamma_{1,1}^{-1}(n-1)})$ von C ebenfalls die Nullstellen u^j für $1 \leq j \leq d - 1$ besitzen, daß also

$$\boldsymbol{x}^{\gamma_{1,1}}(u^j) := \sum_{i=0}^{n-1} x_{\gamma_{1,1}^{-1}(i)} u^{ij} = \sum_{i=0}^{n-1} x_{\gamma_{1,-1}(i)} u^{ij} = 0$$

für $\boldsymbol{x} = (x_0, \ldots, x_{n-1}) \in C$ und $x_n := -\sum_{i=0}^{n-1} x_i$ gilt. Unter Beachtung von $u^{\gamma_{1,1}(i)} = u^i + 1$ bei $i \neq n$ erhält man

$$\begin{aligned}\sum_{i=0}^{n-1} x_{\gamma_{1,1}^{-1}(i)} u^{ij} &= \sum_{\substack{0\le i\le n-1\\ u^i\neq -1}} x_i u^{\gamma_{1,1}(i)j} + x_n = \sum_{\substack{0\le i\le n-1\\ u^i\neq -1}} x_i (u^i+1)^j + x_n \\ &= \sum_{i=0}^{n-1} x_i (u^i+1)^j + x_n = \sum_{i=0}^{n-1} x_i \sum_{k=0}^{j} \binom{j}{k} u^{ir} + x_n \\ &= \sum_{k=0}^{j} \binom{j}{k} \boldsymbol{x}(u^k) + x_n = \boldsymbol{x}(u^0) + x_n = \sum_{i=0}^{n} x_i = 0.\end{aligned}$$

Das zeigt die $\gamma_{1,1}-$Invarianz von $\hat{C}$. □

6.4 Decodierung von BCH - Codes

Es sei C ein primitiver BCH-Code über $\mathbb{F}_q$ mit garantierter Minimaldistanz $d = 2e + 1$. Sind $\boldsymbol{x} \in C$ das gesendete und $\boldsymbol{y} \in \mathbb{F}_q^n$ das empfangene Wort, so bezeichnet

$$\boldsymbol{e} := \boldsymbol{y} - \boldsymbol{x}$$

den **Fehlervektor** zwischen $\boldsymbol{x}$ und $\boldsymbol{y}$ und

$$I := \{1 \le i \le n : e_i \neq 0\}$$

die **Indexmenge der Fehlerpositionen in $\boldsymbol{y}$**. Wir nehmen im folgenden stets $\#I \le e$ an. Neben $g(X) := \sum_{i=1}^{n} y_i X^i$ bezeichnen weiter $h(X) := \sum_{i\in I} e_i X^i$ das **Fehlerpolynom**,

$$\sigma(X) := \prod_{i\in I}(1 - u^i X) = \sum_{j=0}^{e} \sigma_j X^j$$

das **fehlerlokalisiernde Polynom zu $\boldsymbol{y}$** sowie

$$\omega(X) := \sum_{i\in I} e_i u^i \prod_{\substack{j\in I\\ j\neq i}} (1 - u^j X)$$

das **Fehlerauswertungspolynom**. Offensichtlich gilt mit unserer Annahme

$$\deg(\omega) < \deg(\sigma) = \#I \le e.$$

Der Quotient aus $\omega(X)$ und $\sigma(X)$ hat die Gestalt

$$\frac{\omega(X)}{\sigma(X)} = \sum_{i\in I} \frac{e_i u^i}{1 - u^i X} = \sum_{i\in I} \frac{e_i}{X} \sum_{j\ge 1} (u^i X)^j = \sum_{j\ge 1} X^{j-1} \sum_{i\in I} e_i u^{ij} = \sum_{j\ge 1} h(u^j) X^{j-1}.$$

Da $u, u^2, \ldots, u^{2e}$ die designierten Nullstellen von C sind, gilt

$$h(u^j) = \sum_{i=1}^{n}(y_i - x_i)u^{ij} = \sum_{i=1}^{n} y_i u^{ij} = g(u^j)$$

für $j = 1, \ldots, 2e$. Somit können wir das **Syndrompolynom**

$$s(X) := \sum_{j=1}^{2e} g(u^j)X^{j-1} \equiv \frac{\omega(X)}{\sigma(X)} \pmod{X^{2e}}$$

leicht aus der empfangenen Nachricht $\boldsymbol{y}$ berechnen, obwohl $\omega(X)$ und $\sigma(X)$ zunächst unbekannt sind. Aus der Kongruenz folgt die Existenz eines Polynoms $u(X) \in \mathbb{F}_q[X]$ mit

$$s(X)\sigma(X) + u(X)X^{2e} = \omega(X).$$

Bemerkung 6.22. *In der obigen Situation gibt es genau ein Paar teilerfremde Polynome $\sigma(X), \omega(X)$ mit $\deg(\omega) < \deg(\sigma) \leq e$ und $\sigma(0) = 1$, welche die Kongruenz*

$$\omega(X) \equiv s(X)\sigma(X) \pmod{X^{2e}}$$

erfüllen.

Beweis. Es ist lediglich die Eindeutigkeit von $\sigma(X)$ und $\omega(X)$ zu zeigen. Aus der Kongruenz

$$\omega(X) \equiv s(X)\sigma(X) = \sum_{k\in\mathbb{N}} \sum_{i+j=k} s_i\sigma_j X^k \pmod{X^{2e}}$$

ergibt sich sich aufgrund von $\deg(\omega) < e$ das lineare Gleichungssystem

$$\sum_{i+j=k} s_i\sigma_j = 0 \qquad \text{für } e \leq k \leq 2e-1 \tag{6.23}$$

in den Unbestimmten σ_j.

1.Schritt: Es sei nun

$$\tilde{\sigma}(X) = \sum_{j=0}^{e} \tilde{\sigma}_j X^i$$

ein Polynom minimalen Grades, dessen Koeffizienten $\tilde{\sigma}_j$ das Gleichungssystem (6.23) erfüllen. Definiert man $\tilde{\sigma}_j := 0$ für alle $j > e$, so gilt

$$\begin{aligned} 0 &= \sum_{j=0}^{k} s_{k-j}\tilde{\sigma}_j = \sum_{j=0}^{k} g(u^{k-j+1})\tilde{\sigma}_j \\ &= \sum_{j=0}^{k}\sum_{i\in I} e_i u^{(k-j+1)i}\tilde{\sigma}_j = \sum_{i\in I} u^{i(k+1)} e_i \tilde{\sigma}(u^{-i}) \qquad \text{für } e \leq k \leq 2e-1. \end{aligned}$$

Dies ist ein lineares Gleichungssystem in den Unbestimmten $e_i\tilde{\sigma}(u^{-i})$ mit Koeffizientenmatrix $A := (u^{i(k+1)})_{i\in I, e\leq k\leq 2e-1}$. Da A Teilmatrix einer Vandermondeschen Matrix ist, folgt hieraus $e_i\tilde{\sigma}(u^{-i}) = 0$ für alle Fehlerpositionen $i \in I$. Dies impliziert $\tilde{\sigma}(u^{-i}) = 0$ für $i \in I$, d.h. das fehlerlokalisierende Polynom $\sigma(X)$ teilt $\tilde{\sigma}(X)$. Wegen der Minimalität von $\deg(\tilde{\sigma})$ und $\tilde{\sigma}(0) = 1 = \sigma(0)$ stimmt $\tilde{\sigma}(X)$ mit $\sigma(X)$ überein.

2.Schritt: Sind nun $\tilde{\sigma}(X)$ und $\tilde{\omega}(X)$ teilerfremde Polynome mit $\deg(\tilde{\omega}) < \deg(\tilde{\sigma}) \leq e$, $\tilde{\sigma}(0) = 1$ und

$$\tilde{\omega} \equiv s(X)\tilde{\sigma}(X) \pmod{X^{2e}},$$

so erfüllen die Koeffizienten von $\tilde{\sigma}(X)$ das Gleichungssystem (6.23). Hieraus folgt wie im 1.Schritt $\sigma(X)|\tilde{\sigma}(X)$, d.h es gibt ein Polynom $f(X) \in \mathbb{F}_q[X]$ mit $\tilde{\sigma}(X) = f(X)\sigma(X)$ und $\deg(f) = \deg(\tilde{\sigma}) - \deg(\sigma) < e$. Es ist dann $\tilde{\omega}(X) - f(X)\omega(X)$ ein Polynom vom Grad $< 2e$, das der Kongruenz

$$\tilde{\omega}(X) - f(X)\omega(X) \equiv \tilde{\omega}(X) - f(X)s(X)\sigma(X) \equiv \tilde{\omega}(X) - s(X)\tilde{\sigma}(X) \equiv 0 \pmod{X^{2e}}$$

genügt. Folglich stimmen $\tilde{\omega}(X)$ und $f(X)\omega(X)$ überein. Da $\tilde{\omega}(X)$ und $\tilde{\sigma} = f(X)\sigma(X)$ teilerfremd sind, ist $f(X)$ ein konstantes Polynom. Aus $\tilde{\sigma}(0) = 1 = \sigma(0)$ folgt schließlich $f(X) = 1$ und somit $\tilde{\sigma}(X) = \sigma(X)$ und $\tilde{\omega}(X) = \omega(X)$. □

Korollar 6.24. *Das fehlerlokalisierende Polynom $\sigma(X)$ und das Fehlerauswertungspolynom $\omega(X)$ sind mit dem Euklidischen Algorithmus berechenbar.*

Beweis. Wendet man den Euklidischen Algorithmus auf $f_0(X) := X^{2e}$ und $f_1(X) := s(X)$ an, so erhält man endliche Folgen von Polynomen $f_i(X), u_i(X)$ und $v_i(X)$ mit

$$\begin{aligned} f_i(X) &= q_{i+1}(X)f_{i+1}(X) + f_{i+2}(X) \\ &= v_i(X)s(X) + u_i(X)X^{2e} \end{aligned}$$

und $\deg(f_i) < \deg(f_{i-1})$. Dabei gilt $\deg(v_i) = 2e - \deg(f_{i-1})$. Dies sieht man induktiv wie folgt: Wegen $v_1(X) = 1$ und $f_0(X) = X^{2e}$ gilt die Behauptung für $i = 1$. Beim Induktionsschritt von i auf $i+1$ sind aufgrund von $v_{i+1}(X) = v_{i-1}(X) - q_i(X)v_i(X)$ und $\deg(q_i) \geq 1$ die Grade der Polynome $v_{i+1}(X)$ und $q_i(X)v_i(X)$ gleich, wovon man sich durch eine seperate Induktion überzeugen kann. Das führt wie gewünscht zu

$$\begin{aligned} \deg(v_{i+1}) &= \deg(q_i) + \deg(v_i) = \deg(q_i) + 2e - \deg(f_{i-1}) \\ &= \deg(q_i) + 2e - \deg(q_i f_i) = 2e - \deg(f_i). \end{aligned}$$

Da $\mathrm{ggT}(X^{2e}, s(X))$ wegen $s(X)\sigma(X) + u(X)X^{2e} = \omega(X)$ ein Teiler von $\omega(X)$ ist, gilt $\deg(\mathrm{ggT}(X^{2e}, s(X))) \leq \deg(\omega) < e$, und es gibt einen Index $k \in \mathbb{N}$ mit

$$0 \leq \deg(f_k) < e \leq \deg(f_{k-1}).$$

Gemäß dem Euklidischen Algorithmus hat $f_k(X)$ die Gestalt

$$f_k(X) = v_k(X)s(X) + u_k(X)X^{2e} \equiv v_k(X)s(X) \pmod{X^{2e}}$$

mit $\deg(v_k) \leq e$. Somit sind

$$\tilde{\omega}(X) := \frac{f_k(X)}{\mathrm{ggT}(f_k, v_k)} \quad \text{und} \quad \tilde{\sigma}(X) := \frac{v_k(X)}{\mathrm{ggT}(f_k, v_k)}$$

teilerfremde Polynome mit $\deg(\tilde{\omega}) < \deg(\tilde{\sigma}) \leq e$, welche die Kongruenz

$$\tilde{\omega}(X) \equiv s(X)\tilde{\sigma}(X) \pmod{X^{2e}}$$

erfüllen. Nach Bemerkung 6.22 gelten dann

$$\omega(X) = \tilde{\sigma}(0)^{-1} \cdot \tilde{\omega}(X) \quad \text{und} \quad \sigma(X) = \tilde{\sigma}(0)^{-1} \cdot \tilde{\sigma}(X).$$

Das beweist unsere Behauptung. □

Notiz 6.25. Gemäß Bemerkung 10.13 gilt sogar $\mathrm{ggT}(f_k, v_k) = 1$.

Decodieralgorithmus 6.26.
Es seien $\boldsymbol{y} \in \mathbb{F}_q^n$ das empfangene Wort sowie $g(X) := \sum_{i=1}^{n} y_i X^i$.

(1) Konstruiere das Syndrompolynom

$$s(X) := \sum_{j=1}^{2e} g(u^j) X^{j-1}.$$

(2) Berechne das fehlerlokalisiernde Polynom $\sigma(X)$ und das Fehlerauswertungspolynom $\omega(X)$ mit dem Euklidischen Algorithmus gemäß Korollar 6.24.

(3) Bestimme die Indexmenge der Fehlerpositionen I über die Nullstellen von $\sigma(X)$.

(4) Berechne den Fehlervektor $\boldsymbol{e} = (e_1, \ldots, e_n)$ mittels $e_i = 0$ für $i \notin I$ und

$$e_i = -\frac{\omega(u^{-i})}{\sigma'(u^{-i})} \qquad \text{für } i \in I.$$

(5) Decodiere $\boldsymbol{y}$ zu $\boldsymbol{x} = \boldsymbol{y} - \boldsymbol{e}$.

Kapitel 7

Quadratische Reste-Codes

7.1 Quadratische Reste-Codes

Definition 7.1. (Quadratischer Reste-Code)
Es seien r eine ungerade Primzahl und

$$Q_r := \{1 \leq i < r : \left(\frac{i}{r}\right) = 1\} \qquad \text{und} \qquad N_r := \{1 \leq i < r : \left(\frac{i}{r}\right) = -1\}$$

die Menge der quadratischen Reste modulo r bzw. die Menge der Nichtquadrate modulo r. Sind dann $p \in Q_r$ eine Primzahl, u eine primitive r-te Einheitswurzel über $\mathbb{F}_p$ sowie

$$q(X) := \prod_{i \in Q_r} (X - u^i) \qquad \text{und} \qquad n(X) := \prod_{i \in N_r} (X - u^i),$$

so heißen die zyklischen Codes

$$\mathcal{Q}_r := \rho^{-1}(q(X)R_r), \qquad \mathcal{N}_r := \rho^{-1}(n(X)R_r),$$
$$\mathcal{Q}_r^* := \rho^{-1}((X-1)q(X)R_r), \qquad \mathcal{N}_r^* := \rho^{-1}((X-1)n(X)R_r)$$

über $\mathbb{F}_p$ **quadratische Reste-Codes** (oder kürzer auch **QR-Codes**).

Anmerkung 7.2. (a) Die quadratischen Reste-Codes sind Codes über $\mathbb{F}_p$. Denn mit u^i ist wegen $\left(\frac{ip}{r}\right) = \left(\frac{i}{r}\right)\left(\frac{p}{r}\right) = \left(\frac{i}{r}\right)$ auch u^{ip} Nullstelle der definierenden Polynome. Daher erfüllen ihre Koeffizienten

$$a_{r-k} = \sum_{i_1 < i_2 < \ldots < i_k} u^{i_1 + \cdots + i_k}$$

die Gleichung $a_{r-k}^p = a_{r-k}$ und sind somit Elemente von $\mathbb{F}_p$.
(b) Gemäß 6.5 beträgt die Dimension der quadratischen Reste-Codes

$$\dim(\mathcal{Q}_r) = \dim(\mathcal{N}_r) = r - \frac{r-1}{2} = \frac{r+1}{2}$$

beziehungsweise

$$\dim(\mathcal{Q}_r^*) = \dim(\mathcal{N}_r^*) = r - \frac{r+1}{2} = \frac{r-1}{2}\ .$$

(c) Die quadratischen Reste-Codes $\mathcal{Q}_r$ und $\mathcal{N}_r$ bzw. $\mathcal{Q}_r^*$ und $\mathcal{N}_r^*$ sind äquivalent vermöge der Symmetrie

$$\pi : f(X) \mapsto f(X^j)$$

für ein Nichtquadrat j modulo r. Als Codewort aus $\mathcal{Q}_r$ ist $f(X)$ durch $q(X)$ teilbar, d.h. es ist $f(u^i) = 0$ für alle Quadrate i modulo r. Für $k \in N_r$ ist kj ein Quadrat und es gilt daher

$$f((u^k)^j) = f(u^{kj}) = 0.$$

Somit ist $f(X^j)$ durch $n(X)$ teilbar. Ist $f(X)$ zusätzlich durch $(X-1)$ teilbar, d.h. ein Wort aus $\mathcal{Q}_r^*$, so gilt $f(1^j) = f(1) = 0$ und somit $\pi(f(X)) \in \mathcal{N}_r^*$.

Beispiel 7.3. Für $r = 7$ ist $Q_7 = \{1, 2, 4\}$. In $\mathbb{F}_2[X]$ gilt

$$X^7 - 1 = (X+1)(X^3 + X + 1)(X^3 + X^2 + 1).$$

Es gibt eine primitive Einheitswurzel $u \in \mathbb{F}_8$ mit Minimalpolynom

$$q(X) = (X-u)(X-u^2)(X-u^4) = X^3 + X + 1.$$

Definitionsgemäß erzeugt $q(X)$ den BCH-Code $\mathcal{Q}_7$ mit garantierter Minimaldistanz 3. Nach Anmerkung 7.2 ist $\mathcal{Q}_7$ also ein $[7, 4, 3]_2-$Code und folglich äquivalent zum Hamming-Code $\mathrm{Ham}[7, 4]_2$ (vergleiche Anmerkung 5.4).

Definition 7.4. (Erweiterter quadratischer Reste-Code)
In der Situation von Definition 7.1 heißt $\gamma := \sum_{i=1}^{r-1} \left(\frac{i}{r}\right) u^i$ die **Gaußsche Summe** von u. Den Code

$$\hat{\mathcal{Q}}_r := \left\{ \left(x_0, \ldots, x_{r-1}, -\frac{\gamma}{r} \sum_{i=0}^{r-1} x_i \right) : (x_0, \ldots, x_{r-1}) \in \mathcal{Q}_r \right\}$$

nennen wir **erweiterter quadratische Reste-Code** (oder auch **EQR-Code**).

Anmerkung 7.5. Im Fall $p = 2$ ist $\hat{\mathcal{Q}}_r$ ein einfacher *Parity-Check-Code* von $\mathcal{Q}_r$ (vgl. Bemerkung 4.1). Denn aufgrund

$$\gamma = \sum_{i=1}^{r-1} \left(\frac{i}{r}\right) u^i \equiv \sum_{i=1}^{r-1} u^i = 1 \equiv r \pmod 2$$

folgt $\frac{\gamma}{r} = 1$ und somit $\sum_{i=0}^{r} x_i = 2 \cdot \sum_{i=0}^{r-1} x_i = 0$ für die Quersumme eines beliebigen Wortes $\boldsymbol{x} \in \hat{\mathcal{Q}}_r$.

Lemma 7.6. *Für die Gaußsche Summe* $\gamma := \sum_{i=1}^{r-1} \left(\frac{i}{r}\right) u^i$ *gilt*

$$\gamma^2 = \left(\frac{-1}{r}\right) r.$$

Beweis. Mit den Umformungen

$$\begin{aligned}\gamma^2 &= \sum_{i=1}^{r-1}\sum_{j=1}^{r-1}\left(\frac{ij}{r}\right)u^{i+j} = \sum_{j=1}^{r-1}\sum_{ij=1}^{r-1}\left(\frac{ij^2}{r}\right)u^{j+ij} = \sum_{i=1}^{r-1}\left(\frac{i}{r}\right)\sum_{j=1}^{r-1}(u^{1+i})^j \\ &= \left(\frac{r-1}{r}\right)\cdot\sum_{j=1}^{r-1}1 \;+\; \sum_{i=1}^{r-2}\left(\frac{i}{r}\right)\cdot\left(\sum_{j=1}^{r-1}u^j\right) \\ &= \left(\frac{-1}{r}\right)(r-1) - \sum_{i=1}^{r-2}\left(\frac{i}{r}\right) = \left(\frac{-1}{r}\right)r - \sum_{i=1}^{r-1}\left(\frac{i}{r}\right)\end{aligned}$$

erhält man die Behauptung. □

7.2 Dualität bei quadratischen Reste-Codes

Satz 7.7. (Dualität bei quadratischen Reste-Codes)
Die quadratischen Reste-Codes erfüllen folgende Dualitätsrelationen:

(a) *Für die quadratischen Reste-Codes* $\mathcal{Q}_r$ *und* $\mathcal{N}_r$ *gelten*

$$\mathcal{Q}_r^\perp = \begin{cases} \mathcal{Q}_r^* & \text{falls } r \equiv 3 \pmod 4 \\ \mathcal{N}_r^* & \text{falls } r \equiv 1 \pmod 4 \end{cases}$$

sowie

$$\mathcal{N}_r^\perp = \begin{cases} \mathcal{N}_r^* & \text{falls } r \equiv 3 \pmod 4 \\ \mathcal{Q}_r^* & \text{falls } r \equiv 1 \pmod 4 \end{cases}$$

(b) *Der erweiterte quadratische Reste-Code* $\hat{\mathcal{Q}}_r$ *ist im Fall* $r \equiv 3 \pmod 4$ *selbstdual.*

Beweis. (a) Nach Korollar 6.13 hat der duale Code $\mathcal{Q}_r^\perp$ die Nullstellenmenge

$$U_r(\mathcal{Q}_r^\perp) = U_r \backslash \{u^{-i} : i \in Q_r\}.$$

Im Fall $r \equiv 3 \pmod 4$ ist -1 ein Nichtquadrat modulo r, und somit besitzt $\mathcal{Q}_r^\perp$ in diesem Fall genau die selben Nullstellen wie $\mathcal{Q}_r^*$. Folglich sind beide Codes identisch. Entsprechend folgt $\mathcal{Q}_r^\perp = \mathcal{N}_r^*$ im Fall $r \equiv 1 \pmod 4$, da hier -1 ein Quadrat modulo r ist. Die Dualitätsrelationen für $\mathcal{N}_r$ enthält man entsprechend.
(b) Die Differenzmenge $\mathcal{Q}_r \backslash \mathcal{Q}_r^*$ enthält aufgrund

$$\sum_{i=0}^{r-1} X^i = \frac{X^r - 1}{X - 1} = n(X) \cdot q(X)$$

das Wort $\mathbf{1} = (1, \ldots, 1)$. Bezeichnet also G_r^* eine Erzeugermatrix zu $\mathcal{Q}_r^*$, so bildet

$$G_r = \begin{pmatrix} & G_r^* & \\ 1 & \cdots & 1 \end{pmatrix}$$

eine Erzeugermatrix zu $\mathcal{Q}_r$. Desweiteren gilt aufgrund Aussage (a)

$$\sum_{i=0}^{r-1} x_i = \langle \mathbf{1}, \boldsymbol{x} \rangle = 0$$

für alle Codewörter $\boldsymbol{x} = (x_0, \ldots, x_{r-1})$ aus $\mathcal{Q}_r^*$. Daher ist

$$\hat{G}_r = \left(\begin{array}{ccc|c} & & & 0 \\ & G_r^* & & \vdots \\ & & & 0 \\ \hline 1 & \cdots & 1 & -\gamma \end{array}\right)$$

eine Generatormatrix zu $\hat{\mathcal{Q}}_r$. Sämtliche Zeilen aus G_r^* bilden Wörter aus $\mathcal{Q}_r^*$ und $\mathcal{Q}_r$, was aufgrund ihrer Dualitätsrelation $G_r^* \cdot (G_r^*)^T = 0$ zur Folge hat. Bezeichnet $\boldsymbol{z} = (1, \ldots, 1, -\gamma)$ die letzte Zeile von $\hat{G}_r$, so gilt

$$\hat{G}_r \cdot \hat{G}_r^T = \left(\begin{array}{ccc|c} & & & 0 \\ & 0 & & \vdots \\ & & & 0 \\ \hline 0 & \cdots & 0 & \langle \boldsymbol{z}, \boldsymbol{z} \rangle \end{array}\right).$$

Die Selbstdualität von $\hat{\mathcal{Q}}_r$ folgt schließlich aus Lemma 7.6 vermöge

$$\langle \boldsymbol{z}, \boldsymbol{z} \rangle = r + \left(\frac{-1}{r}\right) r = r - r = 0. \qquad \square$$

Korollar 7.8. *Im Fall $r \equiv 7 \pmod 8$ ist der binäre EQR-Code $\hat{\mathcal{Q}}_r$ selbstdual und 4-dividierbar (d.h. es ist $w(\boldsymbol{x}) \equiv 0 \pmod 4$ für alle Wörter $\boldsymbol{x} \in \hat{\mathcal{Q}}_r$).*

Beweis. Wir brauchen lediglich zu zeigen, daß $\hat{\mathcal{Q}}_r$ ein 4-dividierbares Erzeugersystem besitzt, denn daraus folgt wie im Beweis zu Satz 5.10 die 4-Dividierbarkeit von $\hat{\mathcal{Q}}_r$. Aufgrund der Gestalt der Erzeugermatrix $\hat{G}_r$ zu $\hat{\mathcal{Q}}_r$ und

$$w((1, \ldots, 1, -\gamma)) = r + 1 \equiv 0 \pmod 4$$

kann man sich auf den Nachweis beschränken, daß $\mathcal{Q}_r^*$ ein 4-dividierbares Erzeugersystem besitzt. Dazu betrachten wir die Polynome

$$e_n(X) = \sum_{i \in N_r} X^i \qquad \text{und} \qquad e_q(X) = \sum_{i \in Q_r} X^i$$

über $\mathbb{F}_2$. Für eine primitve r-te Einheitswurzel u über $\mathbb{F}_2$ gilt

$$1 + e_n(u) + e_q(u) = 0.$$

Aufgrund $\left(\frac{2}{r}\right) = 1$ erfüllt $e_n(u)$ die Gleichung

$$e_n(u)^2 = e_n(u^2) = \sum_{i \in N_r} u^{2i} = e_n(u).$$

Somit sind $e_n(u)$ und $e_q(u)$ Elemente von $\mathbb{F}_2$. Desweiteren gilt $e_n(u^{-1}) = e_q(u)$, da -1 nach Voraussetzung ein Nichtquadrat modulo r ist. Weil auch u^{-1} eine primitive r-te Einheitswurzel ist, können wir somit ohne Einschränkung

$$e_n(u) = 1$$

annehmen. Wir zeigen nun, daß

$$e(X) := 1 + e_n(X)$$

das erzeugende Idempotent zu $\mathcal{Q}_r^*$ bildet. Zunächst ist $e(X)$ aufgrund

$$e_n(X) \cdot e_n(X) = \sum_{i \in N_r} X^{2i} \equiv \sum_{i \in N_r} X^i = e_n(X) \pmod{X^r - 1}$$

ein Idempotent in R_r. Wegen

$$e(1) = 1 + \frac{r-1}{2} = 1 + 1 = 0$$

und

$$e(u^j) = 1 + e_n(u^j) = 1 + \sum_{i \in N_r} u^{ij} = 1 + e_n(u) = 0 \qquad \text{für alle } j \in Q_r$$

ist $e(X)$ auch Element von $\rho(\mathcal{Q}_r^*)$. Dies impliziert $\rho^{-1}(e(X)R_r) \leq \mathcal{Q}_r^*$. Umgekehrt ist jedes Polynom $f(X) \in \rho(\mathcal{Q}_r^*)$ vermöge seiner Nullstellenmenge $\{u^j : j \in Q_r \cup \{0\}\}$ ein Vielfaches von $e(X)$. Das zeigt

$$\mathcal{Q}_r^* = \rho^{-1}(e(X)R_r) = \rho^{-1}(\mathbb{F}_p\langle e(X), e(X) \cdot X, \ldots, e(X) \cdot X^{r-1}\rangle).$$

Insbesondere hat $\mathcal{Q}_r^*$ wegen

$$w(\rho^{-1}(e(X))) = 1 + w(\rho^{-1}(e_n(X))) = 1 + \frac{r-1}{2} = \frac{r+1}{2} \equiv 0 \pmod 4$$

ein 4-dividierbares Erzeugersystem. □

7.3 Symmetrien quadratischer Reste-Codes

Satz 7.9. *Die projektive Gruppe* $\mathbf{PSL}_2(\mathbb{F}_r)$ *operiert treu auf dem erweiterten quadratischen Reste-Code* $\hat{\mathcal{Q}}_r$*. Insbesondere gilt*

$$\mathbf{PSL}_2(\mathbb{F}_r) \leq \mathrm{Sym}(\hat{\mathcal{Q}}_r).$$

Beweis. Wir identifizieren die Indexmenge von $\hat{\mathcal{Q}}_r$ mit $\{0, 1, \ldots, r-1, \infty\} \cong \mathbb{P}^1(\mathbb{F}_r)$, d.h. das Paritätssymbol von $\hat{\mathcal{Q}}_r$ wird mit x_∞ bezeichnet. Es gilt also

$$\hat{\mathcal{Q}}_r = \{(x_0, x_1, \ldots, x_{r-1}, x_\infty) : (x_0, \ldots, x_{r-1}) \in \mathcal{Q}_r\}.$$

Die Gruppe $\mathbf{PSL}_2(\mathbb{F}_r)$ wird erzeugt von den Automorphismen

$$\sigma : \left\{ \begin{array}{ccc} \mathbb{P}^1(\mathbb{F}_r) & \longrightarrow & \mathbb{P}^1(\mathbb{F}_r) \\ a & \longmapsto & a+1 \end{array} \right.$$

und

$$\tau : \left\{ \begin{array}{ccc} \mathbb{P}^1(\mathbb{F}_r) & \longrightarrow & \mathbb{P}^1(\mathbb{F}_r) \\ a & \longmapsto & -a^{-1}. \end{array} \right.$$

Die Abbildung σ induziert die Verschiebung

$$\hat{\sigma} : (x_0, \ldots, x_{r-1}, x_\infty) \mapsto (x_{r-1}, x_0, \ldots, x_{r-2}, x_\infty),$$

d.h. $\hat{\sigma}$ vertauscht die Symbole $x_0, \ldots, x_{r-1}$ zyklisch und läßt x_∞ invariant. Da $\mathcal{Q}_r$ ein zyklischer Code ist, bildet $\hat{\sigma}$ tatsächlich eine Symmetrie von $\hat{\mathcal{Q}}_r$. Die Abbildung τ induziert die Symmetrie

$$\hat{\tau} : (x_0, \ldots, x_{r-1}, x_\infty) \mapsto (\left(\tfrac{-1}{r}\right) x_\infty, y_1, \ldots, y_{r-1}, x_0)$$

mit

$$y_i = \left(\tfrac{-i^{-1}}{r}\right) x_{-i^{-1}} \qquad \text{für } 1 \leq i \leq r-1.$$

Der Nachweis, dass $\hat{\tau}$ tatsächlich eine Symmetrie von $\hat{\mathcal{Q}}_r$ ist, kann in [Wil99, Lemma 6.3.9] nachgelesen werden. Das erklärt die Operation von $\mathbf{PSL}_2(\mathbb{F}_r)$ auf $\hat{\mathcal{Q}}_r$. Diese ist offensichtlich treu und wir erhalten unsere Behauptung. □

Zusatz 7.10. (Assmus, Mattsen 1972 - Symmetriegruppen der EQR-Codes)
Für den EQR-Code $\hat{\mathcal{Q}}_r$ *gilt*

$$\mathrm{Sym}(\hat{\mathcal{Q}}_r) \cong \mathbf{PSL}_2(\mathbb{F}_r)$$

mit Ausnahme der Fälle

$$\mathrm{Sym}(\hat{\mathcal{Q}}_r) \cong \left\{ \begin{array}{ccc} \mathbf{AGL}_3(\mathbb{F}_2) & \textit{bei } (p,r) = (2,3) & (\hat{\mathcal{Q}}_7 \cong \mathrm{Ham}[7,4]_2) \\ \mathbf{M}_{12} & \textit{bei } (p,r) = (3,11) & (\hat{\mathcal{Q}}_{11} \cong \mathrm{Gol}_{12}) \\ \mathbf{M}_{24} & \textit{bei } (p,r) = (2,23) & (\hat{\mathcal{Q}}_{23} \cong \mathrm{Gol}_{24}) \end{array} \right.$$

Ohne Beweis. (siehe [KS80])

Satz 7.11. (Quadratwurzelschranke)
Für die Distanz d eines quadratischen Reste-Codes $\mathcal{Q}_r$ über $\mathbb{F}_p$ gilt die Ungleichung $d^2 > r$. Im Fall $r \equiv 3 \pmod 4$ erfüllt d sogar die Relation $d^2 - d + 1 \geq r$.

Beweis. Es sei $\boldsymbol{x} = (x_0, \ldots, x_{r-1})$ ein Codewort des QR-Codes $\mathcal{Q}_r$ von minimalem Gewicht $w(\boldsymbol{x}) = d$ und

$$f(X) = \sum_{i=0}^{r-1} x_i X^i$$

das zugehörige Polynom.

Wir nehmen an, es gelte $f(1) = 0$, d.h. $\boldsymbol{x}$ ist Element von $\mathcal{Q}_r^*$. Das Wort $(\boldsymbol{x}, 0)$ ist dann in $\hat{\mathcal{Q}}_r$ enthalten. Im Fall $r \equiv 3 \pmod 4$ folgt dies aus dem Beweis zu Satz 7.7 und im Fall $r \equiv 1 \pmod 4$ folgt dies aus $\mathcal{Q}_r^* \perp \mathcal{N}_r$ und $\mathbf{1} \in \mathcal{N}_r$. Da die Symmetriegruppe von $\hat{\mathcal{Q}}_r$ transitiv ist, entsteht $\mathcal{Q}_r$ durch Entfernen eines beliebigen Symbols in $\hat{\mathcal{Q}}_r$. Streichen wir also ein nichttriviales Symbol von $(\boldsymbol{x}, 0)$, so erhalten wir ein Wort in $\mathcal{Q}_r$ mit Gewicht $w(\boldsymbol{x}) - 1$. Dies steht im Widerspruch zur Wahl von $\boldsymbol{x}$. Also gilt $f(1) \neq 0$.

Für ein Nichtquadrat $j \in N_r$ ist $f(X^j)$ ein Vielfaches von $n(X)$. Das Produkt $f(X) \cdot f(X^j)$ ist also durch

$$q(X) \cdot n(X) = 1 + \cdots + X^{r-1}$$

teilbar, nicht aber durch $(X - 1)$. Daher ist $f(X) \cdot f(X^j) \neq 0$ und besitzt höchstens $w(\boldsymbol{x})^2 = d^2$ nichtverschwindende Koeffizienten. Das zeigt $d^2 \geq r$. Im Fall $r \equiv 3 \pmod 4$ nutzen wir aus, daß -1 ein Nichtquadrat ist. Es gilt dann entsprechend

$$0 \neq f(X) \cdot f(X^{-1}) = \sum_{i=0}^{r-1} \sum_{l=0}^{r-1} x_i x_l X^{i-l}.$$

Da der Absolutkoeffizient aus d Summanden $x_i x_l$ besteht, besitzt dieses Wort höchstens das Gewicht $d^2 - (d - 1)$. Das beweist unsere Behauptung. □

Beispiel 7.12. (1) Es sei $(r, p) = (23, 2)$. Die quadratischen Reste modulo 23 sind

$$Q_{23} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}.$$

Für eine passende primitive 23-te Einheitswurzel u ist

$$q(X) = \prod_{i \in Q_{23}} (X - u^i) = X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1$$

das Minimalpolynom über $\mathbb{F}_2$. Der korrespondierende $[23, 12]_2$-QR-Code $\mathcal{Q}_{23}$ besitzt gemäß der Quadratwurzelschranke wenigstens die Minimaldistanz 6. Der EQR-Code $\hat{\mathcal{Q}}_{23}$ ist 4-dividierbar nach Korollar 7.8. Also gilt $d(\hat{\mathcal{Q}}_{23}) \geq 8$, und $\hat{\mathcal{Q}}_{23}$ ist nach Satz 5.18 äquivalent zu Gol_{24}. Da $\hat{\mathcal{Q}}_{23}$ aus $\mathcal{Q}_{23}$ durch Erweiterung mit einem Paritätsbit

entsteht, ergibt sich $d(\mathcal{Q}_{23}) = 7$, und $\mathcal{Q}_{23}$ ist äquivalent zu Gol_{23} (vgl. Abschnitte 5.2-5.3).
(2) Gemäß der Quadratwurzelschranke besitzen die ternären Codes $\mathcal{Q}_{11}$ und $\hat{\mathcal{Q}}_{11}$ wenigstens die Minimaldistanz 4. Analog zeigt man unter Verwendung von Satz 5.21, daß $\hat{\mathcal{Q}}_{11}$ als 3-dividierbarer $[12, 6]_3$-Code mit $d(\hat{\mathcal{Q}}_{11}) \geq 4$ äquivalent zu Gol_{12} und somit $\mathcal{Q}_{11} \sim \mathrm{Gol}_{11}$ ist.

Kapitel 8

Gruppen-Codes

8.1 Codes und Gruppenalgebren

Konvention. Für eine endliche Permutationsgruppe $G \leq \mathbf{S}_n$ von n Elementen und einen (beliebigen) Körper K bildet

$$K[G] := \bigoplus_{\sigma \in G} K\sigma = \left\{ \sum_{\sigma \in G} a_\sigma \sigma : a_\sigma \in K \right\}$$

die sogenannte **Gruppenalgebra** mit der Multiplikation

$$\left(\sum_{\sigma \in G} a_\sigma \sigma \right) \cdot \left(\sum_{\tau \in G} b_\tau \tau \right) = \sum_{\sigma, \tau \in G} a_\sigma b_\tau \sigma\tau = \sum_{\rho \in G} \left(\sum_{\sigma \cdot \tau = \rho} a_\sigma b_\tau \right) \rho.$$

$K[G]$ ist eine $K-$Algebra der Dimension $\#G$ mit Einselement id. Die bijektive Abbildung

$$^- : \left\{ \begin{array}{ccc} K[G] & \longrightarrow & K[G] \\ \sum_{\sigma \in G} a_\sigma \sigma & \longmapsto & \sum_{\sigma \in G} a_\sigma \sigma^{-1} \end{array} \right.$$

ist ein Anti-Automorphismus von $K[G]$ vermöge

$$\overline{\alpha \cdot \beta} = \sum_{\sigma, \tau \in G} a_\sigma b_\tau (\sigma\tau)^{-1} = \sum_{\sigma, \tau \in G} b_\tau a_\sigma \tau^{-1} \sigma^{-1} = \overline{\beta} \cdot \overline{\alpha}$$

für $\alpha = \sum_{\sigma \in G} a_\sigma \sigma$ und $\beta = \sum_{\tau \in G} b_\tau \tau$. Ist A eine Teilmenge von $K[G]$, so bezeichne

$$L(A) := \{ \gamma \in K[G] : \gamma \cdot \alpha = 0 \text{ für alle } \alpha \in A \}$$

den **Linksannulator** von A. Man beachte, daß $L(A)$ ein Linksideal in $K[G]$ ist, d.h. es gelten $L(A) + L(A) = L(A)$ und $K[G] \cdot L(A) = L(A)$.

Anmerkung 8.1. Es sei $G \leq \mathbf{S}_n$ eine reguläre Gruppe, d.h. G ist transitiv und $\sigma(1) = 1$ ist nur für $\sigma = \mathrm{id}$ möglich. Dann bilden die Gruppenelemente $\sigma_1, \sigma_2, \ldots, \sigma_n$ mit $\sigma_i(1) = i$ die gesamte Gruppe G, da $\sigma^{-1}\sigma_j(1) = \sigma^{-1}(j) = 1$ für jedes $\sigma \in \mathbf{S}_n$ mit $\sigma(1) = j$ gilt. Für eine reguläre Gruppe $G = \{\sigma_1, \ldots, \sigma_n\}$ erhalten wir also einen $K-$Vektorraum-Isomorphismus

$$\lambda_G : \begin{cases} K^n & \longrightarrow & K[G] \\ (x_1, \ldots, x_n) & \longmapsto & \sum_{i=1}^n x_i \sigma_i^{-1}. \end{cases}$$

Definition 8.2. (Gruppen-Code)
Ein linearer Code $C \leq \mathbb{F}_q^n$ heißt **Gruppen-Code**, falls es eine reguläre Permuationsgruppe G von n Elementen gibt, sodaß $\lambda_G(C)$ ein Rechtsideal in $\mathbb{F}_q[G]$ bildet. Wir nennen C dann auch $G-$**Gruppen-Code**.

Bemerkung 8.3. (Symmetrien von Gruppen-Codes)
Die Gruppe G operiert treu auf einen $G-$Gruppen-Code, d.h. für einen $G-$Gruppen-Code C gilt

$$G \leq \mathrm{Sym}(C).$$

Beweis. Es seien $C \leq \mathbb{F}_q^n$ ein $G-$Gruppen-Code und $\sigma \in G$. Für $\boldsymbol{x} = (x_1, \ldots, x_n)$ definieren wir $\boldsymbol{x}^\sigma := (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. Weil $\lambda_G(C)$ ein Rechtsideal in $\mathbb{F}_q[G]$ ist, gilt

$$\lambda_G(\boldsymbol{x}^\sigma) = \sum_{i=1}^n x_{\sigma(i)}\sigma_i^{-1} = \sum_{i=1}^n x_i \sigma_i^{-1}\sigma = \lambda_G(\boldsymbol{x}) \cdot \sigma \in \lambda_G(C)$$

für alle Codewörter $\boldsymbol{x} \in C$. Somit ist mit $\boldsymbol{x}$ auch stets $\boldsymbol{x}^\sigma$ Element von C. Das hat $\sigma \in \mathrm{Sym}(C)$ zur Folge, was unsere Behauptung beweist. □

Beispiel 8.4. (Zyklische Codes als Gruppen-Codes)
Es seien $\sigma = (n\ n-1\ \cdots\ 1)$ die zyklische Verschiebung aller n Elemente auf ihren Vorgänger, $G := \langle\sigma\rangle = \mathbf{Z}_n$ sowie $C \leq \mathbb{F}_q^n$ ein zyklischer Code. Definitionsgemäß ist mit $\boldsymbol{x}$ stets auch $\boldsymbol{x}^\sigma$ ein Codewort von C. Es gilt somit

$$\lambda_G(\boldsymbol{x}) \cdot \sigma = \left(\sum_{i=1}^n x_i \sigma^{1-i}\right) \cdot \sigma = \sum_{i=1}^n x_{\sigma(i)}\sigma^{1-i} = \lambda(\boldsymbol{x}^\sigma) \in \lambda_G(C).$$

Daraus folgt insbesondere $\lambda_G(C) \cdot \sigma^i = \lambda_G(C)$ für $i = 1, \ldots, n$. Also ist $\lambda_G(C)$ ein Rechtsideal in $\mathbb{F}_q[G]$ und C ein $G-$ bzw. $\mathbf{Z}_n-$Gruppencode.

Das kanonische Skalarprodukt von K^n läßt sich auf $K[G]$ übertragen vermöge

$$< \textstyle\sum_{\sigma\in G} a_\sigma \sigma, \sum_{\tau\in G} b_\tau \tau > = \ \sum_{\sigma\in G} a_\sigma b_\sigma.$$

Dementsprechend ist

$$A^\perp := \{\beta \in K[G] : < \alpha, \beta > = \ 0 \ \text{ für alle } \alpha \in I\}$$

für jedes Links- bzw. Rechts-Ideal $A \trianglelefteq K[G]$ definiert.

Satz 8.5. (Dualität in $K[G]$)
Für ein Rechtsideal $A \trianglelefteq K[G]$ gilt

$$A^{\perp} = \overline{L(A)}.$$

Insbesondere ist auch $A^{\perp}$ ein Rechtsideal in $K[G]$.

Beweis. Es seien $\alpha = \sum_{\tau \in G} a_\tau \tau \in A$ und $\beta = \sum_{\sigma \in G} b_\sigma \sigma \in \overline{L(A)}$. Dann gilt

$$0 = \overline{\beta} \cdot \alpha = \sum_{\sigma,\tau \in G} b_\sigma a_\tau \sigma^{-1}\tau = \sum_{\tau \in G} \left(\sum_{\sigma \in G} b_\sigma a_{\sigma\tau} \right) \tau.$$

Folglich ist β genau dann Element von $\overline{L(A)}$, wenn

$$< \beta, \alpha\tau^{-1} > = \sum_{\sigma \in G} b_\sigma a_{\sigma\tau} = 0$$

für alle $\alpha \in A$ und $\tau \in G$ gilt. Da A ein Rechtsideal ist, ist diese Bedingung gleichbedeutend mit $\beta \in A^{\perp}$. Das zeigt $A^{\perp} = \overline{L(A)}$. Weil $^{-}$ Linksideale auf Rechtsideale abbildet, ist $\overline{L(A)}$ und somit $A^{\perp}$ ebenfalls ein Rechtsideal. □

Verwendet man $A = \lambda_G(C)$ für einen $G-$Gruppen-Code C, so erhält man aus Satz 8.5 das

Korollar 8.6. *Die Klasse der $G-$Gruppen-Codes ist abgeschlossen bezüglich der Dualisierung.* □

8.2 Gruppenalgebren zu elementarabelschen Gruppen

Der Schnitt aller maximalen Rechtsideale in $K[G]$ heißt **Jacobson-Radikal** von $K[G]$:

$$\mathrm{Rad}(K[G]) := \bigcap_{\substack{A \trianglelefteq K[G] \\ A \text{ max. Rechtsideal}}} A.$$

Anmerkung 8.7. $\mathrm{Rad}(K[G])$ umfaßt sämtliche nilpotenten Rechtsideale I in $K[G]$. Ist nämlich $I^n = 0$ und $A \trianglelefteq K[G]$ ein maximales Rechtsideal, so ist $K[G]/A \cdot I$ als Untermodul eines einfachen Moduls entweder trivial oder ganz $K[G]/A$. Letzteres führte aber wegen

$$K[G]/A = K[G]/A \cdot I = K[G]/A \cdot I^n = 0$$

zum Widerspruch. Somit gelten $K[G]/A \cdot I = 0$ und $I \leq A$ für alle maximalen Rechtsideale A und nilpotenten Rechtsideale I in $K[G]$.

Bemerkung 8.8. (Jacobson-Radikale von $p-$Gruppenalgebren)
Für eine Primzahl p seien G eine endliche $p-$Gruppe und K ein Körper der Charakteristik p. Dann ist

$$J := \bigoplus_{\substack{\sigma\in G\\ \sigma\neq 1}} K(1-\sigma).$$

ist das einzige maximale Rechtsideal der Gruppenalgebra $K[G]$. Insbesondere gilt $\mathrm{Rad}(K[G]) = J$.

Beweis. Wegen $(1-\sigma)\tau = (1-\sigma\tau) - (1-\tau)$ und $\dim_K(\lambda_G^{-1}(J)) = n-1$ ist

$$J = \bigoplus_{\substack{\sigma\in G\\ \sigma\neq 1}} K(1-\sigma) = \left\{ \sum_{\sigma\in G} a_\sigma\sigma \in K[G] : \sum_{\sigma\in G} a_\sigma = 0 \right\} = \left(K\left(\Sigma_{\sigma\in G}\,\sigma\right)\right)^{\perp}$$

tatsächlich ein maximales Rechtsideal in $K[G]$. Wir zeigen nun per Induktion nach $\#G$, daß J das einzige maximale Rechtsideal in $K[G]$ ist.

Für $\#G = 1$ ist nichts zu zeigen, da in diesem Fall (0) das maximale Ideal von $K[G] = K$ ist. Im Fall $\#G > 1$ besitzt G als $p-$Gruppe eine zentrale Untergruppe U der Ordnung p. Es sei ρ der Erzeuger von U, d.h. es gelte $U = \langle\rho\rangle$ mit $\rho^p = 1$. Zudem seien $\sigma_1, \ldots, \sigma_n \in G$ so gewählt, daß

$$G = \dot{\bigcup_{1\le j\le n}} U\sigma_j$$

eine $U-$Nebenklassenzerlegung von G ist. Wir betrachten nun den kanonischen Epimorphismus

$$\psi : \left\{ \begin{array}{ccc} K[G] & \longrightarrow\!\!\!\!\rightarrow & K[G/U] \\ \sum_{\sigma\in G} a_\sigma\sigma & \longmapsto & \sum_{\sigma\in G} a_\sigma\sigma U. \end{array} \right.$$

Wegen $\psi(\rho-1) = \rho U - U = 0$ liegt $(\rho-1)K[G]$ im Kern von ψ. Ist andererseits $\alpha = \sum_{j=1}^{n}\sum_{i=0}^{p-1} a_{ij}\rho^i\sigma_j$ ein Element von $\mathrm{Kern}(\psi)$, so gilt

$$0 = \psi(\alpha) = \sum_{j=1}^{n}\sum_{i=0}^{p-1} a_{ij}\rho^i\sigma_j U = \sum_{j=1}^{n}\sum_{i=0}^{p-1} a_{ij}\sigma_j$$

und daher $\sum_{i=1}^{p-1} a_{ij} = 0$ für alle $j = 1, \ldots, n$. Somit erhalten wir

$$\alpha = \sum_{i=1}^{p-1}\sum_{j=1}^{n} a_{ij}(\rho^i - 1)\sigma_j = (\rho-1)\sum_{i=1}^{p-1}\sum_{j=1}^{n} a_{ij}(\rho^{i-1} + \cdots + 1)\sigma_j \in (\rho-1)K[G],$$

was $\mathrm{Kern}(\psi) = (\rho-1)K[G]$ zur Folge hat. Wegen $(\rho-1)^p = 0$ ist $\mathrm{Kern}(\psi)$ nilpotent und daher nach Anmerkung 8.7 im Jacobson-Radikal $\mathrm{Rad}(K[G])$ enthalten. Gemäß der Induktionsannahme besitzt

$$K[G/U] = K[G]/\,\mathrm{Kern}(\psi)$$

lediglich ein maximales Rechtsideal. Da aber $\mathrm{Kern}(\psi)$ in jedem maximalen Rechtsideal von $K[G]$ enthalten ist, gibt es auch nur ein maximales Rechtsideal in $K[G]$. Das schließt den Induktionsbeweis. □

Korollar 8.9. *Es seien $G = \mathbf{Z}_p^m$ eine elementarabelsche Gruppe und K ein Körper der Charakteristik p. Dann ist $J := \mathrm{Rad}(K[G])$ nilpotent und es gilt*

$$K[G] = J^0 \supsetneqq J \supsetneqq J^2 \supsetneqq \cdots \supsetneqq J^{m(p-1)} \supsetneqq J^{m(p-1)+1} = 0.$$

Beweis. Es seien $\sigma_1, \ldots, \sigma_m$ die Erzeuger von $G = \mathbf{Z}_p^m$. Das Ideal $J^{m(p-1)}$ ist aufgrund von

$$0 \neq \sum_{\sigma \in G} \sigma = \prod_{i=1}^{m} \left(\sum_{j=0}^{p-1} \sigma_i^j \right) = \prod_{i=1}^{m} (\sigma_i - 1)^{p-1} \in J^{m(p-1)}$$

nicht trivial. Für alle natürlichen Zahlen $b_1, \ldots, b_m$ mit $\sum_{i=1}^m b_i > m(p-1)$ gilt wegen $(\sigma_i - 1)^p = 0$ stets

$$\prod_{i=1}^{m} (\sigma_i - 1)^{b_i} = 0,$$

d.h. $J^{m(p-1)+1}$ ist das Nullideal. □

Aufgabe 8.10. Zeigen Sie, daß $K(\sum_{\sigma \in G} \sigma)$ für elementarabelsche Gruppen G das einzige minimale Rechtsideal von $K[G]$ ist.

Bemerkung 8.11. (Jennings-Basis)
Es seien $G = \mathbf{Z}_p^m = \langle \sigma_1, \ldots, \sigma_m \rangle$ eine elementarabelsche Gruppe, K ein Körper der Charakteristik p und $J = \mathrm{Rad}(K[G])$ das Jacobson-Radikal von $K[G]$. Desweiteren seien

$$\xi_j := \sigma_j - 1 \qquad \text{für } j = 1, \ldots, m.$$

Dann gelten für alle natürlichen Zahlen l mit $0 \leq l \leq m$:

(a) *Die Idealpotenz J^l besitzt die $K-$Basis*

$$B_l := \left\{ \prod_{j=1}^{m} \xi_j^{b_j} \quad : \quad 0 \leq b_j < p, \sum_{j=1}^{m} b_j \geq l \right\}.$$

(b) *Die Dimension des Quotienten J^l/J^{l+1} beträgt*

$$\dim_K(J^l/J^{l+1}) = \sum_{k=0}^{m} (-1)^k \binom{m}{k} \binom{l - kp + m - 1}{m - 1}.$$

Beweis. (a) Nach Bemerkung 8.8 (a) wird J von den $K-$Linearkombinationen der Elemente aus B_1 erzeugt. Daher ist B_l aufgrund von $B_l = B_1^l$ zumindest ein Erzeugendensystem von J^l. Es bleibt also nur zu zeigen, daß B_l als solches minimal ist. Dazu nehmen wir an, es gäbe eine nichttriviale Linearkombination

$$0 = \sum_{\beta \in B_l} c_\beta \beta.$$

Unter den $\beta = \sum_{j=1}^m \xi_j^{b_j}$ aus dem Träger dieser Linearkombination wählen wir eines vom minimalem Grad $\sum_{j=1}^m b_j$, d.h. für jedes $\tilde{\beta} = \sum_{j=1}^m \xi_j^{\tilde{b}_j}$ mit $c_{\tilde{\beta}} \neq 0$ gibt einen Index j mit $\tilde{b}_j > b_j$. Somit sind alle $\tilde{\beta} \neq \beta$ aus dem Träger im Linkssannulator von

$$\alpha := \prod_{j=1}^m \xi_j^{p-1-b_j}$$

enthalten. Dies führt zu

$$0 = \left(\sum_{\tilde{\beta} \in B_l} c_{\tilde{\beta}} \tilde{\beta} \right) \cdot \alpha = \sum_{\tilde{\beta} \in B_l} c_{\tilde{\beta}} \tilde{\beta} \alpha = c_\beta \cdot \beta \cdot \alpha,$$

im Widerspruch zu

$$\beta \cdot \alpha = \prod_{j=1}^m \xi_j^{p-1} = \prod_{j=1}^m \sum_{i=0}^{p-1} \sigma_i^j = \sum_{\sigma \in G} \sigma \neq 0.$$

Somit ist B_l eine $K-$Basis von J^l.
(b) Für $0 \leq l \leq m(p-1)$ setzen wir

$$N := \left\{ (b_1, \ldots, b_m) \in \mathbb{N}^m : 0 \leq b_i < p, \sum_{i=1}^m b_i = l \right\},$$

$$M := \left\{ (b_1, \ldots, b_m) \in \mathbb{N}^m : \sum_{i=1}^m b_i = l \right\}$$

sowie

$$M_j := \{ (b_1, \ldots, b_m) \in M : b_j \geq p \}.$$

Die Dimension des Quotienten J^l / J^{l+1} ist dann gleich der Elementanzahl von

$$N = M \backslash \bigcup_{j=1}^m M_j.$$

Dabei gelten

$$\#M = \binom{l+m-1}{l} = \binom{l+m-1}{m-1}.$$

und nach Inklusions-Exklusions-Prinzip

$$\begin{aligned}\#\bigcup_{j=1}^{m} M_j &= \sum_{k=1}^{m}(-1)^{k-1} \sum_{1\le j_1<\ldots<j_k\le m} \#(M_{j_1}\cap\ldots\cap M_{j_k}) \\ &= \sum_{k=1}^{m}(-1)^{k-1} \quad \binom{m}{k} \quad \binom{l-kp+m-1}{l-kp} \\ &= \sum_{k=1}^{m}(-1)^{k-1} \quad \binom{m}{k} \quad \binom{l-kp+m-1}{m-1}.\end{aligned}$$

Hierzu kann man sich beispielsweise M bzw. $M_{j_1}\cap\ldots\cap M_{j_k}$ als Ergebnismenge von l bzw. $l-kp$ Ziehungen mit Zurücklegen aus einem Lostopf mit m Kugeln vorstellen (vgl. z.B. [Kre02, §1.2]). Es folgt schließlich

$$\dim_K(J^l/J^{l+1}) = \#M - \#\bigcup_{j=1}^{m} M_j = \sum_{k=0}^{m}(-1)^k \binom{m}{k}\binom{l-kp+m-1}{m-1}. \qquad \square$$

Korollar 8.12. *Für $0 \le l \le m(p-1)$ gilt*

$$\dim(J^l/J^{l+1}) = \dim(J^{m(p-1)-l}/J^{m(p-1)-l+1}).$$

Beweis. Sind $n_l \in \mathbb{Z}$ die Koeffizienten von

$$(1+X+\cdots+X^{p-1})^m = \sum_{l=0}^{m(p-1)} n_l X^l \in \mathbb{Z}[X],$$

so gilt offensichtlich $n_l = n_{m(p-1)-l}$. Aus

$$n_l = \#\{(b_1,\ldots,b_m)\in\mathbb{N}^m : 0\le b_i<p, \textstyle\sum_{i=1}^m b_i = l\} = \dim(J^l/J^{l+1})$$

folgt unsere Behauptung. $\square$

8.3 Reed-Muller-Codes

Definition 8.13. (Reed-Muller-Code)
Für eine Primzahl p seien $G = \mathbf{Z}_p^m$ eine elementarabelsche Gruppe vom Rang m, $K = \mathbb{F}_p$ ein Primkörper und $J = \mathrm{Rad}(K[G])$ das Jacobson-Radikal der Gruppenalgebra $K[G]$. Dann heißt

$$\mathrm{RM}(r,m) := J^{m(p-1)-r} \trianglelefteq K[G] \qquad \text{für } -1 \le r \le m(p-1)$$

Reed-Muller-Code der Ordnung r. Reed-Muller-Codes $\mathrm{RM}(r,m)$ über $\mathbb{F}_q$ besitzen die Länge p^m. Für $r=-1$ ist $\mathrm{RM}(-1,m) = \{0\}$ der Nullcode.

Beispiel 8.14. (Zyklische Reed-Muller-Codes)
Wir wollen zeigen, daß die Reed-Muller-Codes $\mathrm{RM}(r,1)$ zyklisch und pseudorational der Länge p sind. Die Zyklizität folgt aus $G = \mathbf{Z}_p = \langle\sigma\rangle$. Das Jacobson-Radikal zu $K[G]$ ist

$$J = \mathrm{Rad}(K[G]) = (\sigma - 1)K[G].$$

Daher haben die Reed-Muller-Codes der Ordnung $p-1-l$ die Gestalt

$$\mathrm{RM}(p-1-l,1) = J^l = (\sigma-1)^l K[G].$$

Nach Korollar 8.9 beträgt ihre Dimension jeweils

$$\dim(\mathrm{RM}(p-1-l,1)) = \dim(J^l) = p - l = n - l.$$

Für unsere Behauptung bleibt somit nur noch $d(J^l) = l+1$ zu zeigen. Dazu reicht es $w(\alpha) \geq l+1$ für alle $\alpha = (\sigma-1)^l\beta = \sum_{i=0}^{p-1} a_i\sigma^i$ mit $\beta \in K[G]$ und $a_0 \neq 0$ nachzuweisen. (Für beliebige $\alpha \in J^l\backslash\{0\}$ folgt die Aussage dann vermöge $w(\alpha) = w(\alpha\tau)$ durch Multiplikation mit geeignetem $\tau \in G$.)
Wir führen eine Induktion nach l durch. Für $l = 0$ ist $\mathrm{RM}(p-1,1) = K[G]$ via λ_G isomorph zu $\mathbb{F}_p^p$ und somit pseudorational. Es sei nun $l > 0$ und es gelte $d(J^k) = k+1$ für alle $k < l$. Da J nilpotent ist, ist α als Element von $J\backslash\{0\}$ nicht in K enthalten. Wir erklären nun eine formale Ableitung auf $K[G]$. Die $K-$Algebren $K[G]$ und $K[X]/(X^p-1)$ sind isomorph vermöge der Abbildung

$$\theta : \begin{cases} K[X]/(X^p-1) & \longrightarrow & K[G] \\ g(X) \mod (X^p-1) & \longmapsto & g(\sigma). \end{cases}$$

Auf $K[X]/(X^p-1)$ ist die formale Ableitung

$$\partial : \begin{cases} K[X]/(X^p-1) & \longrightarrow & K[X]/(X^p-1) \\ \sum_{i=0}^{p-1} f_i X^i \mod (X^p-1) & \longmapsto & \sum_{i=0}^{p-1} i\cdot f_i X^{i-1} \mod (X^p-1) \end{cases}$$

wegen $\partial(X^p-1) = 0$ wohldefiniert. Somit ist die mittels θ auf $K[G]$ übertragene formale Ableitung $\partial_\theta = \theta\circ\partial\circ\theta^{-1}$ ebenfalls wohldefiniert und erfüllt die für Ableitungen bekannte Produktregel. Für die formale Ableitung von α gilt also

$$0 \neq \partial_\theta(\alpha) = (\sigma-1)^{l-1}(l\beta + (\sigma-1)\partial_\theta(\beta)).$$

Als Element von J^{l-1} besitzt $\partial_\theta(\alpha)$ nach Induktionsannahme wenigstens das Gewicht l. Da wir aber $a_1 \neq 0$ vorausgesetzt haben, folgt hieraus $w(\alpha) = w(\partial_\theta(\alpha))+1 \geq l+1$.

Bemerkung 8.15. *Es seien $G = \mathbf{Z}_p^m = \langle\sigma_1,\ldots,\sigma_m\rangle$, N ein Teilmenge von $\{(b_1,\ldots,b_m) \in \mathbb{N}^m : b_1,\ldots,b_m < p\}$ und $B = \{\prod_{j=1}^m \xi_j^{b_j} : \boldsymbol{b} \in N\}$ mit $\xi_j = \sigma_j - 1$. Dann besitzt der von B erzeugte Gruppen-Code die Distanz*

$$d(\mathbb{F}_p\langle B\rangle) = \min\left\{\prod_{j=1}^m (b_j+1) : \boldsymbol{b} \in N\right\}.$$

Beweis. Wir beweisen diese Bemerkung durch Induktion nach m. Für $m = 1$ entnehmen wir die Aussage dem obigen Beispiel 8.14. Es seien nun $m > 1$ und $\alpha \in K[G]\backslash\{0\}$ habe die Gestalt

$$\alpha = \sum_{\boldsymbol{b}\in N} a_{\boldsymbol{b}} \xi_1^{b_1} \cdots \xi_m^{b_m} = \xi_m^r(\alpha_r + \alpha_{r+1}\xi_m + \cdots + \alpha_{r+s}\xi_m^s)$$

mit $a_{\boldsymbol{b}} \in K$ sowie $\alpha_r, \ldots, \alpha_{r+s} \in K[\langle\sigma_1, \ldots, \sigma_{m-1}\rangle]$ und $\alpha_r \neq 0$. Als Element von $\mathbb{F}_p\langle B\rangle \cap K[\langle\sigma_1, \ldots, \sigma_{m-1}\rangle]$ besitzt α_r nach Induktionsannahme wenigstens das Gewicht

$$w := w(\prod_{j=1}^{m-1} \xi_j^{d_j}) \leq w(\alpha_r)$$

für ein geeignetes Tupel $(d_1, \ldots, d_{m-1}, r) \in N$. In der Darstellung

$$\alpha_r = \sum_{0\leq t_1,\ldots,t_{m-1}<p} c_{\boldsymbol{t}} \sigma_1^{t_1} \cdots \sigma_{m-1}^{t_{m-1}}$$

gibt es also mindestens w von Null verschiedene Skalare $c_{\boldsymbol{t}} \in K$. Nun läßt sich α schreiben als

$$\alpha = \xi_m^r \sum_{0\leq t_1,\ldots,t_{m-1}<p} \gamma_{\boldsymbol{t}} \sigma_1^{t_1} \cdots \sigma_{m-1}^{t_{m-1}}$$

mit

$$\gamma_{\boldsymbol{t}} = c_{\boldsymbol{t}} + c_{\boldsymbol{t},1}\xi_m + \cdots + c_{\boldsymbol{t},s}\xi_m^s.$$

Aufgrund von $s \leq p-1$ gehören die Elemente $1, \xi_m, \ldots, \xi_m^s$ zur Jennings-Basis von J (vgl. Bemerkung 8.11) und sind als solche linear unabhängig über K. Somit ist $\gamma_{\boldsymbol{t}} \neq 0$ wenn nur $c_{\boldsymbol{t}} \neq 0$ gilt. Aus Beispiel 8.14 erhalten wir die Abschätzung

$$w(\xi_m^r \gamma_{\boldsymbol{t}}) \geq r + 1$$

für jedes $\gamma_{\boldsymbol{t}} \neq 0$. Insgesamt ergibt sich hieraus mit $r = d_m$

$$w(\alpha) \geq w \cdot (r+1) = w(\prod_{j=1}^{m} \xi_j^{d_j}) = \prod_{j=1}^{m}(d_j + 1). \qquad \square$$

Satz 8.16. (Dimension und Distanz von Reed-Muller-Codes)
Es sei $C = \mathrm{RM}(r, m)$ ein Reed-Muller-Code der Ordnung r über $\mathbb{F}_p$. Dann gelten:

(a) *C besitzt die Dimension*

$$\dim(C) = \sum_{l=0}^{r}\sum_{k=0}^{m}(-1)^k \binom{m}{k} \binom{l - kp + m - 1}{m-1}.$$

(b) *Die Minimaldistanz von C beträgt*

$$d(C) = p^s(t+1)$$

mit $m(p-1) - r = s(p-1) + t$ und $0 \leq t < p-1$.

Beweis. Die Aussage (a) folgt aus Korollar 8.12 und Bemerkung 8.11 (b) vermöge

$$\dim(C) = \dim(J^{m(p-1)-r}) = \sum_{l=0}^{r} \dim(J^{m(p-1)-l}/J^{m(p-1)-l+1} = \sum_{l=0}^{r} n_l.$$

Es bleibt also nur noch (b) zu zeigen. Ist $s(p-1)+t$ die $(p-1)$-adische Darstellung von $m(p-1)-r$, so gilt offensichtlich

$$\xi_1^{p-1} \cdots \xi_s^{p-1} \xi_{s+1}^{t} \in B_{m(p-1)-r} \subseteq J^{m(p-1)-r} = C.$$

Aus Bemerkung 8.15 erhalten wir hieraus $d(C) \leq p^s(t+1)$. Ebenfalls nach Bemerkung 8.15 enthält C ein Wort

$$\beta = \prod_{j=1}^{m} \xi_j^{b_j}$$

mit $w(\beta) = d(C)$. Wir nehmen an, es gäbe mindestens zwei Indices $k \neq l$ mit $0 < b_k, b_l < p-1$. Dann ist auch

$$\tilde{\beta} = \xi_k^{b_k - 1} \xi_l^{b_l + 1} \prod_{j \neq k,l} \xi_j^{b_j}$$

ein nichttriviales Codewort von C mit Gewicht

$$w(\tilde{\beta}) = (b_k - 1)(b_l + 1) \prod_{j \neq k,l} (b_j + 1) < \prod_{j=1}^{m} (b_j + 1) = w(\beta)$$

im Widerspruch zu $d(C) = w(\beta)$ und $\tilde{\beta} \neq 0$. Also gibt es zu β höchstens einen Index l mit $0 < b_l < p-1$ und mindestens s Indices $l_1, \ldots, l_s$ mit $b_{l_j} = p-1$. Das zeigt

$$d(C) = w(\beta) = p^s(t+1). \qquad \square$$

Beispiel 8.17. (Binäre Reed-Muller-Codes)
Für $p = 2$ ist $\mathrm{RM}(r, m)$ ein $[2^m, \sum_{l=0}^{r} \binom{m}{l}, 2^{m-r}]_2$–Code.

Satz 8.18. *Die Klasse der Reed-Muller-Codes ist abgeschlossen bezüglich Dualisierung. Genauer gilt für $-1 \leq r \leq m(p-1)$*

$$\mathrm{RM}(r, m)^{\perp} = \mathrm{RM}(m(p-1) - r - 1, m).$$

Beweis. Offenbar ist

$$J = \bigoplus_{\substack{\sigma \in G \\ \sigma \neq 1}} K(1-\sigma).$$

invariant unter dem $K-$linearen Anti-Automorphismus $^-$ definiert durch $\sigma \mapsto \sigma^{-1}$. Somit sind auch die Reed-Muller-Codes $\mathrm{RM}(r,m)$ invariant unter $^-$. Wegen

$$\mathrm{RM}(r,m)^\perp = (J^{m(p-1)-r})^\perp = \overline{L(J^{m(p-1)-r})}$$

(vgl. Bemerkung 8.3) brauchen wir also gemäß unserer Behauptung lediglich

$$L(J^l) = J^{m(p-1)-l+1} \qquad \text{für } -1 \leq l \leq m(p-1)$$

zu zeigen. Da J nilpotent mit $J^{m(p-1)+1} = (0)$ ist, umfaßt der Linksannulator $L(J^l)$ von J^l die Idealpotenz $J^{m(p-1)-l+1}$. Es sei umgekehrt

$$\alpha = \sum_{\boldsymbol{b} \in \mathbb{N}^m} a_{\boldsymbol{b}} \xi_1^{b_1} \cdots \xi_m^{b_m} = a\xi_1^{d_1} \cdots \xi_m^{d_m} + \beta$$

ein Element von $L(J^l)$, wobei die Quersumme $\sum_{i=1}^m d_i$ von $(d_1, \ldots, d_m)$ minimal unter allen Trägern $\boldsymbol{b}$ von α ist. Wir nehmen an, daß α nicht in $J^{m(p-1)-l+1}$ enthalten sei. Dann gilt $\sum_{i=1}^m d_i \leq m(p-1) - l$. Wegen

$$\sum_{i=1}^m (p-1-d_i) = m(p-1) - \sum_{i=1}^m d_i \geq l$$

ist

$$\gamma = \prod_{j=1}^m \xi_j^{p-1-d_j} \in J^l.$$

Somit folgt

$$0 = \alpha\gamma = a\xi_1^{p-1} \cdots \xi_m^{p-1} = a \sum_{\sigma \in G} \sigma$$

im Widerspruch zu $a \neq 0$. Also ist die Differenzmenge $L(J^l) \backslash J^{m(p-1)-l+1}$ leer und unsere Behauptung ist bewiesen. □

8.4 Symmetrien von Reed-Muller-Codes

Satz 8.19. *Die affine Gruppe* $\mathbf{AGL}_m(\mathbb{F}_p)$ *operiert treu auf einen Reed-Muller-Code, d.h. es gilt*

$$\mathbf{AGL}_m(\mathbb{F}_p) \leq \mathrm{Sym}(\mathrm{RM}(r,m)).$$

Beweis. Zunächst einmal erklären wir auf $G = \mathbf{Z}_p^m = \langle \sigma_1, \ldots, \sigma_m \rangle$ eine $\mathbb{F}_p-$Vektorraumstruktur vermöge

$$a \cdot \sigma_1^{b_1} \cdots \sigma_m^{b_m} = \sigma_1^{ab_1} \cdots \sigma_m^{ab_m} \qquad \text{für } a \in \mathbb{F}_p.$$

Somit sind G und $\mathbb{F}_p^m \cong \mathbb{A}^m(\mathbb{F}_p)$ als $\mathbb{F}_p-$Vektorräume isomorph und es gilt

$$\mathrm{Aut}_{\mathbb{F}_p}(G) \cong \mathbf{GL}_m(\mathbb{F}_p).$$

Somit kann man die affin lineare Gruppe $\mathbf{AGL}_m(\mathbb{F}_p) = \{\phi_{\alpha,\gamma} : \alpha \in \mathbf{GL}_m(\mathbb{F}_p), \gamma \in \mathbb{F}_p^m\}$ mit $\phi_{\alpha,\gamma}(v) = \alpha(v) + \gamma$ auch durch

$$\mathbf{AGL}_m(\mathbb{F}_p) \cong \{\phi_{\alpha,\gamma} : \alpha \in \mathrm{Aut}_{\mathbb{F}_p}(G), \gamma \in G\}$$

mit der rechtsseitigen Operation

$$\sigma^{\phi_{\alpha,\gamma}} = \sigma^\alpha \gamma \qquad \text{für } \sigma \in G$$

beschreiben. Setzen wir dies $K-$linear auf $K[G]$ fort, so bewirkt $\phi_{\alpha,\gamma}$ eine Permutation der Basis von $K[G]$, d.h. es ist $\phi_{\alpha,\gamma} \in \mathrm{Aut}_{\mathbb{F}_p}(K[G])$. Wegen

$$(\sigma - 1)^{\phi_{\alpha,\gamma}} = \sigma^\alpha \gamma - 1^\alpha \gamma = (\sigma^\alpha - 1)\gamma = (\sigma^\alpha \gamma - 1) - (\gamma - 1)$$

ist J und somit auch J^l invariant unter $\phi_{\alpha,\gamma}$ und $\phi_{\alpha,\gamma}$ ist Element von $\mathrm{Sym}(J^l)$. □

Zusatz 8.20. (Knörr-Willems)
Für die Symmetriegruppe eines Reed-Muller-Codes $\mathrm{RM}(r,m)$ *über* $\mathbb{F}_p$ *gilt*

$$\mathrm{Sym}(\mathrm{RM}(r,m)) \cong \begin{cases} \mathbf{M}_m(\mathbb{F}_p) & \textit{für } r = m(p-1) \quad \textit{"monomiale Gruppe"} \\ \mathbb{F}_p^\times \times \mathbf{S}_{p^m} & \textit{für } r = 0, m(p-1)-1 \\ \mathbb{F}_p^\times \times \mathbf{AGL}_m(\mathbb{F}_p) & \textit{sonst.} \end{cases}$$

Ohne Beweis. (siehe [KW90])

Aufgabe 8.21. Zeigen Sie, daß ein linearer Code C über $\mathbb{F}_p$ der Länge m mit $\mathbf{AGL}_m(\mathbb{F}_p) \leq \mathrm{Sym}(C)$ äquivalent zu einem Reed-Muller-Code ist.

Kapitel 9

Schranken für Codes

9.1 Singleton- und Plotkin- Schranke

Definition 9.1. (Relative Distanz, asymtotische Informationsrate)
Es seien $n \in \mathbb{N}$ und q eine Primzahlpotenz. Für $d \in \mathbb{R}_{\geq 0}$ definieren wir

$$A_q(n,d) := \max\{\#C : C \subset \mathbb{F}_q^{\,n}, d(C) \geq d\}.$$

Einen $(n,c,d)_q-$Code C mit $\#C = A_q(n,d)$ nennt man **maximal**. Das Verhältnis

$$\delta := \frac{d}{n}$$

zwischen Minimaldistanz d und Länge n heißt **relative (Minimal-)Distanz** zu C. Es gilt stets $0 \leq \delta \leq 1$. Bei fester relativer Distanz δ wird die **asymptotisch maximale Informationsrate** durch

$$R_q(\delta) := \limsup_{n\to\infty} \left(\frac{1}{n} \log_q(A_q(n,\delta n)) \right)$$

definiert. Für diese gilt ebenfalls $0 \leq R_q(\delta) \leq 1$. Die Elementanzahl von Gitterpunkten in der Kugel $\mathbb{B}_r^n(\boldsymbol{y}) := \{\boldsymbol{z} \in \mathbb{F}_q^{\,n} : d(\boldsymbol{y},\boldsymbol{z}) \leq r\}$ vom Radius r um $\boldsymbol{y} \in \mathbb{F}_q^{\,n}$ bezeichnen wir mit

$$V_q(n,r) := \#\mathbb{B}_r^n(\boldsymbol{y}) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

Die einfachste Abschätzung der asymptotischen Informationsrate erhalten wir aus der im Kapitel 3 bewiesenen *Singleton-Schranke* (Satz 3.1). Diese führt auf das

Korollar 9.2. (Asymptotische Singleton - Schranke)
Bei relativer Minimaldistanz δ gilt

$$R_q(\delta) \leq 1 - \delta.$$

Beweis. Gemäß der *Singleton-Schranke* gilt $c \leq q^{n-d+1}$ für jeden $(n,c,d)_q-$Code. Daraus ergeben sich $A_q(n,d) \leq q^{n-d+1}$ und

$$R_q(n,d) \leq \limsup_{n\to\infty}\left(\frac{1}{n}(n-d+1)\right) = \limsup_{n\to\infty}\left(\frac{1}{n}(n-\lfloor \delta n\rfloor+1)\right) \leq 1-\delta. \qquad \square$$

Satz 9.3. (Plotkin - Schranke)
Die Elementanzahl eines Code $C \subset \mathbb{F}_q^n$ mit Minimaldistanz $d > n\,\frac{q-1}{q}$ ist beschränkt durch

$$\#C \leq \frac{d}{d - n\,\frac{q-1}{q}}.$$

Beweis. Es seien $c = \#C$ und $s := \sum_{(\boldsymbol{x},\boldsymbol{y})\in C\times C} d(\boldsymbol{x},\boldsymbol{y})$ die Summe sämtlicher Hamming-Distanzen in C. Aufgrund von $d(\boldsymbol{x},\boldsymbol{y}) \geq d$ für verschiedene Codewörter $\boldsymbol{x},\boldsymbol{y}$ folgt unmittelbar

$$s \geq c(c-1)d.$$

Wir wollen nun beweisen, daß zusätzlich

$$s \leq c^2 \cdot n \cdot \frac{q-1}{q}$$

gilt. Hieraus erhalten wir dann die Plotkin-Schranke, da aus $c^2 n\frac{q-1}{q} \geq s \geq c(c-1)d$ die Ungleichung

$$c \cdot \left(d - n \cdot \frac{q-1}{q}\right) \leq d$$

folgt. Es seien $\boldsymbol{x}^{(1)},\ldots,\boldsymbol{x}^{(c)}$ alle Codewörter aus C. Für ein $a \in \mathbb{F}_q$ bezeichne

$$t_i(a) := \#\{1 \leq j \leq c : x_i^{(j)} = a\}$$

die Anzahl aller Codewörter mit Eintrag a an der i-ten Stelle. Offensichtlich summieren sich die $t_i(a)$ über $\mathbb{F}_q$ zu c, d.h. es ist $\sum_{a\in\mathbb{F}_q} t_i(a) = c$. Die Anzahl der Paare $(\boldsymbol{x},\boldsymbol{y}) \in C\times C$, die sich im i-ten Symbol unterscheiden, ist $\sum_{a\in\mathbb{F}_q} t_i(a)(c-t_i(a))$. Folglich ist die Summe aller Hamming-Distanzen

$$s = \sum_{i=1}^{n}\sum_{a\in\mathbb{F}_q} t_i(a)(c-t_i(a)) = \sum_{i=1}^{n}\left(c^2 - \sum_{a\in\mathbb{F}_q} t_i(a)^2\right).$$

Mit der Cauchy-Schwarz-Ungleichung erhalten wir hieraus schließlich

$$\begin{aligned} s = \sum_{i=1}^{n}\left(c^2 - \sum_{a\in\mathbb{F}_q} t_i(a)^2\right) &\leq \sum_{i=1}^{n}\left(c^2 - \frac{1}{q}\left(\sum_{a\in\mathbb{F}_q} t_i(a)\right)^2\right) \\ &= \sum_{i=1}^{n}\left(c^2 - \frac{1}{q}\,c^2\right) \quad = \quad nc^2\left(1-\frac{1}{q}\right), \end{aligned}$$

was zu zeigen war. $\square$

Korollar 9.4. (Asymptotische Plotkin - Schranke)
Für die asymptotisch maximale Informationsrate bei relativer Distanz δ gilt

$$R_q(\delta) \begin{cases} \leq 1 - \delta \frac{q}{q-1} & \text{für } 0 \leq \delta \leq \frac{q-1}{q} \\ = 0 & \text{für } \frac{q-1}{q} \leq \delta \leq 1. \end{cases}$$

Beweis. Im Fall $\delta > \frac{q-1}{q}$ folgt unmittelbar aus Satz 9.3

$$A_q(n, \delta n) \leq \frac{\lfloor \delta n \rfloor}{\lfloor \delta n \rfloor - \frac{q-1}{q} n}.$$

Somit erhalten wir als asymptotisch maximale Informationsrate

$$R_q(\delta) = \limsup_{n\to\infty} \left(\frac{1}{n} \log_q(A_q(n, \delta n)) \right) \leq \lim_{n\to\infty} \left(\frac{\log_q \lfloor \delta n \rfloor}{n} - \frac{\log_q(\lfloor \delta n \rfloor - \frac{q-1}{q} n)}{n} \right) = 0.$$

Im Fall $\delta \leq \frac{q-1}{q}$ betrachtet man einen $(n, c, d)_q-$Code C mit Minimaldistanz $d = \lfloor \delta n \rfloor$ und Elementanzahl $c = A_q(n, d)$. Die natürliche Zahl $\tilde{n} := \lfloor (d-1) \frac{q}{q-1} \rfloor$ erfüllt die Ungleichung

$$\tilde{n} \leq (\delta n - 1) \frac{q}{q-1} < \delta \frac{q}{q-1}\, n \leq n.$$

Für $\boldsymbol{b} \in \mathbb{F}_q^{n-\tilde{n}}$ sei $C(\boldsymbol{b})$ der Teilcode $\{\boldsymbol{x} \in C : (x_{\tilde{n}+1}, \ldots, x_n) = \boldsymbol{b}\}$, und es sei $\boldsymbol{a} \in \mathbb{F}_q^{n-\tilde{n}}$ so gewählt, daß

$$\#C(\boldsymbol{a}) = \max_{\boldsymbol{b} \in \mathbb{F}_q^{n-\tilde{n}}} \#C(\boldsymbol{b}) =: \tilde{c}$$

gilt. Dies impliziert $\tilde{c} q^{n-\tilde{n}} \geq c$. Der Code

$$\tilde{C} := \{\boldsymbol{x} \in \mathbb{F}_q^{\tilde{n}} : (\boldsymbol{x}, \boldsymbol{a}) \in C\}$$

ist dann ein $(\tilde{n}, \tilde{c})_q-$Code mit Minimaldistanz

$$d(\tilde{C}) \geq d(C) = d > d - 1 \geq \frac{q-1}{q}\, \tilde{n}.$$

Nach Satz 9.3 hat dies

$$\tilde{c} \leq \frac{d}{d - \tilde{n} \frac{q-1}{q}} \quad \text{und} \quad c \leq q^{n-\tilde{n}} \tilde{c} \leq q^{n-\tilde{n}} \delta n$$

zur Folge. Somit läßt sich die asymptotische Informationsrate im Fall $\delta \leq \frac{q-1}{q}$ durch

$$\begin{aligned} R_q(\delta) &= \limsup_{n\to\infty} \left(\frac{1}{n} \log_q(A_q(n, \delta n)) \right) \leq \lim_{n\to\infty} \left(\frac{1}{n} \log_q(q^{n-\tilde{n}} \delta n) \right) \\ &= \lim_{n\to\infty} \left(\frac{n - \tilde{n}}{n} + \frac{\log_q(\delta n)}{n} \right) = \lim_{n\to\infty} \left(\frac{n - \tilde{n}}{n} \right) = 1 - \lim_{n\to\infty} \left(\frac{(\delta n - 1) q}{n(q-1)} \right) \\ &= 1 - \delta \frac{q}{q-1} \end{aligned}$$

abschätzen. □

9.2 Hamming- und Elias- Schranke

Satz 9.5. (Hamming - Schranke)
Für einen $(n,c,d)_q-$Code gilt mit $e := \lfloor \frac{d-1}{2} \rfloor$ die Abschätzung

$$c \leq \frac{q^n}{V_q(n,e)} .$$

Beweis. Die Vereinigung der Kugeln $\mathbb{B}_e^n(\boldsymbol{x})$ über alle Codewörter $\boldsymbol{x}$ ist disjunkt. Daher ist die Anzahl der Punkte dieser Überdeckung

$$c \cdot V_q(n,e) \leq q^n. \qquad \square$$

Definition 9.6. (q-adische Entropiefunktion)
Die reellwertige Funktion

$$H_q(x) := \begin{cases} 0 & \text{für } x = 0 \\ x \log_q \left(\frac{1-x}{x}(q-1)\right) - \log_q(1-x) & \text{für } 0 < x < \frac{q-1}{q} \\ 1 & \text{für } \frac{q-1}{q} \leq x \leq 1 \end{cases}$$

heißt **q-adische Entropiefunktion**.

Anmerkung 9.7. $H_2(x)$ ist die binäre Entropiefunktion aus Abschnitt 1.2.

Lemma 9.8. *Für $0 \leq \delta < \frac{q-1}{q}$ gilt*

$$H_q(\delta) = \lim_{n\to\infty} \left(\frac{1}{n} \log_q(V_q(n, \delta n)) \right).$$

Beweis. Wir setzen $r := \lfloor \delta n \rfloor$. Dann gelten

$$\binom{n}{r}(q-1)^r = S_q(n,r) \leq V_q(n,r) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i \leq (1+r)\binom{n}{r}(q-1)^r.$$

Hieraus erhält man

$$0 \leq \log_q(V_q(n,r)) - r \cdot \log_q(q-1) - \log_q(\binom{n}{r}) \leq \log_q(1+r)$$

und nach Division durch n

$$\lim_{n\to\infty} \left(\frac{1}{n} \log_q(V_q(n,r)) \right) = \delta \log_q(q-1) + \lim_{n\to\infty} \left(\frac{1}{n} \log_q \binom{n}{r} \right).$$

Es bleibt somit nur noch die Gültigkeit von

$$\lim_{n\to\infty} \left(\frac{1}{n} \log_q \binom{n}{r} \right) = \delta \log_q \left(\frac{1-\delta}{\delta} \right) - \log_q(1-\delta)$$

zu zeigen. Aus der Stirlingschen Formel ergibt sich

$$\ln(n!) = n\ln(n) - n + \mathcal{O}(\ln n) \qquad \text{für } n \to \infty,$$

wobei ln den natürlichen Logarithmus bezeichnet. Da für große n einerseits

$$r = \delta n + \mathcal{O}(1)$$

und andererseits $\mathcal{O}(\ln n) = o(n)$ gelten, erhalten wir

$$\frac{1}{n}\ \ln\binom{n}{r} = \frac{1}{n}(n\ln(n) - r\ln(r) - (n-r)\ln(n-r) + o(n)).$$

Beim Grenzprozeß $n \to \infty$ folgt hieraus

$$\begin{aligned}\frac{1}{n}\ \ln\binom{n}{r} &= \ln(n) - \delta\ln(\delta n) - (1-\delta)\ln((1-\delta)n) + o(1)\\ &= \ln(n) - \delta\ln(\delta) - \ln(n) - (1-\delta)\ln(1-\delta) + o(1)\\ &= \delta\ln\left(\frac{1-\delta}{\delta}\right) - \ln(1-\delta) + o(1).\end{aligned}$$

Dies führt mit der Transformation $\log_q(a) = \frac{\ln(a)}{\ln(q)}$ auf die Restbehauptung. □

Korollar 9.9. (Asymptotische Hamming - Schranke)
Für die asymptotische Informationsrate bei relativer Distanz $\delta < \frac{q-1}{q}$ gilt

$$R_q(\delta) \le 1 - H_q\left(\delta/2\right).$$

Beweis. Nach Satz 9.5 gilt

$$R_q(\delta) = \limsup_{n\to\infty}\left(\frac{1}{n}\ \log_q\left(\frac{q^n}{V_q(n, \frac{\delta n}{2})}\right)\right) = 1 - \lim_{n\to\infty}\left(\frac{1}{n}\ \log_q(V_q\left(n, \frac{\delta n}{2}\right))\right).$$

Mit Lemma 9.8 folgt die Behauptung. □

Ohne Beweise zitieren wir die Elias- und die asymptotische Elias-Schranke. Wir verweisen hierzu auf [Lü03, Satz 5.2.8, Kor. 5.2.11].

Satz 9.10. (Elias - Schranke)
Es seien C ein $(n, c, d)_q-$Code und r eine Zahl mit

$$r \le \frac{q-1}{q}\ n \qquad \textit{und} \qquad \frac{q}{q-1}\ r^2 - 2nr + nd > 0.$$

Dann ist die Elementanzahl von C beschränkt durch

$$c \le \frac{nd}{\frac{q}{q-1}r^2 - 2nr + nd} \cdot \frac{q^n}{V_q(n,r)}\ .$$

Korollar 9.11. (Asymptotische Elias - Schranke)
Für die asymptotische Informationsrate von Codes mit relativer Distanz δ gilt

$$R_q(\delta)\begin{cases} \le 1 - H_q\left(\frac{q-1}{q}\left(1 - \sqrt{1 - \frac{q}{q-1}\ \delta}\right)\right) & \textit{für } 0 \le \delta \le \frac{q-1}{q} \\ = 0 & \textit{für } \frac{q-1}{q} \le \delta \le 1. \end{cases}$$

9.3 Gilbert-Varshomov-Schranke

Die bisher betrachteten Schranken sind obere Schranken für Codes. Im Gegensatz dazu liefert die Gilbert-Varshomov-Schranke eine untere Abschätzung für $A_q(n,d)$.

Satz 9.12. (Gilbert - Varshomov - Schranke)
Ein maximaler Code der Länge n und Minimaldistanz d besitzt mindestens $\frac{q^n}{V_q(n,d-1)}$ Codewörter, d.h. es gilt

$$A_q(n,d) \geq \frac{q^n}{V_q(n,d-1)} .$$

Beweis. Es seien C ein maximaler $(n,c,d)_q-$Code und $\boldsymbol{y}$ ein beliebiges Element aus $\mathbb{F}_q^{\,n}$. Dann ist der Schnitt $\mathbb{B}_{d-1}^n(\boldsymbol{y}) \cap C$ nicht leer, da sonst $C \cup \{\boldsymbol{y}\}$ ein $(n,c+1,d)_q-$Code wäre, im Widerspruch zur Maximalität von C. Der gesamte Raum $\mathbb{F}_q^{\,n}$ wird also überdeckt von den Kugeln $\mathbb{B}_{d-1}^n(\boldsymbol{x})$ mit $\boldsymbol{x} \in C$, und es folgt somit

$$c \cdot V_q(n,d-1) \geq q^n. \qquad \square$$

Korollar 9.13. (Asymptotische Gilbert-Varshomov-Schranke)
Für die asymptotische Informationsrate bei relativer Distanz δ gilt

$$R_q(\delta) \geq 1 - H_q(\delta) .$$

Beweis. Aus der Gilbert-Varshomov-Schranke folgt unmittelbar

$$R_q(\delta) \geq \lim_{n\to\infty} \left(\frac{1}{n} \log_q \left(\frac{q^n}{V_q(n,\delta n-1)} \right) \right) = 1 - \lim_{n\to\infty} \left(\frac{1}{n} \log_q (V_q(n,\delta n-1)) \right) .$$

Mit Lemma 9.8 und der Definition der q-adischen Entropiefunktion erhalten wir daraus die Behauptung. $\square$

Satz 9.14. (Hinreichendes Kriterium für die Existenz von $[n,k,d]_q-$Codes)
Es seien n,k,d natürliche Zahlen mit

$$q^{n-k+1} > V_q(n,d-1).$$

Dann gibt es einen linearen $[n,k,d]_q-$Code.

Beweis. Wir beweisen diese Aussage induktiv. Der Fall $k=0$ ist trivial. Es seien nun $k>0$ und C_l ein linearer $[n,l,d]_q-$Code der Dimension $l<k$. Nach Voraussetzung gilt

$$\#C_l = q^l < \frac{q^n}{V_q(n,d-1)} .$$

Gemäß der *Gilbert-Varshomov-Schranke* ist C_l nicht maximal und es gibt ein $\boldsymbol{y} \in \mathbb{F}_q^{\,n}$ mit $\mathbb{B}_{d-1}^n(\boldsymbol{y}) \cap C_l = \emptyset$. Nun sei

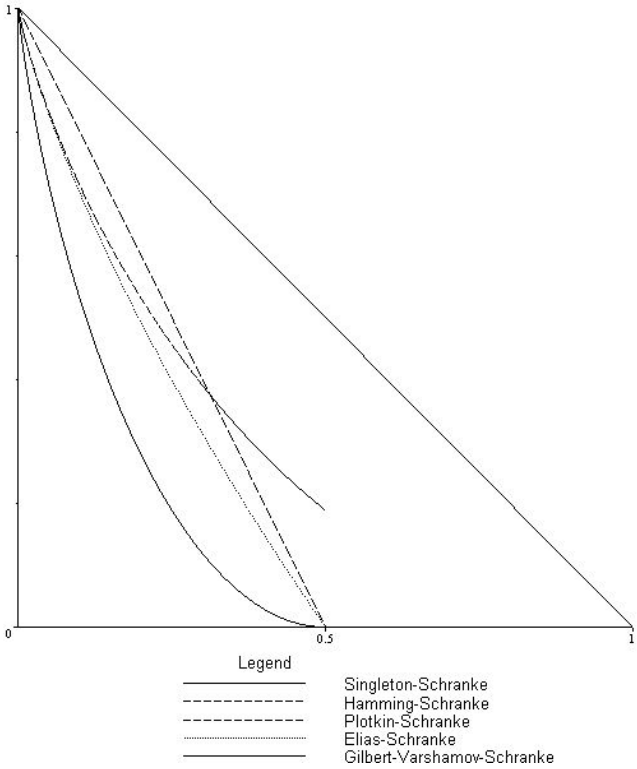
$$C_{l+1} := C_l \oplus \mathbb{F}_q \cdot \boldsymbol{y}$$

der von C_l und $\boldsymbol{y}$ aufgespannte $[n, l+1]_q-$Code. Für jedes $a \neq 0$ und $\boldsymbol{x} \in C_l$ gilt

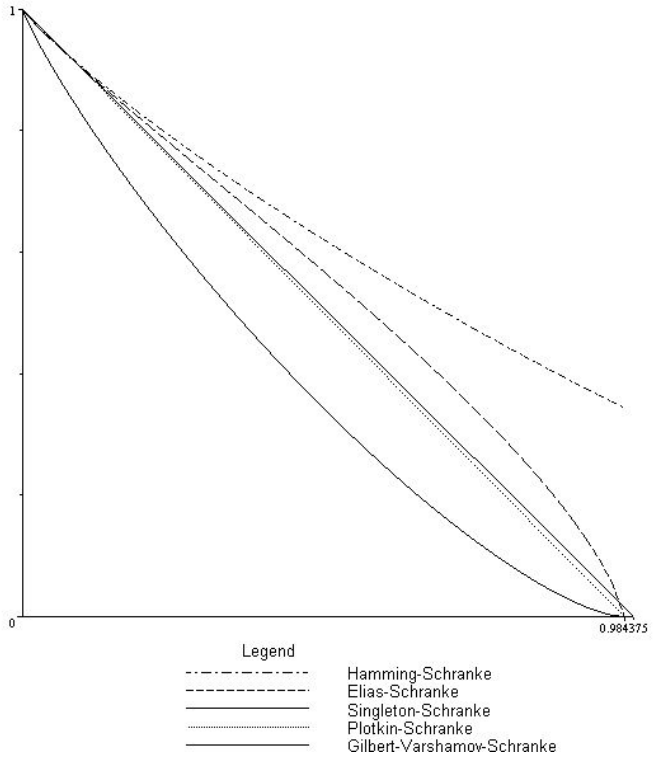
$$w(\boldsymbol{x} + a\boldsymbol{y}) = d(\boldsymbol{x}, -a\boldsymbol{y}) = d(-a^{-1}\boldsymbol{x}, \boldsymbol{y}) \geq d.$$

Also haben alle nichttrivialen Codewörter aus C_{l+1} mindestens das Gewicht d. Der Code C_{l+1} ist daher linear mit den Parametern $[n, l+1, d]_q$. □

Die Unterschiede der in diesen Kapitel vorgestellten Schranken werden in den beiden folgenden Diagrammen für $q = 2$ und 64 verdeutlich. Im zweiten Diagramm wird die Unbrauchbarkeit der Elias- und Hamming-Schranke für größere q erkennbar.



Schranken für $q = 2$



Schranken für $q = 64$

Kapitel 10

Klassische Goppa-Codes

Die Klasse der klassischen Goppa-Code liefert uns Beispiele von Codes, welche die *Gilbert-Varshomov-Schranke* asymptotisch erreichen. Im zweiten Teil des Skriptums werden wir dann noch Codes konstruieren, die diese sogar übertreffen (Kapitel 18 und 19).

10.1 Goppa-Codes

Definition 10.1. (Klassischer Goppa-Code)
Es seien $g(X) \in \mathbb{F}_{q^m}[X]$ ein normiertes Polynom vom Grad $\deg(g) \geq 2$ und $\boldsymbol{a} = (a_1, \ldots, a_n)$ ein n-Tupel paarweise verschiedener Elemente aus $\mathbb{F}_{q^m}$ mit $g(a_i) \neq 0$ für $i = 1, \ldots, n$. Dann heißt der lineare Code

$$\Gamma(\boldsymbol{a}, g) := \left\{ (x_1, \ldots, x_n) \in \mathbb{F}_q^n : \sum_{i=1}^{n} \frac{x_i}{X - a_i} \equiv 0 \pmod{g(X)} \right\}$$

über $\mathbb{F}_q$ **(klassischer) Goppa-Code** zum **Goppa-Polynom** $g(X)$. Ist zudem $g(X)$ ein irreduzibles Polynom, so heißt $\Gamma(\boldsymbol{a}, g)$ **irreduzibel**.

Notiz 10.2. Im polynomialen Restklassenring

$$R_g := \mathbb{F}_{q^m}[X]/(g(X))$$

sind die Quotienten $\frac{1}{X-a_i}$ aufgrund der Identiät

$$\frac{1}{X - a_i} = -\frac{1}{g(a_i)} \frac{g(X) - g(a_i)}{X - a_i}$$

stets als Polynome vom Grad $\deg(g)-1$ darstellbar. Setzt man $f_i(X) := -\frac{1}{g(a_i)} \frac{g(X)-g(a_i)}{X-a_i}$, so erhält man aus der Kongruenz

$$\sum_{i=1}^{n} \frac{x_i}{X - a_i} = \sum_{i=1}^{n} x_i f_i(X) \equiv 0 \pmod{g(X)}$$

wegen $\deg(f_i) < \deg(g)$ die Kontrollgleichung

$$\sum_{i=1}^{n} x_i f_i(X) = 0 \quad \text{in } \mathbb{F}_{q^m}[X]$$

für Codewörter $(x_1, \ldots, x_n)$ aus $\Gamma(\boldsymbol{a}, g)$.

Aufgabe 10.3. Wählt man $g(X) = X^{d-1}$ mit $d \leq n+1$ und $\boldsymbol{a} = (1, w, \ldots, w^{n-1})$ für eine primitive n-te Einheitswurzel w aus $\mathbb{F}_{q^m}$, so ist $\Gamma(\boldsymbol{a}, g)$ ein zyklischer Code über $\mathbb{F}_q$ der Länge n mit garantierter Minimaldistanz d (Kapitel 6).

Die Goppa-Codes können als Teilkörpercodes von Reed-Solomon-Codes (vgl. Abschnitt 3.2) konstruiert werden. Dies ist die Aussage von

Bemerkung 10.4. *Es sei $\Gamma(\boldsymbol{a}, g)$ ein Goppa-Code über $\mathbb{F}_q$ der Länge n mit Goppa-Polynom g vom Grad $\deg(g) = k$. Dann gelten:*

(a) *Im Fall $k \geq n$ ist $\Gamma(\boldsymbol{a}, g)$ der Nullcode.*

(b) *Bei $k < n$ gilt mit $\boldsymbol{b} = -(g(a_1)^{-1}, \ldots, g(a_n)^{-1})$:*

$$\Gamma(\boldsymbol{a}, g) = (RS_k(\boldsymbol{a}, \boldsymbol{b})^{\perp})|_{\mathbb{F}_q}.$$

Beweis. Nach Notiz 10.2 enthält $\Gamma(\boldsymbol{a}, g)$ genau dann das Wort $\boldsymbol{x} = (x_1, \ldots, x_n)$, falls im Polynomring $\mathbb{F}_{q^m}[X]$ die Gleichung

$$\sum_{i=1}^{n} x_i f_i(X) = 0 \qquad \text{mit } f_i(X) = b_i \cdot \frac{g(X) + b_i^{-1}}{X - a_i}$$

erfüllt ist. Aus $(X - a_i) f_i(X) = b_i g(X) + 1$ erhalten wir durch Koeffizientenvergleich die Koeffizienten der Polynome $f_i(X)$, und es gilt

$$f_i(X) = b_i \cdot \sum_{i=1}^{k} (g_i + g_i a_i + \cdots + g_i a_i^{k-i}) X^{i-1}.$$

Sämtliche Codewörter $\boldsymbol{x} \in \Gamma(\boldsymbol{a}, g)$ sind also Lösungen des homogenen Gleichungssystems $H \cdot \boldsymbol{x}^T = 0$ mit der Kontrollmatrix

$$H = \begin{pmatrix} g_k b_1 & \cdots & g_k b_n \\ (g_{k-1} + a_1 g_k) b_1 & & (g_{k-1} + a_n g_k) b_n \\ \vdots & & \vdots \\ (g_1 + g_2 a_1 + \cdots + g_k a_1^{k-1}) b_1 & \cdots & (g_1 + g_2 a_n + \cdots + g_k a_n^{k-1}) b_n \end{pmatrix}$$

$$= \begin{pmatrix} g_k & & & \\ g_{k-1} & g_k & 0 & \\ \vdots & & \ddots & \\ g_1 & \cdots & \cdots & g_k \end{pmatrix} \begin{pmatrix} b_1 & \cdots & b_n \\ a_1 b_1 & & a_n b_n \\ \vdots & & \vdots \\ a_1^{k-1} b_1 & \cdots & a_n^{k-1} b_n \end{pmatrix}.$$

Wegen

$$\det \begin{pmatrix} g_k & & 0 \\ \vdots & \ddots & \\ g_1 & \cdots & g_k \end{pmatrix} \neq 0$$

können wir auch $(b_i a_i^j)_{1 \leq i \leq n, 0 \leq j \leq k-1}$ als Kontrollmatrix zu $\Gamma(\boldsymbol{a}, g)$ auffassen. Im Fall $k \geq n$ ist eine Lösung $\boldsymbol{x}$ insbesondere eine Lösung eines Vandermondeschen Gleichungssystems und es folgt $\boldsymbol{x} = 0$. Im Fall $k < n$ ist $(b_i a_i^j)_{1 \leq i \leq n, 1 \leq j \leq k-1}$ nach Bemerkung 3.10 eine Erzeugermatrix von $RS_k(\boldsymbol{a}, \boldsymbol{b})$. Das zeigt unsere Behauptung. □

Satz 10.5. (Parameter klassischer Goppa-Codes)
Für einen Goppa-Code $\Gamma(\boldsymbol{a}, g) \leq \mathbb{F}_q^n$ mit Goppa-Polynom g vom Grad $k < n$ gelten:

(a) $\Gamma(\boldsymbol{a}, g)$ *besitzt mindestens Dimension* $n - m \cdot k$.

(b) *Die Minimaldistanz von* $\Gamma(\boldsymbol{a}, g)$ *beträgt wenigstens* $k + 1$.

Beweis. Nach Bemerkung 10.4 müssen wir lediglich den Teilkörpercode des Reed-Solomon-Codes $RS_k(\boldsymbol{a}, \boldsymbol{b})^\perp$ betrachten. Über $\mathbb{F}_{q^m}$ besitzt $RS_k(\boldsymbol{a}, \boldsymbol{b})^\perp$ die Parameter $[n, n-k, k+1]_{q^m}$. Da die Minimaldistanz beim Körperabstieg höchstens besser werden kann, folgt hieraus schon die Aussage (b). Mit dem Korollar 4.16 erhalten außerdem

$$\begin{aligned} \dim_{\mathbb{F}_q}(\Gamma(\boldsymbol{a}, g)) &\geq \dim_{\mathbb{F}_{q^m}}(RS_k(\boldsymbol{a}, \boldsymbol{b})^\perp) - (m-1)(n - \dim_{\mathbb{F}_{q^m}}(RS_k(\boldsymbol{a}, \boldsymbol{b})^\perp) \\ &= n - k - (m-1)k, \end{aligned}$$

was die Aussage (a) beweist. □

10.2 Asymtotisches Verhalten von Goppa-Codes

Definition 10.6. (Möbiusfunktion)
Die zahlentheoretische Funktion $\mu : \mathbb{N} \to \{-1, 0, 1\}$ definiert durch

$$\mu(n) = \begin{cases} 1 & : \text{ für } n = 1 \\ (-1)^l & : \text{ falls } n = \prod_{i=1}^{l} p_i \text{ mit } p_i \text{ prim und } \mathrm{ggT}(p_i, \frac{n}{p_i}) = 1 \\ 0 & : \text{ sonst} \end{cases}$$

heißt **Möbiusfunktion**. Die Menge aller normierter $\mathbb{F}_q$-Primpolynome vom Grad t bezeichnen wir mit $\mathcal{P}_q(t)$ und ihre Elementanzahl mit $N_q(t)$.

Man beachte, daß $N_q(t)$ ebenfalls eine zahlentheoretische Funktion in t ist. Es folgen einige Aussagen aus der elementaren Zahlentheorie.

Anmerkung 10.7. Die zur Möbiusfunktion μ gehörige summatorische Funktion $\sum_{d|n} \mu(d)$ ist die Nullfunktion.

Beweis. Es sei $n = \prod_{i=1}^{l} p_i^{e_i}$ die Primfaktorzerlegung einer natürlichen Zahl n mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_l$. Dann gilt für einen Teiler d von n genau dann $\mu(d) \neq 0$, wenn d ein Teiler von $m := \prod_{i=1}^{l} p_i$ ist. Daher folgt unsere Behauptung vermöge

$$\sum_{d|n} \mu(d) = \sum_{d|m} \mu(d) = \sum_{i=0}^{l} \binom{l}{i} (-1)^i = (1-1)^l = 0. \qquad \square$$

Lemma 10.8. (Möbiussche Umkehrformel)
Es seien $f : \mathbb{N} \to \mathbb{C}$ eine zahlentheoretische Abbildung und F die zu f gehörige summatorische Funktion definiert durch $F(n) = \sum_{d|n} f(d)$. Dann gilt

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Beweis. Nach Anmerkung 10.7 gilt

$$f(n) = \sum_{t|n} f(t) \sum_{d|\frac{n}{t}} \mu(d).$$

Hieraus folgt die Möbiussche Umkehrformel vermöge

$$f(n) = \sum_{t|n} \sum_{d|\frac{n}{t}} \mu(d) f(t) = \sum_{t \cdot d|n} \mu(d) f(t) = \sum_{d|n} \mu(d) \sum_{t|\frac{n}{d}} f(t) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right). \qquad \square$$

Anmerkung 10.9. Das separable Polynom $X^{q^k} - X$ ist das Produkt aller irreduziblen normierten Polynom $f(X)$ aus $\mathbb{F}_q[X]$ mit $\deg(f)|k$, d.h. es gilt

$$X^{q^k} - X = \prod_{\substack{f(X) \in \mathcal{P}_q(t) \\ \deg(f)|k}} f(X).$$

Dies folgt aus der Tatsache, daß der Zerfällungskörper eines jeden irreduziblen $\mathbb{F}_q$ - Polynoms mit Grad $d|k$ in $\mathbb{F}_{q^k}$, dem Zerfällungskörper von $X^{q^k} - X$, eingebettet ist.

Bemerkung 10.10. *Für die Anzahl normierter Primpolynome aus $\mathbb{F}_q[X]$ vom Grad t gilt*

$$N_q(k) = \frac{1}{k} \sum_{d|k} \mu(d) q^{\frac{k}{d}} \geq \frac{1}{k} \left(q^k - q^{\frac{k+2}{2}}\right).$$

Insbesondere existieren irreduzible Polynome über $\mathbb{F}_q$ von jedem beliebigen Grad.

Beweis. Nach Anmerkung 10.9 gilt

$$q^k = \deg\left(X^{q^k} - X\right) = \sum_{d|k} d \cdot N_q(d).$$

Mit der *Möbiusschen Umkehrformel* erhalten wir daraus

$$N_q(k) = \frac{1}{k} \sum_{d|k} \mu(d) q^{\frac{k}{d}}.$$

Die Ungleichung erhält man schließlich durch die grobe Abschätzung

$$\sum_{d|k} \mu(d) q^{\frac{k}{d}} \geq q^k - q^{\frac{k}{2}} - \cdots - q \geq q^k - \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} q^i \geq q^k - q^{\frac{k}{2}+1}. \qquad \square$$

Bemerkung 10.11. *Es seien d, k natürliche Zahlen mit $d \leq q^m$ und $2 < k < q^m$, und es sei*

$$N_{q^m}(k) > \sum_{j=1}^{d-1} \left\lfloor \frac{j-1}{k} \right\rfloor \binom{q^m}{j} (q-1)^j.$$

Dann gibt es einen Goppa-Code C über $\mathbb{F}_q$ der Länge q^m, der Dimension $\dim(C) \geq n - mk$ und der Minimaldistanz $d(C) \geq d$.

Beweis. Es seien $n := q^m$ sowie

$$\boldsymbol{a} := (a_1, \ldots, a_n) \qquad \text{mit } \mathbb{F}_n = \{a_1, \ldots, a_n\}.$$

Für den Nachweis unserer Behauptung reicht es zu zeigen, daß es ein irreduzibles Polynom $g(X) \in \mathbb{F}_n[X]$ vom Grad k gibt mit

$$d(\Gamma(\boldsymbol{a}, g)) \geq d.$$

Dazu betrachten wir die Anzahl der Polynome $g(X) \in \mathcal{I}_n(k)$ mit $d(\Gamma(\boldsymbol{a}, g)) < d$. Es seien $\boldsymbol{x} \neq 0$ ein Wort aus $\mathbb{F}_q^n$ vom Gewicht

$$w(\boldsymbol{x}) = j < d$$

und $I(\boldsymbol{x}) := \{1 \leq i \leq n : x_i \neq 0\}$ der Träger von $\boldsymbol{x}$. Es gilt dann

$$\sum_{i=1}^{n} \frac{x_i}{X - a_i} = \sum_{i \in I(\boldsymbol{x})} \frac{x_i}{X - a_i} = \prod_{i \in I(\boldsymbol{x})} (X - a_i)^{-1} \left(\sum_{i \in I(\boldsymbol{x})} x_i \prod_{\substack{l \in I(\boldsymbol{x}) \\ l \neq i}} (X - a_l) \right).$$

Ein Goppa-Code $\Gamma(\boldsymbol{a}, g)$ enthält also genau dann das Wort $\boldsymbol{x}$, falls das Goppa-Polynom $g(X)$ ein Teiler von $u(X) := \sum_{i \in I(\boldsymbol{x})} x_i \prod_{l \in I(\boldsymbol{x}) \setminus \{i\}} (X - a_l)$ ist. Es folgt daher

$$\begin{aligned} \#\{g(X) \in \mathcal{I}_n(k) : \boldsymbol{x} \in \Gamma(\boldsymbol{a}, g)\} &= \#\{g(X) \in \mathcal{I}_n(k) : g(X) | u(X)\} \\ &\leq \left\lfloor \frac{\deg(u)}{k} \right\rfloor \leq \left\lfloor \frac{j-1}{k} \right\rfloor. \end{aligned}$$

Summiert man diese Anzahl über alle Wörter $\boldsymbol{x} \in \mathbb{F}_n^n$ mit Gewicht $0 < w(\boldsymbol{x}) < d$, so erhält man

$$\#\{g \in \mathcal{I}_n(k) : d(\Gamma(\boldsymbol{a}, g)) < d\} \leq \sum_{j=1}^{d-1} \left\lfloor \frac{j-1}{k} \right\rfloor \binom{q^m}{j} (q-1)^j.$$

Nach Voraussetzung aber ist die Elementanzahl von $\mathcal{I}_n(k)$ echt größer als diese Zahl. Somit gibt es einen irreduziblen Goppa-Code C mit Distanz $d(C) \geq d$. □

Satz 10.12. *Die Gilbert-Varshomov-Schranke wird durch die klassischen Goppa-Codes asymptotisch erreicht.*

Beweis. Es ist zu zeigen, daß es für alle $\delta \in \mathbb{R}$ mit $0 \leq \delta \leq \frac{q-1}{q}$ eine Folge $\left(C_m^{(\delta)}\right)_{m \gg 0}$ von Goppa-Codes mit jeweils der Länge q^m und relativer Minimaldistanz $\frac{d(C_m^{(\delta)})}{q^m} \geq \delta$ gibt, deren asymptotische Informationsrate die Gleichung

$$\lim_{m \to \infty} \frac{\dim(C_m^{(\delta)})}{q^m} = 1 - H_q(\delta)$$

erfüllt.

Es seien δ mit $0 \leq \delta \leq \frac{q-1}{q}$ und $m \in \mathbb{N}$ gegeben. Wir setzen $n = n(m) := q^m$ sowie $d = d(m) := \min\{r \in \mathbb{N} : r \geq \delta n\}$. Weiterhin sei $k = k(m)$ die kleinste natürliche Zahl, sodaß

$$A := d \cdot V_q(n, d-1) \leq n^k - n^{\frac{k+2}{2}}$$

gilt, wobei $V_q(n, d-1)$ die Elementanzahl der Kugel $\mathbb{B}_{d-1}^n = \{\boldsymbol{x} \in \mathbb{F}_n^n : w(\boldsymbol{x}) < d\}$ bezeichnet. Es gilt nach Bemerkung 10.10

$$N_{q^m}(k) = N_n(k) = \frac{1}{k} \sum_{s|k} \mu(s) n^{\frac{k}{s}} \geq \frac{1}{k} \left(n^k - n^{\frac{k+2}{2}}\right).$$

Somit erhalten wir mit unserer Voraussetzung

$$\begin{aligned} N_n(k) \quad &\geq \quad \frac{d}{k} V_q(n, d-1) \quad = \quad \frac{d}{k} \sum_{j=0}^{d-1} \binom{n}{j} (q-1)^j \\ &> \quad \frac{d}{k} \sum_{j=1}^{d-1} \binom{n}{j} (q-1)^j \quad > \quad \sum_{j=0}^{d-1} \left\lfloor \frac{j-1}{k} \right\rfloor \binom{n}{j} (q-1)^j. \end{aligned}$$

Im Fall $k < n$ folgt dann nach Bemerkung 10.11 die Existenz eines Goppa-Codes $C_m^{(\delta)}$ der Länge n mit Distanz $d(C_m^{(\delta)}) \geq \delta \cdot n$ und Dimension $\dim(C_m^{(\delta)}) \geq n - mk$.

Wir zeigen nun, daß $k(m) < n(m)$ für fast alle $m \in \mathbb{N}$ gilt. Ohne Einschränkung können wir $k(m) > 3$ annehmen, da unsere Behauptung endlich viele Ausnahmen zuläßt. Aus der Minimalität von $k = k(m)$ folgt

$$n^{k-2} \leq n^{k-1} - n^{\frac{k+1}{2}} < A \leq n^k - n^{\frac{k+2}{2}} < n^k$$

und somit (unter Verwendung der monoton steigenden Funktion $\frac{1}{n}\ \log_q(\cdot)$)

$$\frac{1}{n}\ (k-2)m < \frac{1}{n}\ \log_q(A) = \frac{1}{n}\ (\log_q(d) + \log_q(V_q(n, d-1))) < \frac{1}{n}\ mk.$$

Das führt auf

$$\begin{aligned}\lim_{m\to\infty}\left(\frac{k(m)\cdot m}{n(m)}\right) &= \lim_{m\to\infty}\left(\frac{1}{n(m)}\log_q(V_q(n(m), d(m)-1))\right)\\ &= \lim_{m\to\infty}\left(\frac{1}{n(m)}\log_q(V_q(n(m), \delta n(m)))\right)\\ &= H_q(\delta) < 1,\end{aligned}$$

wobei das letzte Gleichheitszeichen aus Lemma 9.8 stammt. Daher gilt $k(m) < n(m)$ für alle hinreichend großen $m \in \mathbb{N}$.
Wir haben also gesehen, daß für alle $\delta \in \mathbb{R}$ mit $0 \le \delta \le \frac{q-1}{q}$ und alle hinreichend großen m Goppa-Codes $C_m^{(\delta)}$ mit Länge $n(m) = q^m$ und relativer Distanz $\frac{d(C_m^{(\delta)})}{q^m} \ge \delta$ existieren. Folglich gilt:

$$\lim_{m\to\infty}\left(\frac{\dim(C_m^{(\delta)})}{n(m)}\right) = \lim_{m\to\infty}\left(\frac{q^m - k(m)m}{q^m}\right) = 1 - H_q(\delta)$$

was unsere Behauptung beweist. □

10.3 Decodierung mit Euklidischem Algorithmus

Der in diesen Abschnitt beschriebene Decodieralgorithmus ermöglicht es, bei einem Goppa-Code $\Gamma(\boldsymbol{a}, g) \le \mathbb{F}_q^n$ bis zu

$$e := \left\lfloor \frac{\deg(g)}{2} \right\rfloor$$

Fehler zu korrigieren. Dabei machen wir die Generalannahme, daß der Fehlervektor

$$\boldsymbol{e} := \boldsymbol{y} - \boldsymbol{x}$$

zwischen gesendeter Nachricht $\boldsymbol{x} \in \Gamma(\boldsymbol{a}, g)$ und empfangenem Wort $\boldsymbol{y} \in \mathbb{F}_q^n$ höchstens das Gewicht e besitzt. Wesentlich bei der Fehlerkorrektur ist die Lokalisierung der fehlerhaften Symbolen, d.h. die Ermittlung der **Indexmenge der Fehlerpositionen** in $\boldsymbol{y}$

$$I := \{1 \le i \le n : e_i \ne 0\}.$$

Es bezeichnen im folgenden $s(X) \in \mathbb{F}_{q^m}[X]$ mit

$$s(X) \equiv \sum_{i=1}^{n} \frac{e_i}{X - a_i} \pmod{g(X)}$$

und $\deg(s) < \deg(g)$ das **Syndrompolynom** zu $\boldsymbol{y}$,

$$\sigma(X) := \prod_{i \in I}(X - a_i)$$

das **fehlerlokalisierende Polynom** zu $\boldsymbol{y}$ sowie

$$\omega(X) := \sum_{i \in I} e_i \prod_{j \in I \setminus \{i\}} (X - a_j)$$

das **Fehlerauswertungspolynom**. Während das Syndrompolynom $s(X)$ wegen

$$\sum_{i=1}^{n} \frac{e_i}{X - a_i} = \sum_{i=1}^{n} \frac{y_i}{X - a_i} - \sum_{i=1}^{n} \frac{x_i}{X - a_i} \equiv \sum_{i=1}^{n} \frac{y_i}{X - a_i} \pmod{g(X)}$$

direkt aus $\boldsymbol{y}$ berechenbar ist, wird zur Berechnung von $\sigma(X)$ und $\omega(X)$ der Euklidische Algorithmus benötigt. Dazu bemerken wir zunächst, daß $\omega(X)$ aufgrund von

$$s(X) \cdot \sigma(X) = \sum_{i \in I} \frac{e_i}{X - a_i} \prod_{i \in I}(X - a_i) \equiv \omega(X) \pmod{g(X)}$$

aus $s(X)$ und $g(X)$ linear kombinierbar ist, d.h. daß es ein $u(X) \in \mathbb{F}_{q^m}[X]$ gibt mit

$$s(X) \cdot \sigma(X) + u(X) \cdot g(X) = \omega(X). \qquad (*)$$

Die folgende Bemerkung zeigt, wie man $\sigma(X)$ und $\omega(X)$ mit dem Euklidischen Algorithmus explizit berechnen kann. Dabei sei $(f_i(X))_{i \in \mathbb{N}}$ die Folge von Polynomen mit $f_0(X) = g(X)$ und $f_1(X) = s(X)$, die man durch fortgestzte Division mit Rest erhält:

$$f_i(X) = q_{i+1}(X) f_{i+1}(X) + f_{i+2}(X).$$

Bemerkung 10.13. *Mit den obigen Bezeichnungen gelten:*

(a) *Es gibt einen Index $j \in \mathbb{N}$ mit*

$$0 \leq \deg(f_j) < e \leq \deg(f_{j-1}).$$

(b) *Aus der Darstellung $f_j(X) = a_j(X)g(X) + b_j(X)s(X)$ erhält man mit einen geeigneten Koeffizienten $c \in \mathbb{F}_{q^m}^{\times}$*

$$\sigma(X) = c \cdot b_j(X) \qquad \textit{und} \qquad \omega(X) = c \cdot f_j(X).$$

Beweis. (a) Die Folge $(f_i(X))_{i \in \mathbb{N}}$ enthält den größten gemeinsamen Teiler von $g(X)$ und $s(X)$, d.h. es gibt eine Zahl $l \in \mathbb{N}$ mit

$$f_l(X) = \mathrm{ggT}(g(X), s(X)).$$

Aufgrund der Gleichung (*) ist $f_l(X)$ ein Teiler von $\omega(X)$ und besitzt somit den Grad $\deg(f_l) \leq \deg(w) < e$. Die Behauptung folgt nun aus $\deg(f_{i+1}) < \deg(f_i)$ und $\deg(f_0) = \deg(g) > e$.
(b) Mit dem Euklidischen Algorithmus gewinnt man Polynome $a_0(X), \ldots, a_l(X)$ und $b_0(X), \ldots, b_l(X)$ aus $\mathbb{F}_{q^m}[X]$ mit

$$f_i(X) = a_i(X)g(X) + b_i(X)s(X).$$

Behauptung 1: Die Polynompaare $(a_i(X), b_i(X))$ *sind teilerfremd für* $i = 0, \ldots, l$.
Aufgrund $f_{i+1}(X) = f_{i-1}(X) - q_i(X)f_i(X)$ gelten

$$a_{i+1}(X) = a_{i-1}(X) - q_i(X)a_i(X) \qquad \text{und} \qquad b_{i+1}(X) = b_{i-1}(X) - q_i(X)b_i(X).$$

Daraus folgt induktiv

$$\begin{aligned}\det \begin{pmatrix} a_{i+1}(X) & b_{i+1}(X) \\ a_i(X) & b_i(X) \end{pmatrix} &= \det \begin{pmatrix} a_{i-1}(X) & b_{i-1}(X) \\ a_i(X) & b_i(X) \end{pmatrix} \\ &= \quad \cdots \quad = \pm \det \begin{pmatrix} a_0(X) & b_0(X) \\ a_1(X) & b_1(X) \end{pmatrix} = \pm \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \pm 1.\end{aligned}$$

Insbesondere gibt es also Polynome $q(X), r(X)$ mit

$$q(X) \cdot \begin{pmatrix} a_{i+1}(X) \\ a_i(X) \end{pmatrix} + r(X) \cdot \begin{pmatrix} b_{i+1}(X) \\ b_i(X) \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Behauptung 2: Es gilt $\deg(b_i) = \deg(g) - \deg(f_{i-1})$ *für* $i = 1, \ldots, l$.
Auch dies beweisen wir induktiv. Wegen $b_1(X) = 1$ und $f_0(X) = g(X)$ gilt die Behauptung für $i = 1$. Beim Induktionsschritt von i auf $i + 1$ sind aufgrund von $b_{i+1}(X) = b_{i-1}(X) - q_i(X)b_i(X)$ und $\deg(q_i) \geq 1$ die Grade der Polynome $b_{i+1}(X)$ und $q_i(X)b_i(X)$ gleich, wovon man sich durch eine seperate Induktion überzeugen kann. Das führt zu

$$\begin{aligned}\deg(b_{i+1}) &= \deg(q_i) + \deg(b_i) = \deg(q_i) + \deg(g) - \deg(f_{i-1}) \\ &= \deg(q_i) + \deg(g) - \deg(q_i f_i) = \deg(g) - \deg(f_i).\end{aligned}$$

Behauptung 3: Es gelten

$$\sigma(X) \cdot f_j(X) = \omega(X) \cdot b_j(X) \qquad \textit{und} \qquad \sigma(X) \cdot a_j(X) = u(X) \cdot b_j(X).$$

Mit dem Euklidischen Algorithmus erhält man einerseits

$$\sigma(X) \cdot f_j(X) = \sigma(X) \cdot (a_j(X)g(X) + b_j(X)s(X))$$

und andererseits mit (*)

$$\omega(X) \cdot b_j(X) = (s(X)\sigma(X) + u(X)g(X)) \cdot b_j(X).$$

Das Differenzpolynom ist dann

$$\sigma(X)f_j(X) - \omega(X)b_j(X) = (\sigma(X)a_j(X) - u(X)b_j(X)) \cdot g(X).$$

Es gilt dabei nach Aussage (a)

$$\deg(\sigma f_j) = e + \deg(f_j) < 2e \leq \deg(g)$$

und mit Behauptung 2

$$\deg(wb_j) = \deg(w) + (\deg(g) - \deg(f_{j-1})) \leq (e-1) + \frac{\deg(g)}{2} < \deg(g).$$

Also besitzen sowohl $\sigma(X)f_j(X)$ wie auch $\omega(X)b_j(X)$ einen kleineren Polynomgrad als $g(X)$. Dies führt zu

$$\sigma(X)f_j(X) - \omega(X)b_j(X) = 0 \qquad \text{und} \qquad \sigma(X)a_j(X) - u(X)b_j(X) = 0.$$

Nun schließt man aus Behauptung 3 auf Aussage (b) wie folgt: Da $\sigma(X)$ und $\omega(X)$ teilerfremd sind, teilt $\sigma(X)$ das Polynom $b_j(X)$, das wiederum aufgrund der Behauptung 1 ein Teiler von $\sigma(X)$ ist. Also unterscheiden sich $\sigma(X)$ und $b_j(X)$ nur durch Multiplikation einer Einheit $c \in \mathbb{F}_{q^m}$. Desweiteren folgt aus Behauptung 3

$$\omega(X) \cdot b_j(X) = \sigma(X) \cdot f_j(X) = c \cdot b_j(X) \cdot f_j(X)$$

und somit $\omega(X) = c \cdot f_j(X)$, was zu zeigen war. □

Decodieralgorithmus 10.14. Es sei $\boldsymbol{y} \in \mathbb{F}_q^n$ die empfangene Nachricht.

(1) Konstruiere das Syndrompolynom $s(X) \in \mathbb{F}_q[X]$ mit

$$s(X) \equiv \textstyle\sum_{i=1}^{n} \frac{y_i}{X - a_i} \pmod{g(X)}$$

und $\deg(s) < \deg(g)$.

(2) Berechne das Fehlerortungspolynom $\sigma(X)$ und das Fehlerauswertungspolynom $\omega(X)$ mit dem Euklidischem Algorithmus gemäß Bemerkung 10.13.

(3) Bestimme die Fehlerstellenmenge I als Nullstellenmenge von $\sigma(X)$.

(4) Berechne den Fehlervektor $\boldsymbol{e} = (e_1, \ldots, e_n)$ mittels $e_i = 0$ für $i \notin I$ und

$$\omega(a_i) = e_i \cdot \textstyle\prod_{j \in I \setminus \{i\}} (a_i - a_j) \qquad \text{für } i \in I.$$

(5) Decodiere $\boldsymbol{y}$ zu $\boldsymbol{x} := \boldsymbol{y} - \boldsymbol{e}$.

Teil II

Arithmetische Codes

Kapitel 11

Geometrische Goppa-Codes

11.1 Konstruktion arithmetischer Codes

Anfang der 80er Jahre stellte V.D.Goppa einen faszinierenden Zusammenhang zwischen algebraischer Geometrie und Codierungstheorie vor [Gop02] und begründete damit die arithmetische Codierungstheorie. Durch Residuen- oder Restklassenauswertung von algebraischen Funktionen erhält man Einbettungen in $\mathbb{F}_q^n$. Eine zentrale Bedeutung hat hierbei der Satz von *Riemann-Roch* mit dessen Hilfe man gute und exakte Aussagen über die arithmetischen Codes gewinnen kann. Insbesondere erhalten wir eine untere Schranke für die Minimaldistanz, die in der Codierungstheorie eher selten zu bekommen ist. Das Geschlecht der zugrundeliegenden Kurve bzw. des algebraischen Funktionenkörpers steht in enger Beziehung mit dem Singletondefekt der arithmetischen Codes. In Kapitel 20 werden wir sogar sehen, daß jeder lineare Codes im wesentlichen ein arithmetischer Code ist. Eine weitere besondere Anwendung für arithmetische Codes findet man beim Versuch, die *Gilbert-Varshamov-Schranke* zu verbessern, was mit Hilfe von Modulkurven auch tatsächlich gelingt. Darauf gehen wir in den Kapiteln 18 und 19 ein. Die Beschreibung der arithmetischen Codes erfolgt hier über algebraischen Funktionenkörpern wie im Buch von H.Stichtenoth [Sti93]. Dort kann man ebenfalls die Grundlagen der Theorie der algebraischen Funktionen nachlesen, die hier vorgesetzt werden. Zentrale Aussagen können aber im Anhang nachgelesen werden und sind kursiv gekennzeichnet.

Definition 11.1. (Arithmetischer Code)
Es seien $F{:}\mathbb{F}_q$ ein algebraischer Funktionenkörper einer Variablen und $\mathfrak{P}_1, \ldots, \mathfrak{P}_n \in \mathbb{P}_{F:\mathbb{F}_q}^{(1)}$ paarweise verschiedene rationale Stellen in F sowie $\mathfrak{A} = \prod_{i=1}^{n} \mathfrak{P}_i$ ihr Produkt. Weiter sei $\mathfrak{G}$ ein zu $\mathfrak{A}$ teilerfremder Divisor und $\mathcal{L}(\mathfrak{G})$ der zugehörige Riemann-Roch-Raum. Der durch die Auswertung der algebraischen Funktionen von $\mathcal{L}(\mathfrak{G})$ an den Stellen $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ gewonnene Code

$$C = C(\mathfrak{A}, \mathfrak{G}) := \{(x(\mathfrak{P}_1), \ldots, x(\mathfrak{P}_n)) : x \in \mathcal{L}(\mathfrak{G})\}$$

heißt **geometrischer Goppa-Code** oder **arithmetischer Code** (über $F{:}\mathbb{F}_q$). Der Divisor $\mathfrak{A}$ heißt **Auswertungsdivisor** von C und $\mathfrak{G}$ **Goppa-Divisor** von C.

Satz 11.2. (Parameter und Erzeugermatrix von $C(\mathfrak{A}, \mathfrak{G})$)
Für einen arithmetischen Code $C = C(\mathfrak{A}, \mathfrak{G})$ mit Auswertungsdivisor $\mathfrak{A} = \prod_{i=1}^{n} \mathfrak{P}_i$ gelten:

(a) *C ist ein linearer $[n, k, d]_q$-Code mit der Länge $n = \deg(\mathfrak{A})$, der Dimension $k = \dim(\mathfrak{G}) - \dim(\mathfrak{A}^{-1}\mathfrak{G})$ und der Minimaldistanz $d \geq n - \deg(\mathfrak{G})$.*

(b) *Ist $x_1, ..., x_k$ ein Vertretersystem in $\mathcal{L}(\mathfrak{G})$ einer Basis von $\mathcal{L}(\mathfrak{G})/\mathcal{L}(\mathfrak{A}^{-1}\mathfrak{G})$, so ist die Matrix $(x_i(\mathfrak{P}_j))_{1 \leq i \leq k, 1 \leq j \leq n}$ eine erzeugende Matrix von C.*

Beweis. Zunächst stellen wir fest, daß die Restklassenkörper $\mathcal{R}_{\mathfrak{P}_i}$ von $\mathfrak{P}_i$ mit dem Konstantenkörper $\mathbb{F}_q$ übereinstimmen. Somit ist C in $\mathbb{F}_q^{\,n}$ enthalten. Die Auswertungsabbildung

$$\phi : \begin{cases} \mathcal{L}(\mathfrak{G}) & \longrightarrow\!\!\!\!\!\rightarrow \quad C(\mathfrak{A}, \mathfrak{G}) \\ x & \longmapsto \quad (x(\mathfrak{P}_1), ..., x(\mathfrak{P}_n)) \end{cases}.$$

ist $\mathbb{F}_q$-linear und daher ist C ein linearer Code. Eine Funktion x aus dem linearen Raum $\mathcal{L}(\mathfrak{G})$ zum Goppa-Divisor $\mathfrak{G}$ liegt genau dann im Kern von ϕ, wenn $x(\mathfrak{P}) = 0$ für alle Primteiler $\mathfrak{P}$ von $\mathfrak{A}$ gilt, d.h. wenn x Element von $\mathcal{L}(\mathfrak{A}^{-1}\mathfrak{G})$ ist. Damit gilt nach dem Homomorphiesatz

$$C(\mathfrak{A}, \mathfrak{G}) \cong \mathcal{L}(\mathfrak{G})/\mathcal{L}(\mathfrak{A}^{-1}\mathfrak{G}).$$

Die Dimension von C ergibt sich nun als

$$k = \dim(C) = \dim(\mathcal{L}(\mathfrak{G})) - \dim(\mathcal{L}(\mathfrak{A}^{-1}\mathfrak{G})) = \dim(\mathfrak{G}) - \dim(\mathfrak{A}^{-1}\mathfrak{G}).$$

Hieraus folgt Aussage (b), da die Bilder von $x_1, ..., x_k$ unter ϕ, nämlich die Vektoren $(x_i(\mathfrak{P}_1), ..., x_i(\mathfrak{P}_n))$, eine Basis von C bilden. Wir bestimmen nun die Minimaldistanz d von C. Dazu nehmen wir an, daß C nicht der Nullraum sei. Dann gibt es eine Funktion x aus $\mathcal{L}(\mathfrak{G})$, sodaß das Wort $\phi(x)$ Hamming-Gewicht d besitzt. Folglich verschwindet x auf $n - d$ paarweise verschiedenen Stellen $\mathfrak{P}_{i_1}, \ldots, \mathfrak{P}_{i_{n-d}}$ für Indices $i_j \in \{1, \ldots, n\}$ und es gilt $x \in \mathcal{L}(\mathfrak{B}^{-1}\mathfrak{G})$, wobei $\mathfrak{B}$ das Produkt $\prod_{j=1}^{n-d} \mathfrak{P}_{i_j}$ bezeichne. Hieraus folgt

$$0 \leq \deg(\mathfrak{B}^{-1}\mathfrak{G}) = \deg(\mathfrak{G}) - n + d. \qquad \square$$

Aus der obigen Charakterisierung der Minimaldistanz läßt sich eine explizite Formel gewinnen.

Zusatz 11.3. *Es sei $c \in \mathbb{N}$ der minimale Grad eines ganzen Divisors $\mathfrak{C}$, der zu einem Divisor der Gestalt $\mathfrak{B}^{-1}\mathfrak{G}$ äquivalent ist, wobei $\mathfrak{B}$ ein ganzer Teiler von $\mathfrak{A}$ sei. Dann hat der arithmetische Code $C(\mathfrak{A}, \mathfrak{G})$ die Minimaldistanz*

$$d = n - \deg(\mathfrak{G}) + c.$$

Die untere Schranke für die Minimaldistanz in Satz 11.2 wird also genau dann angenommen, wenn der Goppa-Divisor äquivalent zu einem Teiler des Auswertungsdivisors ist.

Beweis. Alle Funktionen x aus dem linearen Raum $\mathcal{L}(\mathfrak{G})$ haben einen Divisor der Form $\mathfrak{B}\mathfrak{C}\mathfrak{G}^{-1}$, wobei $\mathfrak{B}$ das Produkt aller Primteiler von $\mathfrak{A}$ ist, in denen x verschwindet. Das Wort $\phi(x)$ hat somit das Gewicht

$$w(\phi(x)) = w(x(\mathfrak{P}_1), \ldots, x(\mathfrak{P}_n)) = n - \deg(\mathfrak{B}) = n - (\deg(\mathfrak{G}) - \deg(\mathfrak{C})).$$

Für ein gegebenes Wort $(x(\mathfrak{P}_1), \ldots, x(\mathfrak{P}_n))$ von Minimalgewicht d ist also der Grad des zugehörigen Teilers $\tilde{\mathfrak{C}}$ von $(x)_0$ gerade

$$c = \min\{\deg(\mathfrak{C}) : 1|\mathfrak{C},\ \mathfrak{C} \sim \mathfrak{B}^{-1}\mathfrak{G} \text{ mit } 1|\mathfrak{B}|\mathfrak{A}\}. \qquad \square$$

Korollar 11.4. *Es sei $C = C(\mathfrak{A}, \mathfrak{G})$ ein arithmetischer Code über einen Funktionenkörper F:$\mathbb{F}_q$ vom Geschlecht g.*

(a) *Unter der Voraussetzung $\deg(\mathfrak{A}^{-1}\mathfrak{G}) < 0$ hat C Dimension $k = \dim(\mathfrak{G})$ und Minimaldistanz $d \geq n - k + 1 - g$. Insbesondere ist der Singletondefekt von C durch das Geschlecht des zugrundeliegenden Funktionenkörpers beschränkt.*

(b) *Bei $\deg(\mathfrak{A}^{-1}\mathfrak{G}) \geq 2g - 1$ ist C der volle Vektorraum $\mathbb{F}_q^n$.*

Beweis. Im Fall $\deg(\mathfrak{A}^{-1}\mathfrak{G}) < 0$ ist der Riemann-Roch-Raum $\mathcal{L}(\mathfrak{A}^{-1}\mathfrak{G})$ leer. Hieraus folgt $\dim(C) = \dim(\mathfrak{G}) - \dim(\mathfrak{A}^{-1}\mathfrak{G}) = \dim(\mathfrak{G})$. Aus dem Satz von *Riemann-Roch* ergibt sich zudem

$$d \geq n - \deg(\mathfrak{G}) \geq n - (\dim(\mathfrak{G}) + (g-1)) = n - k - (g-1).$$

Es sei nun $\deg(\mathfrak{A}^{-1}\mathfrak{G}) \geq 2g - 1$. Dann folgt nach dem Satz von *Riemann-Roch* $\dim(\mathfrak{A}^{-1}\mathfrak{G}) = \deg(\mathfrak{A}^{-1}\mathfrak{G}) - g + 1$. Da der Grad von $\mathfrak{A}$ positiv ist, gilt ebenso $\dim(\mathfrak{G}) = \deg(\mathfrak{G}) - g + 1$. Für die Dimension von C impliziert dies

$$k = \dim(C) = \dim(\mathfrak{G}) - \dim(\mathfrak{A}^{-1}\mathfrak{G}) = \deg(\mathfrak{G}) - \deg(\mathfrak{A}^{-1}\mathfrak{G}) = \deg(\mathfrak{A}) = n. \qquad \square$$

Beispiel 11.5. Wir betrachten den Kongruenzfunktionenkörper $F = \mathbb{F}_4(x, y)$ mit der definierenden Gleichung $x^3 + y^3 + 1 = 0$. Bezeichnet w eine primtive dritte Einheitswurzel in $\mathbb{F}_4$, so ist F:$\mathbb{F}_4(x)$ eine *Kummererweiterung* mit Minimalpolynom

$$g(T) = T^3 + x^3 + 1 = T^3 + \prod_{i=1}^{3} (x + w^i)$$

für y. Für alle Primdivisoren $\mathfrak{P} \neq (x)_\infty$ aus $\mathbb{F}_4(x)$ ist y ganz über den Bewertungsring $\mathcal{O}_\mathfrak{P}$ und es ist somit der Differentenexponent einer Divisorenerweiterung $\mathfrak{P}'|\mathfrak{P}$ beschränkt durch

$$0 \leq d_{\mathfrak{P}'}(F{:}\mathbb{F}_4(x)) \leq \operatorname{ord}_{\mathfrak{P}'}(g'(y)) = \operatorname{ord}_{\mathfrak{P}'}(y^2),$$

wobei $g'(T)$ die gewöhnliche Ableitung von $g(T)$ bezeichne (vgl. [Sti93, III.5.10.]). Wegen der Relation $y^3 = x^3 + 1$ können daher nur die Primstellen $\mathfrak{P}_i = (x + w^i)_0$

sowie der bisher ausgenommene Primdivisor $\mathfrak{O} = (x)_\infty$ in $F{:}\mathbb{F}_4(x)$ verzweigen. Wegen $g(T)(\mathfrak{P}_i) = T^3$ sind $\mathfrak{P}_1, \mathfrak{P}_2$ und $\mathfrak{P}_3$ nach dem *Dedekindschen Kriterium* und dem *Dedekindschen Differentensatz* total verzweigt in $F{:}\mathbb{F}_4(x)$ mit jeweils Differentenexponenten 2. Die Stellen $\mathfrak{P}_0 = (x)_0$ und $\mathfrak{O} = (x)_\infty$ sind hingegen voll zerlegt in $F{:}\mathbb{F}_4(x)$. Das Minimalpolynom $g(T)$ zerfällt modulo $\mathfrak{P}_0$ in paarweise verschiedene Linearfaktoren und somit zerfällt $\mathfrak{P}_0$ nach dem *Dedekindschen Kriterium* in $F{:}\mathbb{F}_4(x)$. Die gleiche Betrachtung wenden wir für $\mathfrak{O}$ an. Unter der Variablensubstitution $y \mapsto \frac{y}{x}$ bleibt F invariant und es ist $h(T) = T^3 + \frac{x^3+1}{x^3}$ das Minimalpolynom für $\frac{y}{x}$. Dann gilt $h(T)(\mathfrak{O}) = T^3 + 1 = g(T)(\mathfrak{P}_0)$ und es ist somit auch $\mathfrak{O}$ voll zerlegt in $F{:}\mathbb{F}_4(x)$. Damit ist der Grad der Differente $\mathfrak{D}(F{:}\mathbb{F}_4(x))$ nach der *Hurwitzschen Relativgeschlechtformel*

$$6 = \deg(\mathfrak{D}(F{:}\mathbb{F}_4(x)) = 2\, g_{F:\mathbb{F}_4} - 2\,(1 - [F{:}\mathbb{F}_4(x)]) = 2\, g_{F:\mathbb{F}_4} + 4.$$

Insgesamt erhalten wir

$$g_{F:\mathbb{F}_4} = 1 \qquad \text{und} \qquad \#\mathbb{P}^{(1)}_{F:\mathbb{F}_4} = 9,$$

insbesondere ist F ein elliptischer Funktionenkörper (vgl. Kapitel 13).
Es bezeichne $F_1 = \mathbb{F}_2(x, y)$ und $F_3 = \mathbb{F}_8(x, y)$. Mit $\#\mathbb{P}^{(1)}_{F:\mathbb{F}_4}$ lassen sich die L-Polynome $L_{F:\mathbb{F}_4}, L_{F_1:\mathbb{F}_2}$ und $L_{F_3:\mathbb{F}_8}$ berechnen (siehe Anhang). Es gilt

$$\begin{aligned} L_{F:\mathbb{F}_4}(t) &= 1 + (\#\mathbb{P}^{(1)}_{F:\mathbb{F}_4} - (q+1))t + qt^2 = 1 + 4t + 4t^2 \\ &= (1 - \omega_1^2 t)(1 - \omega_2^2 t) \end{aligned}$$

mit $\omega_1 = \sqrt{-2}$ und $\omega_2 = -\sqrt{-2}$. Daraus folgen

$$\begin{aligned} & & L_{F_1:\mathbb{F}_2}(t) &= (1 - \omega_1 t)(1 - \omega_2 t) = 1 + 2t^2 \\ \text{und} & & L_{F_3:\mathbb{F}_8}(t) &= (1 - \omega_1^3 t)(1 - \omega_2^3 t) = 1 + 8t^2. \end{aligned}$$

Mit der Formel

$$\#\mathbb{P}^{(1)}_{F_r:\mathbb{F}_{2^r}} = 2^r + 1 - (\omega_1^r + \omega_2^r)$$

folgern wir schließlich, daß $F_1{:}\mathbb{F}_2$ drei und $F_3{:}\mathbb{F}_8$ neun rationale Stellen besitzt. Mit den Konstantenerweiterungen $F{:}F_1$ bzw. $F_3{:}F_1$ werden also 6 rationale Stellen gewonnen. Nur Primdivisoren, deren Grad mit dem Grad der Konstantenerweiterung übereinstimmt, zerfallen in ein Produkt rationaler Stellen. Der Funktionenkörper F_1 besitzt folglich 3 Primdivisoren vom Grad 2 und 2 Primstellen vom Grad 3.
Es seien $\mathfrak{Q}_1$ und $\mathfrak{Q}_2$ die Einbettungen in F der beiden Primdivisoren vom Grad 3. Dann ist der Divisor $\mathfrak{G} = \mathfrak{Q}_1\mathfrak{Q}_2$ fremd zu $\mathfrak{A} = \prod_{\mathfrak{P} \in \mathbb{P}_F^{(1)}} \mathfrak{P}$. Somit ist der arithmetische Code $C(\mathfrak{A}, \mathfrak{G})$ wohldefiniert. Da der Divisorgrad bei einer (algebraischen) Konstantenerweiterung invariant bleibt (siehe Anhang), hat $\mathfrak{G}$ Grad 6 und es gilt für $C(\mathfrak{A}, \mathfrak{G})$ nach Korollar 11.4

$$k = \dim(\mathfrak{G}) = \deg(\mathfrak{G}) = 6 \qquad \text{und} \qquad d \geq n - k = 3.$$

$C(\mathfrak{A}, \mathfrak{G})$ ist also ein Beispiel für einen arithmetischen $[9, 6, d]_4$-Code mit Distanz $d = 3$ oder 4. Nach der *MDS-Vermutung* müßte dieser Code Singletondefekt 1 und somit Distanz $d = 3$ besitzen. Dies können wir später in Kapitel 13 bestätigen, da wir dort die *MDS-Vermutung* für Codes über elliptischen Funktionenkörpern beweisen.

Aufgabe 11.6. Konstruieren Sie sogenannte Standardcodes $C(\mathfrak{A}, \mathfrak{P}^r)$ über den Funktionenkörper $\mathbb{F}_q(x, y)$ mit der definierenden Relation $x^3y + y^3 + x = 0$ für $q = 8, 9$. Wählen Sie als Goppa-Divisor Potenzen $\mathfrak{P}^r$ der einzigen und rationalen Polstelle $\mathfrak{P}$ von y und als Auswertungsdivisor $\mathfrak{A}$ das Produkt sämtlicher rationaler Stellen ausgenommen $\mathfrak{P}$.

11.2 Duale arithmetische Codes

In diesen Abschnitt stellen wir eine Konstruktion von Codes via Residuenauswertung vor. Diese Codes sind dual zu den arithmetischen Codes und, wie wir im nächsten Abschnitt sehen werden, selbst wieder arithmetische Codes.

Definition 11.7. (Dualer arithmetischer Code)
In der Situation von Definition 11.1 heißt der durch die Residuenauswertung der Differentiale aus $\Delta(\mathfrak{A}^{-1}\mathfrak{G})$ an den Stellen $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ gewonnene Code

$$C^*(\mathfrak{A}, \mathfrak{G}) := \{(\mathrm{Res}_{\mathfrak{P}_1}(\delta), \ldots, \mathrm{Res}_{\mathfrak{P}_n}(\delta)) : \delta \in \Delta(\mathfrak{A}^{-1}\mathfrak{G})\}$$

dualer arithmetischer Code.

Satz 11.8. (Parameter und Erzeugermatrix von $C^*(\mathfrak{A}, \mathfrak{G})$)
Für einen dualen arithmetischen Code $C^* = C^*(\mathfrak{A}, \mathfrak{G})$ mit $\mathfrak{A} = \prod_{i=1}^n \mathfrak{P}_i$ über einem Funktionenkörper F:$\mathbb{F}_q$ vom Geschlecht g gelten:

(a) *C^* ist ein linearer $[n, k^*, d^*]_q$-Code mit der Dimension $k^* = i(\mathfrak{A}^{-1}\mathfrak{G}) - i(\mathfrak{G})$ und der Minimaldistanz $d^* \geq \deg(\mathfrak{G}) - 2g + 2$, wobei $i(\mathfrak{S})$ den Spezialitätsindex eines Divisors $\mathfrak{S}$ bezeichne.*

(b) *Sind $\delta_1, \ldots, \delta_{k^*} \in \Delta(\mathfrak{A}^{-1}\mathfrak{G})$ Vertreter einer Basis von $\Delta(\mathfrak{A}^{-1}\mathfrak{G})/\Delta(\mathfrak{G})$, so bildet $(\mathrm{Res}_{\mathfrak{P}_j}(\delta_i))_{1 \leq i \leq k^*, 1 \leq j \leq n}$ eine Erzeugermatrix von C^*.*

Beweis. Wiederum ist zu bemerken, daß die Residuen an den Stellen $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ Werte in $\mathbb{F}_q$ ergeben. Daher ist C^* in $\mathbb{F}_q^n$ enthalten und linear, da die Residuenauswertung

$$\psi : \begin{cases} \Delta(\mathfrak{A}^{-1}\mathfrak{G}) & \twoheadrightarrow & C^*(\mathfrak{A}, \mathfrak{G}) \\ \delta & \longmapsto & (\mathrm{Res}_{\mathfrak{P}_1}(\delta), \ldots, \mathrm{Res}_{\mathfrak{P}_n}(\delta)) \end{cases}$$

wie die Restklassenauswertung $\mathbb{F}_q$-linear ist. Ein Differential δ aus $\Delta(\mathfrak{A}^{-1}\mathfrak{G})$ hat definitionsgemäß Ordnung $\mathrm{ord}_{\mathfrak{P}}(\delta) \geq -1$ bei den Primteiler $\mathfrak{P}$ von $\mathfrak{A}$. Also sind genau die Differentiale aus $\Delta(\mathfrak{A}^{-1}\mathfrak{G})$ im Kern der Abbildung ψ enthalten, die bei $\mathfrak{P}$ regulär sind, d.h. die $\mathrm{ord}_{\mathfrak{P}}(\delta) \geq 0$ für $\mathfrak{P}|\mathfrak{A}$ erfüllen. Damit gilt $\mathrm{Kern}(\psi) = \Delta(\mathfrak{G})$ und es folgt nach dem Homorphiesatz

$$C^*(\mathfrak{A}, \mathfrak{G}) \cong \Delta(\mathfrak{A}^{-1}\mathfrak{G})/\Delta(\mathfrak{G}).$$

Hieraus folgt sofort die Aussage (b) sowie

$$k^* = \dim(C^*(\mathfrak{A}, \mathfrak{G})) = \dim(\Delta(\mathfrak{A}^{-1}\mathfrak{G})) - \dim(\Delta(\mathfrak{G})) = i(\mathfrak{A}^{-1}\mathfrak{G}) - i(\mathfrak{G}).$$

Es bleibt noch die Abschätzung für die Minimaldistanz zu beweisen. Dazu seien $C^* \neq \{0\}$ und $\psi(\delta)$ ein Wort aus C^* von minimalem Hamming-Gewicht d^*. Dann gilt $\mathrm{ord}_{\mathfrak{P}}(\delta) = -1$ für genau d^* Primteiler $\mathfrak{P}$ von $\mathfrak{A}$. Ist $\mathfrak{B}$ deren Produkt, so ist δ in $\Delta(\mathfrak{B}^{-1}\mathfrak{G})$ enthalten und es folgt somit $i(\mathfrak{B}^{-1}\mathfrak{G}) = \dim(\Delta(\mathfrak{B}^{-1}\mathfrak{G})) > 0$. Also ist $\mathfrak{B}^{-1}\mathfrak{G}$ ein spezieller Divisor und folglich ist sein Grad durch $2g-2$ beschränkt. Wir erhalten schließlich

$$d^* = \deg(\mathfrak{B}) = \deg(\mathfrak{G}) - \deg(\mathfrak{B}^{-1}\mathfrak{G}) \geq \deg(\mathfrak{G}) - 2g + 2. \qquad \square$$

Zusatz 11.3 und Korollar 11.4 besitzen Analoga für duale arithmetische Codes.

Zusatz 11.9. *Es sei c der minimale Grad eines ganzen Divisors $\mathfrak{C}$, sodaß $\mathfrak{B}^{-1}\mathfrak{G}\mathfrak{C}$ für einen ganzen Teiler $\mathfrak{B}$ von $\mathfrak{A}$ ein kanonischer Divisor ist. Dann hat der Code $C^*(\mathfrak{A}, \mathfrak{G})$ die Minimaldistanz*

$$d^* = \deg(\mathfrak{G}) - 2g + 2 + c.$$

Insbesondere wird die untere Schranke in Satz 11.8 genau dann angenommen, wenn die kanonische Klasse $\mathbf{W}_{F:\mathbb{F}_q}$ von $F{:}\mathbb{F}_q$ einen Divisor der Gestalt $\mathfrak{B}^{-1}\mathfrak{G}$ mit $1|\mathfrak{B}|\mathfrak{A}$ besitzt.

Beweis. Der kanonische Divisor eines Differentials δ sus $\Delta(\mathfrak{A}^{-1}\mathfrak{G})$ hat die Form $(\delta) = \mathfrak{B}^{-1}\mathfrak{G}\mathfrak{C}$, wobei $\mathfrak{B}$ wie im Beweis von Satz 11.8 das Produkt der Primteiler $\mathfrak{P}$ von $\mathfrak{A}$ mit $\mathrm{ord}_{\mathfrak{P}}(\delta) = -1$ und $\mathfrak{C}$ ein zu $\mathfrak{A}$ fremder ganzer Divisor ist. Dann gilt für das Gewicht von $\psi(\delta)$

$$w(\psi(\delta)) = \deg(\mathfrak{B}) = \deg(\mathfrak{G}\mathfrak{C}) - 2g + 2 = \deg(\mathfrak{G}) - 2g + 2 + \deg(\mathfrak{C}).$$

Ist umgekehrt $\mathfrak{C}$ ein ganzer Divisor, für den $\mathfrak{B}^{-1}\mathfrak{G}\mathfrak{C}$ für einen Teiler $\mathfrak{B}$ von $\mathfrak{A}$ kanonisch ist, so gehören die Differentiale δ mit $(\delta) = \mathfrak{B}^{-1}\mathfrak{G}$ zu $\Delta(\mathfrak{B}^{-1}\mathfrak{G}) \subseteq \Delta(\mathfrak{A}^{-1}\mathfrak{G})$. Dies beweist die Behauptung. $\square$

Aus Satz 11.8 erhalten wir unmittelbar

Korollar 11.10. *Ist der Goppa-Divisor eines dualen arithmetischen Codes kein spezieller Divisor, so hat der Code die Dimension $i(\mathfrak{A}^{-1}\mathfrak{G})$.* $\square$

Beispiel 11.11. Wir betrachten nun das "duale Analogon" zu Beispiel 11.5. Wegen $\deg(\mathfrak{G}) = 6 > 0 = 2g_{F:\mathbb{F}_4} - 2$ hat der duale Code $C^*(\mathfrak{A}, \mathfrak{G})$ Dimension

$$k^* = i(\mathfrak{A}^{-1}\mathfrak{G}) = \dim(\mathfrak{A}^{-1}\mathfrak{G}) - \deg(\mathfrak{A}^{-1}\mathfrak{G}) + g_{F:\mathbb{F}_4} - 1 = -\deg(\mathfrak{A}^{-1}\mathfrak{G}) = 3$$

sowie Minimaldistanz

$$d^* \geq \deg(\mathfrak{G}) - 2g_{F:\mathbb{F}_4} + 2 = 6.$$

Also ist $C^*(\mathfrak{A}, \mathfrak{G})$ ein $[9, 3, d^*]_4$-Code mit Minimaldistanz 6 oder 7. Auf dieselbe Weise erhält man, daß $C^*(\mathfrak{A}, \mathfrak{Q}_i)$ für $i = 1, 2$ lineare $[9, 6, d^*]_4$-Codes mit Minimaldistanz $d^* \geq 3$ sind.

Satz 11.12. *Die Codes $C(\mathfrak{A},\mathfrak{G})$ und $C^*(\mathfrak{A},\mathfrak{G})$ sind dual zueinander.*

Beweis. Zunächst vergleichen wir die Dimensionen der Codes $C^*(\mathfrak{A},\mathfrak{G})$ und $C(\mathfrak{A},\mathfrak{G})^\perp$ und erhalten unter Verwendung des Satzes von *Riemann-Roch*

$$\begin{aligned}\dim(C^*(\mathfrak{A},\mathfrak{G})) &= i(\mathfrak{A}^{-1}\mathfrak{G}) - i(\mathfrak{G}) \\ &= \dim(\mathfrak{A}^{-1}\mathfrak{G}) - \deg(\mathfrak{A}^{-1}\mathfrak{G}) + g - 1 - (\dim(\mathfrak{G}) - \deg(\mathfrak{G}) + g - 1) \\ &= \deg(\mathfrak{A}) - \dim(\mathfrak{G}) + \dim(\mathfrak{A}^{-1}\mathfrak{G}) = n - \dim(C(\mathfrak{A},\mathfrak{G})).\end{aligned}$$

Ihre Dimensionen stimmen also überein und wir benötigen für den Beweis des Satzes lediglich eine Inklusion. Wir zeigen

$$C^*(\mathfrak{A},\mathfrak{G}) \leq C(\mathfrak{A},\mathfrak{G})^\perp.$$

Es seien x eine Funktion des Riemann-Roch-Raums $\mathcal{L}(\mathfrak{G})$ und δ ein Differential aus $\Delta(\mathfrak{A}^{-1}\mathfrak{G})$. Es ist zu zeigen, daß die zugehörigen Codewörter $\phi(x)$ und $\psi(\delta)$ orthogonal zueinander sind, d.h. daß sie die Gleichung

$$< \phi(x), \psi(\delta) >= (x(\mathfrak{P}_1), \ldots, x(\mathfrak{P}_n)) \begin{pmatrix} \mathrm{Res}_{\mathfrak{P}_1}(\delta) \\ \vdots \\ \mathrm{Res}_{\mathfrak{P}_n}(\delta) \end{pmatrix} = \sum_{\mathfrak{P}|\mathfrak{A}} x(\mathfrak{P}) \,\mathrm{Res}_{\mathfrak{P}}(\delta) = 0$$

erfüllen. Nach dem *schwachen Approximationssatz* existiert zu jedem Primdivisor $\mathfrak{P}$ von $\mathfrak{A}$ ein Element $t = t_{\mathfrak{P}}$ mit $\mathrm{ord}_{\mathfrak{P}}(t) = 1$. Bezüglich dieses sogenannten Primelementes t zu $\mathfrak{P}$ hat eine Funktion $x \in \mathcal{L}(\mathfrak{G})$ in der Komplettierung $F_{\mathfrak{P}} = \mathbb{F}_q((t))$ eine Laurententwicklung $x = \sum_{n \gg -\infty} a_n t^n$ mit Koeffizienten aus $\mathbb{F}_q$. Da $\mathfrak{P}$ kein Teiler von $\mathfrak{G}$ ist, verschwindet der Hauptteil dieser Laurententwicklung und es gilt

$$x = \sum_{n \in \mathbb{N}} a_n t^n \in \mathbb{F}_q[[t]] \qquad \text{mit } a_0 = x(\mathfrak{P}).$$

Das Differential $\delta \in \Delta(\mathfrak{A}^{-1}\mathfrak{G})$ hat bezüglich dieses Primelements t eine Darstellung $\delta = s\,dt$ mit $\mathrm{ord}_{\mathfrak{P}}(s) = \mathrm{ord}_{\mathfrak{P}}(\delta) \geq -1$. Genauer hat man

$$\delta = \left(\sum_{n \geq -1} b_n t^n \right) dt \qquad \text{mit } b_n \in \mathbb{F}_q \text{ und } b_{-1} = \mathrm{Res}_{\mathfrak{P}}(\delta).$$

Insgesamt gilt also

$$\mathrm{Res}_{\mathfrak{P}}(x\delta) = a_0 b_{-1} = x(\mathfrak{P}) \,\mathrm{Res}_{\mathfrak{P}}(\delta).$$

An zu $\mathfrak{A}$ teilerfremden Primdivisoren $\mathfrak{P}$ ist $x\delta \in \Delta(\mathfrak{A}^{-1})$ regulär mit $\mathrm{Res}_{\mathfrak{P}}(x\delta) = 0$. Mit Hilfe des *Residuensatzes* erhalten wir schließlich

$$0 \;=\; \sum_{\mathfrak{P} \in \mathbb{P}_{F:K}} \mathrm{Res}_{\mathfrak{P}}(x\delta) = \sum_{\mathfrak{P}|\mathfrak{A}} \mathrm{Res}_{\mathfrak{P}}(x\delta) = < \phi(x), \psi(\delta) > . \qquad \square$$

Aus der allgemeinen Dualitätstheorie linearer Codes (Abschnitt 2.2) folgt nun

Korollar 11.13. *Jede Erzeugermatrix von $C^*(\mathfrak{A},\mathfrak{G})$ ist eine Kontrollmatrix von $C(\mathfrak{A},\mathfrak{G})$ und umgekehrt.* $\square$

11.3 Duale Goppa-Divisoren

Satz 11.14. *Die Klasse der arithmetischen Codes ist abgeschlossen bezüglich Dualisierung. Ein dualer arithmetischer Code $C^*(\mathfrak{A},\mathfrak{G})$ kann wie folgt als arithmetischer Code konstruiert werden:*

(a) *Es gibt ein Differential $\delta \in \Delta$ mit $\mathrm{ord}_{\mathfrak{P}}(\delta) = -1$ und $\mathrm{Res}_{\mathfrak{P}}(\delta) = 1$ für alle Teiler $\mathfrak{P}$ von $\mathfrak{A}$.*

(b) *Mit $\mathfrak{G}^* := (\delta)\mathfrak{A}\mathfrak{G}^{-1}$ gilt dann $C^*(\mathfrak{A},\mathfrak{G}) = C(\mathfrak{A},\mathfrak{G}^*)$.*

Beweis. Die Aussage (a) folgt fast direkt aus dem *schwachen Approximationssatz*. Nach diesem gibt es eine Variable z, die an allen Stellen $\mathfrak{P}_1,\ldots,\mathfrak{P}_n$ Ordnung 1 besitzt. Dann ist das Differential $\delta = \frac{dz}{z}$ an diesen Stellen nicht regulär und es gilt $\mathrm{ord}_{\mathfrak{P}}(\delta) = \mathrm{ord}_{\mathfrak{P}}(z^{-1}) = -1$ sowie $\mathrm{Res}_{\mathfrak{P}}(\delta) = \mathrm{res}_{\mathfrak{P}}(z^{-1}) = 1$ für $\mathfrak{P}|\mathfrak{A}$. Der Divisor $\mathfrak{G}^*$ ist wegen

$$\mathrm{ord}_{\mathfrak{P}_i}(\mathfrak{G}^*) = \mathrm{ord}_{\mathfrak{P}_i}((\delta)\mathfrak{A}\mathfrak{G}^{-1}) = \mathrm{ord}_{\mathfrak{P}_i}(\mathfrak{G}^{-1}) = 0$$

wie $\mathfrak{G}$ fremd zu $\mathfrak{A}$ und somit ist $C(\mathfrak{A},\mathfrak{G}^*)$ ein wohldefinierter arithmetischer Code. Es bleibt also nur noch die Gültigkeit von $C^*(\mathfrak{A},\mathfrak{G}) = C(\mathfrak{A},\mathfrak{G}^*)$ nachzuweisen.
Die zum Wort $\boldsymbol{x} = (x(\mathfrak{P}_1),\ldots,x(\mathfrak{P}_n)) \in C(\mathfrak{A},\mathfrak{G}^*)$ zugehörige Funktion x ist ein Element des Raumes $\mathcal{L}(\mathfrak{G}^*)$ und besitzt den Divisor $(x) = \mathfrak{C}(\mathfrak{G}^*)^{-1} = \mathfrak{C}\mathfrak{G}(\delta)^{-1}\mathfrak{A}^{-1}$. Für den kanonischen Divisor von $x\delta$ impliziert dies $(x\delta) = (x)(\delta) = \mathfrak{C}\mathfrak{A}^{-1}\mathfrak{G}$. Damit ist $x\delta$ ein Differential aus $\Delta(\mathfrak{A}^{-1}\mathfrak{G})$. Werten wir das Residuum von $x\delta$ an den Stellen $\mathfrak{P}|\mathfrak{A}$ aus, so ergibt sich nach Definition von δ

$$\mathrm{Res}_{\mathfrak{P}}(x\delta) = x(\mathfrak{P})\,\mathrm{Res}_{\mathfrak{P}}(\delta) = x(\mathfrak{P}).$$

Also ist $C(\mathfrak{A},\mathfrak{G}^*)$ ein linearer Unterraum von $C^*(\mathfrak{A},\mathfrak{G})$ der Dimension

$$\dim(C(\mathfrak{A},\mathfrak{G}^*)) = \dim(\mathfrak{G}^*) - \dim(\mathfrak{A}^{-1}\mathfrak{G}^*) = \dim((\delta)\mathfrak{A}\mathfrak{G}^{-1}) - \dim((\delta)\mathfrak{G}^{-1}).$$

Nach dem Satz von *Riemann-Roch* gelten $\dim((\delta)\mathfrak{G}^{-1}) = i(\mathfrak{G})$ bzw. $\dim((\delta)\mathfrak{A}\mathfrak{G}^{-1}) = i(\mathfrak{A}^{-1}\mathfrak{G})$ und somit folgt

$$\dim(C(\mathfrak{A},\mathfrak{G}^*)) = i(\mathfrak{A}^{-1}\mathfrak{G})) - i(\mathfrak{G}) = \dim(C^*(\mathfrak{A},\mathfrak{G})).$$

Das zeigt $C(\mathfrak{A},\mathfrak{G}^*) = C^*(\mathfrak{A},\mathfrak{G})$. □

Korollar 11.15. *Zwischen der Restklassenauswertung und der Residuenauswertung eines arithmetischen Codes besteht folgender Zusammenhang*

$$C(\mathfrak{A},\mathfrak{G}^*) = C^*(\mathfrak{A},\mathfrak{G}) = C(\mathfrak{A},\mathfrak{G})^{\perp}.$$

Definition 11.16. (Dualer Goppa-Divisor)
Der Divisor $\mathfrak{G}^*$ in Satz 11.14(b) definiert durch $\mathfrak{G}^* := (\delta)\mathfrak{A}\mathfrak{G}^{-1}$ mit einem Differential $\delta \in \Delta_{F:K}$ mit Ordnung -1 und Residuum 1 an den Stellen $\mathfrak{P}_1,\ldots,\mathfrak{P}_n$ wird im folgenden als zu $\mathfrak{G}$ **dualer Goppa-Divisor** bezeichnet. Sind überdies sowohl $\mathfrak{G}$ als auch $\mathfrak{G}^*$ nicht-speziell, so heißen sie **normale Goppa-Divisoren**.

Korollar 11.17. *Ist der Goppa-Divisor $\mathfrak{G}$ eines arithmetischen Codes $C = C(\mathfrak{A}, \mathfrak{G})$ gleich seinem dualen Goppa-Divisors $\mathfrak{G}^*$, so ist C selbstdual.* □

Definition 11.18. (Quasiäquivalenz)
Zwei lineare Codes $C, \tilde{C} \leq \mathbb{F}_q^n$ heißen **quasiäquivalent**, falls es Elemente $c_1, \ldots, c_n$ aus $\mathbb{F}_q^\times$ und eine Permutation σ von n Elementen gibt, sodaß gilt:

$$(x_1, \ldots, x_n) \in C \Longleftrightarrow (c_1 x_{\sigma(1)}, \ldots, c_n x_{\sigma(n)}) \in \tilde{C}.$$

Anmerkung 11.19. Quasiäquivalente Codes haben dasselbe Gewichtspolynom, aber nicht notwendig dieselbe Symmetriegruppe.

Aufgabe 11.20. Zeigen Sie, daß äquivalente Goppa-Divisoren bei gleichen Auswertungsdivisor quasiäquivalente arithmetische Codes erzeugen.
Genauer: Ist $C(\mathfrak{A}, \mathfrak{G})$ ein arithmetischer Code und $\tilde{\mathfrak{G}}$ ein zu $\mathfrak{G}$ äquivalenter Divisor, so sind folgende Paare von arithmetischen Codes jeweils quasiäquivalent:

(a) $C(\mathfrak{A}, \mathfrak{G})$ und $C(\mathfrak{A}, \tilde{\mathfrak{G}})$ sowie (b) $C^*(\mathfrak{A}, \mathfrak{G})$ und $C^*(\mathfrak{A}, \tilde{\mathfrak{G}})$.

Kapitel 12

Rationale Codes und Symmetrien

12.1 Rationale Codes

Definition 12.1. (Rationaler Code)
Ein arithmetischer Code $C(\mathfrak{A}, \mathfrak{G})$ über einem Funktionenkörper einer Variablen $F{:}\mathbb{F}_q$ heißt **rational**, falls $F{:}\mathbb{F}_q$ ein rationaler Funktionenkörper ist.

Da rationale Funktionenkörper Geschlecht 0 besitzen, gilt als unmittelbare Folgerung des Korollars 11.4 die

Bemerkung 12.2. *Rationale Codes sind pseudorational.* □

Dieses Ergebnis wird auch durch die in diesen Abschnitt gelieferten expliziten Beschreibungen der rationalen Codes bestätigt.

Notiz 12.3. (a) Nach dem Satz von F.K. Schmidt [Sti93, V.1.11.] ist der kleinste positive Divisorgrad eines Kongruenzfunktionenkörpers gleich 1. Demnach sind Kongruenzfunktionenkörper vom Geschlecht $g = 0$ stets rational.
(b) Rationale Kongruenzfunktionenkörper haben die Nullklassenzahl 1 [Sti93, V.1.], d.h. zwei Divisoren sind äquivalent, sofern sie gleichen Grades sind.
(c) Die Länge eines arithmetischen Codes ist stets durch die Anzahl der rationalen Stellen, also durch $\#\mathbb{P}^{(1)}_{F:\mathbb{F}_q}$, beschränkt. Rationale Codes über $\mathbb{F}_q(t)$ haben somit höchstens die Länge $q + 1$.
(d) Hat ein rationaler Code $C(\mathfrak{A}, \mathfrak{G})$ einen Goppa-Divisor $\mathfrak{G}$ mit $\deg(\mathfrak{G}) \geq -1$, so gilt unmittelbar nach Korollar 11.4

$$\dim_{\mathbb{F}_q}(C(\mathfrak{A}, \mathfrak{G})) = \min\{\deg(\mathfrak{G}) + 1, \deg(\mathfrak{A})\}.$$

In Kapitel 3 haben wir *(verallgemeinerte)* ***Reed-Solomon-Codes*** eingeführt. Für $q \geq n \geq k \geq 0$ sind diese definiert durch

$$RS_k(\boldsymbol{a}, \boldsymbol{b}) = \{(b_1 f(a_1), \ldots, b_n f(a_n)) : f \in \mathbb{F}_q[t], \deg(f) < k\}$$

mit paarweise verschiedenen Elementen $a_1, \ldots, a_n \in \mathbb{F}_q$ und beliebigen $b_1, \ldots, b_n \in \mathbb{F}_q^\times$. Gemäß Bemerkung 3.10 haben diese Codes haben Singletondefekt 0.

Satz 12.4. (Zusammenhang zwischen Reed-Solomon-Codes und rationalen Codes)

(a) *Jeder Reed-Solomon-Code* $RS_k(\boldsymbol{a}, \boldsymbol{b})$ *über* $\mathbb{F}_q$ *ist ein rationaler Code. Dabei gilt* $RS_k(\boldsymbol{a}, \boldsymbol{b}) = C(\mathfrak{A}, \mathfrak{G})$ *mit* $\mathfrak{A} := \prod_{j=1}^{n} (t - a_j)_0$ *und* $\mathfrak{G} := (t)_\infty^{k-1}(u)^{-1}$*, wobei* $u \in \mathbb{F}_q[t]$ *ein Polynom mit* $u(a_j) = b_j$ *und* $\deg(u) < n$ *ist.*

(b) *Jeder rationale Code* $C(\mathfrak{A}, \mathfrak{G})$ *über* $\mathbb{F}_q[t]$ *mit* $0 \leq \deg(\mathfrak{G}) < n \leq q$ *ist ein Reed-Solomon-Code.*

Beweis. (a) Die Existenz eines Polynoms $u \in \mathbb{F}_q[t]$ vom Grad $\deg(u) < n$ mit $u(a_j) = b_j$ für $j = 1, \ldots, n$ folgt aus der Lagrangeschen Interpolationsformel. Wir betrachten im rationalen Kongruenzfunktionenkörper $\mathbb{F}_q(t)$:$\mathbb{F}_q$ die Divisoren $\mathfrak{P}_j := (t - a_j)_0$, $\mathfrak{A} := \prod_{j=1}^{n} \mathfrak{P}_j$ und $\mathfrak{G} := (t)_\infty^{k-1}(u)^{-1}$. Wegen $\deg(\mathfrak{A}) = n > k - 1 = \deg(\mathfrak{G}) \geq -1$ gilt für den arithmetischen Code $\tilde{C} := C(\mathfrak{A}, \mathfrak{G})$ nach Notiz 12.3(d)

$$\dim_{\mathbb{F}_q}(\tilde{C}) = \deg(\mathfrak{G}) + 1 = k.$$

Die Funktionen $u, tu, \ldots, t^{k-1}u$ bilden eine Basis des linearen Raums von $\mathfrak{G}$ und wir erhalten nach Satz 11.2 (b) $(t^i u(\mathfrak{P}_j))_{0 \leq i \leq k-1, 1 \leq j \leq n}$ als Erzeugermatrix von $\tilde{C}$. Diese Matrix erzeugt aber auch $RS_k(\boldsymbol{a}, \boldsymbol{b})$; wegen $t(\mathfrak{P}_j) = a_j$ und $u(\mathfrak{P}_j) = b_j$ gilt nämlich

$$\big(t^i u(\mathfrak{P}_j)\big)_{0 \leq i \leq k-1, 1 \leq j \leq n} = \big(a_j^i b_j\big)_{0 \leq i \leq k-1, 1 \leq j \leq n}.$$

Das zeigt die Gleichheit der Codes $RS_k(\boldsymbol{a}, \boldsymbol{b})$ und $C(\mathfrak{A}, \mathfrak{G})$.
(b) Es seien der Goppadivisor $\mathfrak{G}$ und der Auswertungsdivisor $\mathfrak{A} := \prod_{j=1}^{n} \mathfrak{P}_j$ eines rationalen Codes über $\mathbb{F}_q(t)$ der Länge $n \leq q$ gegeben. Wir setzen $k := \deg(\mathfrak{G}) + 1$ und $a_j := t(\mathfrak{P}_j)$. Die Elemente $a_1, \ldots, a_n$ sind somit paarweise verschieden. Da ein rationaler Funktionenkörper über $\mathbb{F}_q$ genau $q + 1$ rationale Stellen besitzt, gibt es einen Primdivisor $\mathfrak{P}_\infty$ vom Grad 1, der fremd zu $\mathfrak{A}$ ist. Ohne Einschränkung können wir $(t)_\infty = \mathfrak{P}_\infty$ annehmen. Der Divisor $\mathfrak{G}\mathfrak{P}_\infty^{-(k-1)}$ hat Grad 0 und Dimension 1 (nach dem Satz von *Riemann-Roch*). Somit existiert eine Funktion $u \in \mathbb{F}_q(t)$ mit Divisor $(u) = \mathfrak{P}_\infty^{k-1}\mathfrak{G}^{-1}$. Damit ist $\mathcal{L}(\mathfrak{G}) = \mathbb{F}_q\langle u, tu, \ldots, t^{k-1}u\rangle$. Wir setzen $b_j := u(\mathfrak{P}_j)$. Da $\mathfrak{G}$ fremd zu den Primdivisoren $\mathfrak{P}_j$ ist, sind $b_1, \ldots, b_n$ Elemente der multiplikativen Gruppe $\mathbb{F}_q^\times$ des endlichen Körpers $\mathbb{F}_q$. Nach Satz 11.2 ist daher die Matrix

$$\big(t^i u(\mathfrak{P}_j)\big)_{0 \leq i \leq k-1, 1 \leq j \leq n} = \big(a_j^i b_j\big)_{0 \leq i \leq k-1, 1 \leq j \leq n}$$

eine Erzeugermatrix von $C(\mathfrak{A}, \mathfrak{G})$. Gemäß der Voraussetzungen $0 \leq k \leq n \leq q$ und $b_1, \ldots, b_n \in \mathbb{F}_q^\times$ sowie $a_i \neq a_j$ für $i \neq j$ erzeugt diese Matrix aber auch einen (verallgemeinerten) Reed-Solomon-Code. □

Zusatz 12.5. *Rationale Codes über* $\mathbb{F}_q(t)$ *der Maximallänge* $q + 1$ *sind projektive Reed-Solomon-Codes.*

Beweis. Es sei ein rationaler Code $C = C(\mathfrak{A}, \mathfrak{G})$ über $\mathbb{F}_q(t)$ mit Auswertungsdivisor $\mathfrak{A} := \prod_{j=1}^{q+1} \mathfrak{P}_j$ gegeben. Da $\mathbb{F}_q^{q+1}$ ein projektiver Reed-Solomon Code ist, können wir nach Notiz 12.3(d) ohne Einschränkung $\dim_{\mathbb{F}_q}(C) = \dim(\mathfrak{G}) = \deg(\mathfrak{G}) + 1$ annehmen. Wir können ebenfalls die Erzeugende t von $\mathbb{F}_q(t)$ so normieren, daß $(t) = \mathfrak{P}_1 \mathfrak{P}_{q+1}^{-1}$ gilt. Divisoren vom Grad 0 über rationalen Funktionenkörpern sind nach dem Satz von Riemann-Roch Hauptdivisoren. Daher existiert wie schon im Beweis zu Satz 12.4 eine Funktion $u \in \mathbb{F}_q(t)$ mit $(u) = \mathfrak{P}_{q+1}^{k-1} \mathfrak{G}^{-1}$. Somit ist $\mathcal{L}(\mathfrak{G}) = \mathbb{F}_q\langle u, tu, \ldots, t^{k-1}u\rangle$. Wir definieren $a_j := t(\mathfrak{P}_j) \in \mathbb{F}_q$ und $b_j := u(\mathfrak{P}_j) \in \mathbb{F}_q^\times$ für $j = 1, \ldots, q$ sowie $c := t^{k-1}u(\mathfrak{P}_{q+1}) \in \mathbb{F}_q^\times$ (wegen $\left(t^{k-1}u\right) = \mathfrak{P}_1^{k-1}\mathfrak{G}^{-1}$). Die Elemente $a_1, \ldots, a_q$ sind paarweise verschieden und es gelten für $i \in \{0, \ldots, k-1\}$ und $j \in \{1, \ldots, q\}$

$$t^i u(\mathfrak{P}_i) = t^i(\mathfrak{P}_j) u(\mathfrak{P}_j) = a_j^i b_j \quad \text{sowie} \quad t^i u(\mathfrak{P}_{q+1}) = 0.$$

Die Erzeugermatrix von C hat somit die Gestalt

$$\begin{pmatrix} u(\mathfrak{P}_1) & \ldots & u(\mathfrak{P}_q) & u(\mathfrak{P}_{q+1}) \\ \vdots & & & \vdots \\ t^{k-2}u(\mathfrak{P}_1) & & t^{k-2}u(\mathfrak{P}_q) & t^{k-2}u(\mathfrak{P}_{q+1}) \\ t^{k-1}u(\mathfrak{P}_1) & \ldots & t^{k-1}u(\mathfrak{P}_q) & t^{k-1}u(\mathfrak{P}_{q+1}) \end{pmatrix} = \begin{pmatrix} b_1 & \ldots & b_q & 0 \\ \vdots & & \vdots & \vdots \\ a_1^{k-2}b_1 & \ldots & a_q^{k-2}b_q & 0 \\ a_1^{k-1}b_1 & \ldots & a_q^{k-1}b_q & c \end{pmatrix}$$

und ist daher nach Abschnitt 3.3 auch eine erzeugende Matrix eines projektiven Reed-Solomon-Codes. □

Anmerkung 12.6. Die Gewichtspolynome rationaler Codes erhält man durch die Gewichtspolynome von Reed-Solomon-Codes, die schon in Abschnitt 3.4 berechnet worden sind.

Die Umkehrung von Zusatz 12.5 gilt bei einer Erweiterung des Begriffs *arithmetischer Code* für nicht-fremde Divisoren $\mathfrak{A}$ und $\mathfrak{G}$.

Definition 12.7. (Quasiarithmetischer Code)
Es seien Divisoren $\mathfrak{A} := \prod_{i=1}^{n} \mathfrak{P}_i$ mit $\mathfrak{P}_i \in \mathbb{P}_{F:\mathbb{F}_q}^{(1)}$ und $\mathfrak{G}$ zu einem Kongruenzfunktionenkörper $F : \mathbb{F}_q$ gegeben. Weiterhin seien $t_i \in \mathfrak{P}_i$ Primelemente zu den Teilern $\mathfrak{P}_i$ von $\mathfrak{A}$ und $e_i := \mathrm{ord}_{\mathfrak{P}_i}(\mathfrak{G})$ die Ordnung von $\mathfrak{G}$ an diesen Stellen. Dann heißt

$$C(\mathfrak{A}, \mathfrak{G}) := \{(t_1^{e_1} x(\mathfrak{P}_1), \ldots, t_n^{e_n} x(\mathfrak{P}_n)) : x \in \mathcal{L}(\mathfrak{G})\} \leq \mathbb{F}_q^n.$$

ein **quasiarithmetischer Code**.

Anmerkung 12.8. Die Definition eines arithmetischen Codes $C(\mathfrak{A}, \mathfrak{G})$ bei nichtfremden Divisoren $\mathfrak{A}$ und $\mathfrak{G}$ ist abhängig von der Wahl der Primelemente $t_i \in \mathfrak{P}_i$. Daher sind diese quasiarithmetischen Codes nur eindeutig bis auf Quasiäquivalenz.

Aufgabe 12.9. Man zeige, daß projektive Reed-Solomon-Codes quasiarithmetische Codes über rationalen Funktionenkörpern sind.

12.2 Symmetrien arithmetischer Codes

Die Automorphismengruppe $\mathrm{Aut}(F{:}K)$ eines (allgemeinen) algebraischen Funktionenkörpers $F{:}K$ operiert auf der Divisorengruppe $\mathbb{D}_{F:K}$ via $\mathfrak{P}^\alpha = \{x^\alpha : x \in \mathfrak{P}\}$ und $(\mathfrak{P}\mathfrak{Q})^\alpha = \mathfrak{P}^\alpha\mathfrak{Q}^\alpha$ für $\alpha \in \mathrm{Aut}(F{:}K)$ und Primdivisoren $\mathfrak{P}, \mathfrak{Q} \in \mathbb{P}_{F:K}$. Tatsächlich ist mit $\mathfrak{P}$ auch $\mathfrak{P}^\alpha$ ein Primdivisor, da offensichtlich $\mathcal{O}_\mathfrak{P}^\alpha$ ein Bewertungsring von $F{:}K$ mit zugehörigem maximalen Ideal $\mathfrak{P}^\alpha$ ist. Ferner gilt $\mathfrak{P}^\alpha = t^\alpha \mathcal{O}_\mathfrak{P}^\alpha$ für ein Primelement $t \in \mathfrak{P}$, was

$$\mathrm{ord}_{\mathfrak{P}^\alpha}(x^\alpha) = \mathrm{ord}_\mathfrak{P}(x)$$

zur Folge hat. Ein Automorphismus $\alpha \in \mathrm{Aut}(F{:}K)$ induziert weiterhin eine Isomorphie zwischen den Restklassenkörpern $\mathcal{R}_\mathfrak{P} = \mathcal{O}_\mathfrak{P}/\mathfrak{P}$ und $\mathcal{R}_{\mathfrak{P}^\alpha} = \mathcal{O}_{\mathfrak{P}^\alpha}/\mathfrak{P}^\alpha$ via $z(\mathfrak{P}) \mapsto z^\alpha(\mathfrak{P}^\alpha)$. Das zeigt

$$\deg(\mathfrak{P}) = [\mathcal{R}_\mathfrak{P}{:}K] = [\mathcal{R}_{\mathfrak{P}^\alpha}{:}K] = \deg(\mathfrak{P}^\alpha)$$

sowie

$$(x)^\alpha = \left(\prod_{i=1}^{m} \mathfrak{P}_i \prod_{j=1}^{n} \mathfrak{Q}_j^{-1}\right)^\alpha = \prod_{i=1}^{m} \mathfrak{P}_i^\alpha \prod_{j=1}^{n} \left(\mathfrak{Q}_j^\alpha\right)^{-1} = (x^\alpha)\,.$$

Speziell für einen rationalen Funktionenkörper $F = K(t)$ ist $\mathrm{Aut}(F{:}K)$ isomorph zu $\mathbf{PGL}_2(K)$, da die Automorphismen von $F{:}K$ durch die Möbiustransformationen $t \mapsto \frac{at+b}{ct+d}$ mit $\det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \neq 0$ gegeben sind. Desweiteren stehen die rationalen Stellen von $F{:}K$ in Bijektion zu den projektiven Punkten aus $\mathbb{P}^{(1)}(K)$ vermöge

$$\mathfrak{P}_\infty = (x)_\infty \mapsto (0:1) \qquad \text{und} \qquad \mathfrak{P}_a = (x-a)_0 \mapsto (1:a)$$

(vgl. auch [Sti93, I.2.3.]). Da $\mathbf{PGL}_2(K)$ dreifach transitiv auf $\mathbb{P}^{(1)}(K)$ wirkt, operiert auch $\mathrm{Aut}(F{:}K)$ dreifach transitiv auf $\mathbb{P}_{F:K}^{(1)}$.

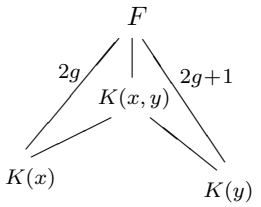
Bemerkung 12.10. *Ein Automorphismus $\alpha \in \mathrm{Aut}(F{:}K)$ eines algebraischen Funktionenkörpers $F{:}K$ ist die Identität, falls* (1) *oder* (2) *gilt.*
(1) *Alle Primdivisoren $\mathfrak{P} \in \mathbb{P}_{F:K}$ sind invariant unter α.*
(2) *Der Automorphismus α fixiert mehr als $2g_{F:K}+2$ Stellen in $\mathbb{P}_{F:K}^{(1)}$.*

Beweis. (1) Sind alle Primdivisoren invariant unter $\alpha \in \mathrm{Aut}(F{:}K)$, so gilt dies auch für alle Divisoren von $F{:}K$ und somit insbesondere für alle Hauptdivisoren, d.h. es ist $(x^\alpha) = (x)^\alpha = (x)$ für alle Funktionen $x \in F^\times$. Es gibt daher für jede Funktion $x \in F^\times$ eine nichtverschwindende Konstante $c_x \in K^\times$ mit $x^\alpha = c_x x$. Zwei Konstanten c_x, c_y zu K-linear unabhängigen Variablen x und y sind gleich, da aufgrund der Homomorphieeigenschaft von α

$$c_x x + c_y y = x^\alpha + y^\alpha = (x+y)^\alpha = c_{x+y}(x+y)$$

und somit $c_x = c_{x+y} = c_y$ gilt. Also ist α eine Streckung um eines Faktor c, d.h. es gilt $\alpha = c \cdot \mathrm{id}_{F:K}$. Wegen $\alpha|_K = \mathrm{id}_K$ ist dies aber nur für $c = 1$ möglich.

(2) Die Primstellen $\mathfrak{P}_1, \ldots, \mathfrak{P}_{2g+2}, \mathfrak{P}_\infty \in \mathbb{P}^{(1)}_{F:K}$ seien invariant unter $\alpha \in \mathrm{Aut}(F{:}K)$. Da $2g$ und $2g+1$ keine Fehlzahlen einer rationalen Stelle sind, existieren zwei Funktionen x und y aus F mit Polstellendivisoren $(x)_\infty = \mathfrak{P}_\infty^{2g}$ und $(y)_\infty = \mathfrak{P}_\infty^{2g+1}$. Dann sind die Körpergrade $[F{:}K(x)] = \deg(x)_\infty = 2g$ und $[F{:}K(y)] = \deg(y)_\infty = 2g+1$ teilerfremd. Aus der Gradformel für Körpererweiterungen folgt $F = K(x,y)$. Nach Voraussetzung gilt für die Primdivisoren $\mathfrak{P}_1, \ldots, \mathfrak{P}_{2g+2}$ wegen $x(\mathfrak{P}_i) \in K$



$$(x - x^\alpha)(\mathfrak{P}_i) = x(\mathfrak{P}_i) - x^\alpha(\mathfrak{P}_i) = x(\mathfrak{P}_i) - \left(x\left(\mathfrak{P}_i^{\alpha^{-1}}\right)\right)^\alpha = x(\mathfrak{P}_i) - (x(\mathfrak{P}_i))^\alpha = 0$$

und entsprechend $(y - y^\alpha)(\mathfrak{P}_i) = 0$. Wir nehmen nun an, daß $x \neq x^\alpha$ ist. Nach Voraussetzung hat x^α denselben Polstellendivisor wie x wegen

$$(x^\alpha)_\infty = (x)_\infty^\alpha = \left(\mathfrak{P}_\infty^{2g}\right)^\alpha = \mathfrak{P}_\infty^{2g}.$$

Also hat die Funktion $x - x^\alpha$ höchstens den Polstellengrad $2g$ (Dreiecksungleichung) bei mindestens $2g+2$ Nullstellen (nämlich $\mathfrak{P}_1, \ldots, \mathfrak{P}_{2g+2}$). Das ist ein Widerspruch, da Hauptdivisoren Grad 0 haben. Hieraus folgt $x = x^\alpha$ und in analoger Weise $y = y^\alpha$. Das zeigt $\alpha = \mathrm{id}_F$, da F von x und y erzeugt wird. □

Definition 12.11. Zu einem arithmetischen Code $C(\mathfrak{A}, \mathfrak{G})$ über $F : \mathbb{F}_q$ mit $\mathfrak{A} := \prod_{i=1}^n \mathfrak{P}_i$ definieren wir

$$\mathrm{Aut}(\mathfrak{A}, \mathfrak{G}) := \{\alpha \in \mathrm{Aut}(F{:}\mathbb{F}_q) : \mathfrak{A}^\alpha = \mathfrak{A} \text{ und } \mathfrak{G}^\alpha = \mathfrak{G}\},$$

$$\mathrm{Aut}^*(\mathfrak{A}, \mathfrak{G}) := \{\alpha \in \mathrm{Aut}(F{:}\mathbb{F}_q) : \mathfrak{A}^\alpha = \mathfrak{A} \text{ und } \mathfrak{G}^\alpha = (u)\mathfrak{G} \text{ für } u \in F \text{ mit } u(\mathfrak{P}_i) = 1\}.$$

Notiz 12.12. Wegen der Bedingung $\mathfrak{A}^\alpha = \mathfrak{A}$ permutiert ein Element α der Automorphismengruppe $\mathrm{Aut}(\mathfrak{A}, \mathfrak{G})$ bzw. $\mathrm{Aut}^*(\mathfrak{A}, \mathfrak{G})$ die Primteiler $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ des Auswertungsdivisors $\mathfrak{A}$.

Satz 12.13. (Operation der Automorphismengruppe auf dem Code)
Es sei $C(\mathfrak{A}, \mathfrak{G})$ ein arithmetischer Code über dem Kongruenzfunktionenkörper $F{:}\mathbb{F}_q$. Dann gelten

(a) $\mathrm{Aut}(\mathfrak{A}, \mathfrak{G})$ *operiert auf* $C(\mathfrak{A}, \mathfrak{G})$ *vermöge*

$$\pi : \mathrm{Aut}(\mathfrak{A}, \mathfrak{G}) \to \mathrm{Sym}(C(\mathfrak{A}, \mathfrak{G})), \quad \alpha \mapsto \pi_\alpha \text{ mit}$$

$$\pi_\alpha(\boldsymbol{x}) := (x(\mathfrak{P}_1^\alpha), \ldots, x(\mathfrak{P}_n^\alpha)) = (x(\mathfrak{P}_{\pi_\alpha(1)}), \ldots, x(\mathfrak{P}_{\pi_\alpha(n)})) \text{ für } x \in \mathcal{L}(\mathfrak{G}).$$

(b) *Unter der Voraussetzung $n > 2g_{F:\mathbb{F}_q} + 2$ ist diese Operation treu, d.h. π ist injektiv.*

Beweis. (a) Für $\alpha \in \mathrm{Aut}(\mathfrak{A}, \mathfrak{G})$ liegt mit $x \in \mathcal{L}(\mathfrak{G})$ auch das Urbild $x^{\alpha^{-1}}$ unter α in $\mathcal{L}(\mathfrak{G})$, und es gilt aufgrund $x(\mathfrak{P}_i) \in \mathbb{F}_q$ die Gleichheit $x(\mathfrak{P}_i^\alpha) = x^{\alpha^{-1}}(\mathfrak{P}_i)$. Somit ist $\pi_\alpha(\boldsymbol{x})$ ein Codewort aus $C(\mathfrak{A}, \mathfrak{G})$ und die Permutation π_α gehört zur Symmetriegruppe $\mathrm{Sym}(C(\mathfrak{A}, \mathfrak{G}))$. Also ist die Abbildung π wohldefiniert. Es bleibt ihre Homomorphie zu zeigen. Dazu benutzen wir auf der Symmetriegruppe die Verknüpfung $\pi \cdot \phi := \phi \circ \pi$, die die Gruppenstruktur von $\mathrm{Sym}(C(\mathfrak{A}, \mathfrak{G}))$ erhält. Es ist

$$\pi_{\alpha\beta}(\boldsymbol{x}) = (x(\mathfrak{P}_1^{\alpha\beta}), \ldots, x(\mathfrak{P}_n^{\alpha\beta})) = \pi_\beta((x(\mathfrak{P}_1^\alpha), \ldots, x(\mathfrak{P}_n^\alpha))) = \pi_\beta \circ \pi_\alpha(\boldsymbol{x}),$$

und damit $\pi(\alpha\beta) = \pi(\alpha) \cdot \pi(\beta)$.
(b) Es sei α ein Element aus dem Kern von π, das heißt es sei $\pi_\alpha = \mathrm{id}_{S_n}$. Dann besitzt α mehr als $2g+2$ Fixpunkte in $\mathbb{P}^{(1)}_{F:\mathbb{F}_q}$, was nach Bemerkung 12.10 (2) $\alpha = \mathrm{id}_F$ impliziert. □

12.3 Symmetrien rationaler Codes

Es sei $F = \mathbb{F}_q(t)$ ein rationaler Funktionenkörper mit endlichem Konstantenkörper $\mathbb{F}_q$. Ziel dieses Abschnittes ist der Beweis von

Satz 12.14. (Isomorphie zwischen Automorphismen- und Symmetriegruppe)
Es sei $C = C(\mathfrak{A}, \mathfrak{G})$ ein rationaler Code mit $1 \leq \deg(\mathfrak{G}) \leq \deg(\mathfrak{A}) - 3$. Dann ist die Symmetriegruppe $\mathrm{Sym}(C)$ des Codes isomorph zu $\mathrm{Aut}^*(\mathfrak{A}, \mathfrak{G})$. Ist zusätzlich der Goppadivisor $\mathfrak{G}$ ganz, so gilt $\mathrm{Sym}(C) \cong \mathrm{Aut}(\mathfrak{A}, \mathfrak{G})$.

Notiz 12.15. Die Bedingung $1 \leq \deg(\mathfrak{G}) \leq \deg(\mathfrak{A}) - 3$ aus Satz 12.14 besagt, daß C ein nichttrivialer Code ist, d.h. C ist weder der Nullcode noch besitzt er die Parameter $[n, 1, n]_q, [n, n-1, 2]_q$ oder $[n, n, 1]_q$.

Das folgende Beispiel zeigt, daß der Satz 12.14 im allgemeinen nicht gilt, falls der Goppadivisor den Grad $\deg(\mathfrak{G}) = 0$ oder $\deg(\mathfrak{G}) = n - 2$ hat.

Beispiel 12.16. Es ist $C = C(\mathfrak{A}, 1) = \mathbb{F}_q \cdot (1, \ldots, 1)$ ein trivialer rationaler $[n, 1, n]_q$-Code mit beliebigen Auswertungsdivisor. Dann ist die Symmetriegruppe des Codes C äquivalent zur Permutationsgruppe S_n. Da aber im allgemeinen $\mathrm{Aut}(F{:}\mathbb{F}_q) \cong \mathbf{PGL}_2(\mathbb{F}_q)$ nicht isomorph zu S_n ist, kann die Aussage des Satzes 12.14 nicht für $\deg(\mathfrak{G}) = 0$ gelten. Ein Gegenbeispiel für $\deg(\mathfrak{G}) = n - 2$ findet man wie folgt: Der duale arithmetische Code $C^* = C^*(\mathfrak{A}, 1)$ ist nach Satz 11.14 arithmetisch mit Goppadivisor $\mathfrak{G} = (\delta)\mathfrak{A}$ und nach Satz 11.12 dual zu C. Dann gelten $\deg(\mathfrak{G}) = \deg(\mathfrak{A}) + \deg((\delta)) = n + 2g - 2 = n - 2$ und $\mathrm{Sym}(C^*) = \mathrm{Sym}(C^\perp)$. Es ist leicht einzusehen, daß die Symmetriegruppen von C und $C^\perp$ übereinstimmen, da ein Codewort $(x_1, \ldots, x_n) \in C^\perp$ durch $\sum_{i=1}^n x_i = 0$ charakterisiert ist. Also ist auch $\mathrm{Sym}(C^*)$ isomorph zu S_n und daher gilt im allgemeinen $\mathrm{Sym}(C^*) \neq \mathrm{Aut}(\mathfrak{A}, (\delta)\mathfrak{A})$.

Dem Beweis des Satzes 12.14 stellen wir zwei Lemmata voraus.

Lemma 12.17. *Die rationalen Codes* $C(\mathfrak{A}, \mathfrak{G})$ *und* $C(\mathfrak{A}, \tilde{\mathfrak{G}})$ *mit* $0 \leq \deg(\mathfrak{G}) \leq \deg(\mathfrak{A}) - 2$ *seien identisch. Dann sind* $\mathfrak{G}$ *und* $\tilde{\mathfrak{G}}$ *äquivalent, und es existiert eine Funktion* $u \in F$ *mit Hauptdivisor* $(u) = \mathfrak{G}\tilde{\mathfrak{G}}^{-1}$ *sowie* $u(\mathfrak{P}_i) = 1$ *für alle Primteiler* $\mathfrak{P}_i$ *von* $\mathfrak{A}$.

Beweis. Nach Notiz 12.3 sind zwei Divisoren in F äquivalent, sobald sie nur den gleichen Grad haben. Dies ist für die Goppadivisoren $\mathfrak{G}$ und $\tilde{\mathfrak{G}}$ der Fall, wegen

$$\deg(\mathfrak{G}) + 1 = \dim_{\mathbb{F}_q}(C) = \dim_{\mathbb{F}_q}(\tilde{C}) = \min\{\deg(\tilde{\mathfrak{G}}) + 1, \deg(\mathfrak{A})\} = \deg(\tilde{\mathfrak{G}}) + 1,$$

wobei C und $\tilde{C}$ die Codes $C(\mathfrak{A}, \mathfrak{G})$ bzw. $C(\mathfrak{A}, \tilde{\mathfrak{G}})$ bezeichnen. Also existiert eine Funktion $u \in F$ mit Divisor $(u) = \mathfrak{G}\tilde{\mathfrak{G}}^{-1}$. Für diese gilt insbesondere $u(\mathfrak{P}_j) \in \mathbb{F}_q^\times$ für $j = 1, \ldots, n$. Dabei sei ohne Einschränkung $u(\mathfrak{P}_1) = 1$ (sonst wählen wir die Funktion $(u(\mathfrak{P}_1))^{-1} \cdot u$). Es ist nun zu zeigen, daß $u(\mathfrak{P}_j) = 1$ auch für $j = 2, \ldots, n$ gilt. Dazu betrachten wir einen ganzen Teiler $\mathfrak{B}$ von $\mathfrak{A}(\mathfrak{P}_1\mathfrak{P}_j)^{-1} = \prod_{i \neq 1,j} \mathfrak{P}_i$ vom Grad $\deg(\mathfrak{B}) = \deg(\mathfrak{G}) \leq \deg(\mathfrak{A}) - 2$. Wie oben existiert wegen der Gradgleichheit eine Funktion $x \in F$ mit $(x) = \mathfrak{B}\mathfrak{G}^{-1}$. Also hat das Produkt ux den Divisor $(ux) = \mathfrak{B}\tilde{\mathfrak{G}}^{-1}$ und liegt in $\mathcal{L}(\tilde{\mathfrak{G}})$. Wegen $C = \tilde{C}$ gibt es also eine Funktion y aus $\mathcal{L}(\mathfrak{G})$, sodaß die Codewörter $\boldsymbol{ux} = (ux(\mathfrak{P}_1), \ldots, ux(\mathfrak{P}_n))$ und $\boldsymbol{y} = (y(\mathfrak{P}_1), \ldots, y(\mathfrak{P}_n))$ übereinstimmen. Für Primteiler $\mathfrak{P}$ von $\mathfrak{B}$ ist $x(\mathfrak{P}) = 0$ und somit auch $y(\mathfrak{P}) = 0$. Wegen $u(\mathfrak{P}_1) = 1$ gilt zudem $x(\mathfrak{P}_1) = y(\mathfrak{P}_1)$. Also befindet sich die Differenzfunktion $x - y$ im trivialen linearen Raum $\mathcal{L}(\mathfrak{G}(\mathfrak{P}_1\mathfrak{B})^{-1}) = \{0\}$. Damit folgt $u(\mathfrak{P}_j) = 1$ aus:

$$0 \neq x(\mathfrak{P}_j) = y(\mathfrak{P}_j) = ux(\mathfrak{P}_j) = u(\mathfrak{P}_j)x(\mathfrak{P}_j). \qquad \square$$

Lemma 12.18. *Die rationalen Codes* $C(\mathfrak{A}, \mathfrak{G}) = \{(x(\mathfrak{P}_1), \ldots, x(\mathfrak{P}_n)) : x \in \mathcal{L}(\mathfrak{G})\}$ *und* $C(\tilde{\mathfrak{A}}, \tilde{\mathfrak{G}}) = \{(x(\tilde{\mathfrak{P}}_1), \ldots, x(\tilde{\mathfrak{P}}_n)) : x \in \mathcal{L}(\tilde{\mathfrak{G}})\}$ *mit* $1 \leq \deg(\mathfrak{G}) \leq \deg(\mathfrak{A}) - 3$ *seien identisch. Dann gibt es einen Automorphismus* $\alpha \in \mathrm{Aut}(F{:}\mathbb{F}_q)$ *mit* $\mathfrak{P}_i^\alpha = \tilde{\mathfrak{P}}_i$ *für* $i = 1, \ldots, n$.

Beweis. Wie in Abschnitt 12.2 gezeigt, operiert $\mathrm{Aut}(F{:}\mathbb{F}_q)$ dreifach transitiv auf $\mathbb{P}^{(1)}_{F:\mathbb{F}_q}$, folglich existiert ein $\alpha \in \mathrm{Aut}(F{:}\mathbb{F}_q)$, sodaß $\mathfrak{P}_i^\alpha = \tilde{\mathfrak{P}}_i$ für $i = 1, 2, 3$ gilt. Nach Bemerkung 12.10 (2) ist dieser Automorphismus sogar eindeutig. Wir setzen $\mathfrak{H} := \mathfrak{G}^\alpha$ und $\mathfrak{Q}_i := \mathfrak{P}_i^\alpha$. Es gilt mit unseren Voraussetzungen folgende Gleichheit der Codes

$$C(\mathfrak{Q}_1 \cdots \mathfrak{Q}_n, \mathfrak{H}) = C(\mathfrak{P}_1 \cdots \mathfrak{P}_n, \mathfrak{G}) = C(\tilde{\mathfrak{P}}_1 \cdots \tilde{\mathfrak{P}}_n, \tilde{\mathfrak{G}}) = C(\mathfrak{Q}_1\mathfrak{Q}_2\mathfrak{Q}_3\tilde{\mathfrak{P}}_4 \cdots \tilde{\mathfrak{P}}_n, \tilde{\mathfrak{G}}).$$

Zu zeigen ist nun, daß aus $\mathfrak{Q}_i = \tilde{\mathfrak{P}}_i$ für $i = 1, 2, 3$ auch $\mathfrak{Q}_i = \tilde{\mathfrak{P}}_i$ für $i = 4, \ldots, n$ folgt. Angenommen, es sei $\mathfrak{Q}_j \neq \tilde{\mathfrak{P}}_j$ für ein $j \geq 4$. Wir setzen $m := \deg(\mathfrak{H}) = \deg(\mathfrak{G})$ und wählen $m-1$ Indices $i_1, \ldots, i_{m-1}$ aus $\{4, \ldots, n\} \setminus \{j\}$. Dies ist möglich, da nach Voraussetzung

$$m \leq n - 3$$

gilt. Als rationaler Funktionenkörper enthält F Variablen x, y mit

$$(x) = \frac{\tilde{\mathfrak{P}}_j\mathfrak{Q}_{i_1} \cdots \mathfrak{Q}_{i_{m-1}}}{\mathfrak{H}} \qquad \text{und} \qquad (y) = \frac{\mathfrak{P}_j\mathfrak{Q}_{i_1} \cdots \mathfrak{Q}_{i_{m-1}}}{\mathfrak{H}}.$$

Nach unserer Annahme ist also die Funktion $\frac{x}{y}$ nicht-konstant. Zudem gibt es aufgrund $C(\mathfrak{Q}_1 \cdots \mathfrak{Q}_n, \mathfrak{H}) = C(\tilde{\mathfrak{P}}_1 \cdots \tilde{\mathfrak{P}}_n, \tilde{\mathfrak{G}})$ Variablen $\tilde{x}, \tilde{y} \in \mathcal{L}(\tilde{\mathfrak{G}})$ mit

$$x(\mathfrak{Q}_i) = \tilde{x}(\tilde{\mathfrak{P}}_i) \qquad \text{und} \qquad y(\mathfrak{Q}_i) = \tilde{y}(\tilde{\mathfrak{P}}_i) \qquad \text{für } i = 1, \ldots, n.$$

Die Divisoren von $\tilde{x}$ und $\tilde{y}$ haben also die Gestalt

$$(\tilde{x}) = \frac{\mathfrak{R}\tilde{\mathfrak{P}}_{i_1} \cdots \tilde{\mathfrak{P}}_{i_{m-1}}}{\tilde{\mathfrak{G}}} \qquad \text{sowie} \qquad (\tilde{y}) = \frac{\tilde{\mathfrak{P}}_j \tilde{\mathfrak{P}}_{i_1} \cdots \tilde{\mathfrak{P}}_{i_{m-1}}}{\tilde{\mathfrak{G}}}$$

mit $\mathfrak{R} \notin \{\mathfrak{Q}_1, \mathfrak{Q}_2, \mathfrak{Q}_3\}$. Wegen

$$\left(\frac{x}{y}\right) = \frac{\tilde{\mathfrak{P}}_j}{\mathfrak{Q}_j} \quad \text{und} \quad \left(\frac{\tilde{x}}{\tilde{y}}\right) = \frac{\mathfrak{R}}{\tilde{\mathfrak{P}}_j}$$

sind die Quotienten $\frac{x}{y}$ und $\frac{\tilde{x}}{\tilde{y}}$ verschieden. Somit ist mit $\frac{x}{y}$ auch die Differenz $\frac{x}{y} - \frac{\tilde{x}}{\tilde{y}} \in \mathcal{L}(\mathfrak{Q}_j \tilde{\mathfrak{P}}_j)$ eine nicht-konstante Funktion mit höchstens zwei Polstellen und mindestens drei Nullstellen, was wegen $\mathfrak{Q}_i = \mathfrak{P}_i$ für $i = 1, 2, 3$ aus

$$\left(\frac{x}{y} - \frac{\tilde{x}}{\tilde{y}}\right)(\mathfrak{Q}_i) = \frac{x(\mathfrak{Q}_i)}{y(\mathfrak{Q}_i)} - \frac{\tilde{x}(\mathfrak{Q}_i)}{\tilde{y}(\mathfrak{Q}_i)} = 0 \quad \text{für } i = 1, 2, 3$$

folgt. Dies ergibt einen Widerspruch zur Annahme $\mathfrak{Q}_j \neq \tilde{\mathfrak{P}}_j$. □

Beweis zu Satz 12.14. Den Homorphismus $\pi^* : \mathrm{Aut}^*(\mathfrak{A}, \mathfrak{G}) \to \mathrm{Sym}(C), \alpha \mapsto \pi_\alpha$ für $C := C(\mathfrak{A}, \mathfrak{G})$ definieren wir analog zu Satz 12.13, wobei die Wohldefiniertheit aus der Bedingung $u(\mathfrak{P}_i) = 1$ für $i = 1, \ldots, n$ folgt. Ein von der Identität verschiedener Automorphismus $\alpha \in \mathrm{Aut}^*(\mathfrak{A}, \mathfrak{G})$ kann nach Bemerkung 12.10 (2) nicht mehr als zwei rationale Stellen auf sich selbst abbilden, also induziert α aufgrund $\deg(\mathfrak{A}) \geq 3$ eine nichttriviale Permutation π_α in $\mathrm{Sym}(C)$. Das zeigt die Injektivität von π^*.
Für $\sigma \in \mathrm{Sym}(C)$ und $x \in \mathcal{L}(\mathfrak{G})$ bildet $(x(\mathfrak{P}_{\sigma(1)}), \ldots, x(\mathfrak{P}_{\sigma(n)}))$ ein Codewort aus C. Mit geordneter Reihenfolge der Primteiler $\mathfrak{P}_i$ haben wir demnach also die Gleichheit der Codes $C = C(\mathfrak{P}_1 \cdots \mathfrak{P}_n, \mathfrak{G}) = C(\mathfrak{P}_{\sigma(1)} \cdots \mathfrak{P}_{\sigma(n)}, \mathfrak{G})$. Nach Lemma 12.18 existiert somit ein Automorphismus $\alpha \in \mathrm{Aut}(F{:}\mathbb{F}_q)$, der die rationalen Stellen $\mathfrak{P}_i$ genauso wie σ permutiert, das heißt $\mathfrak{P}_{\sigma(i)} = \mathfrak{P}_i^\alpha$ für $i = 1, \ldots, n$. Dies impliziert die Gleichheit $\mathfrak{A}^\alpha = \mathfrak{A}$ und damit $C(\mathfrak{A}^\alpha, \mathfrak{G}^\alpha) = C(\mathfrak{A}, \mathfrak{G}) = C(\mathfrak{A}^\alpha, \mathfrak{G})$, da $x(\mathfrak{P}_i)$ invariant unter α ist. Mit Lemma 12.17 erhalten wir nun eine Funktion $u \in F$ mit Divisor $(u) = \mathfrak{G}(\mathfrak{G}^\alpha)^{-1}$ sowie $u(\mathfrak{P}_i) = 1$ für $i = 1, \ldots, n$. Also ist α ein Element aus $\mathrm{Aut}^*(\mathfrak{A}, \mathfrak{G})$ und es gilt $\pi_\alpha = \pi^*(\alpha) = \sigma$.
Für die zusätzliche Aussage betrachten wir die Funktion $u - 1$. Diese verschwindet an den Stellen $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$. Im Falle $u \neq 1$ steht dies im Widerspruch zu

$$\deg((u-1)_0) = \deg((u-1)_\infty) \leq \deg((u)_\infty) = \deg((u)_0) = \deg(\mathfrak{G}) \leq n - 3.$$

Also ist $u = 1$ und daher $\mathfrak{G}^\alpha = \mathfrak{G}$. □

Beispiel 12.19. Es seien wie bisher $F = \mathbb{F}_q(t)$ ein rationaler Funktionenkörper und

$$\mathbb{P}^{(1)}_{F:\mathbb{F}_q} = \{\mathfrak{P}_0, \mathfrak{P}_1, \ldots, \mathfrak{P}_q, \mathfrak{P}_\infty\}$$

seine rationalen Stellen mit $(t - a_i) = \mathfrak{P}_i \mathfrak{P}_\infty^{-1}$.
(a) Wir betrachten die sogenannten **Standardcodes** $C_m = C(\mathfrak{A}, \mathfrak{P}_\infty^m)$ mit Auswertungsdivisor $\mathfrak{A} = \mathfrak{P}_0 \mathfrak{P}_1 \cdots \mathfrak{P}_q$. Für $1 \leq m \leq q-3$ gilt nach Satz 12.14

$$\mathrm{Sym}(C_m) = \mathrm{Aut}(\mathfrak{A}, \mathfrak{P}_\infty^m) = \mathrm{Stab}(\mathfrak{P}_\infty).$$

Die Automorphismen aus $\mathrm{Stab}(\mathfrak{P}_\infty)$ entsprechen bijektiv den affinen Abbildungen $t \mapsto at + b$ auf $\mathbb{F}_q$ mit $a \in \mathbb{F}_q^\times$ und $b \in \mathbb{F}_q$, d.h. für einen Automorphismus $\alpha \in \mathrm{Stab}(\mathfrak{P}_\infty)$ gilt $\alpha(\mathfrak{P}_i) = \left(t - \frac{a_i + b}{a}\right)_0$. Folglich sind die Symmetriegruppen der rationalen Standardcodes für $1 \leq m \leq q-3$ allesamt gleich dem semidirekten Produkt

$$\mathrm{Sym}(C_m) = \mathbb{F}_q^+ \rtimes \mathbb{F}_q^\times \cong \mathbf{Z}_q \rtimes \mathbf{Z}_{q-1}.$$

(b) Betrachten wir nun die punktierten Standardcodes $C_m^{(0)} = C(\mathfrak{P}_1 \cdots \mathfrak{P}_q, \mathfrak{P}_\infty^m)$ für $1 \leq m \leq q-4$. Dann ist die Symmetriegruppe von $C_m^{(0)}$ isomorph zum Stabilisator von $\mathfrak{P}_0$ und $\mathfrak{P}_\infty$ in $\mathrm{Aut}(F{:}\mathbb{F}_q)$. Das sind alle Automorphismen α mit der Eigenschaft $\alpha(\mathfrak{P}_i) = (t - aa_i)_0$ für $a \in \mathbb{F}_q^\times$. Das zeigt

$$\mathrm{Sym}(C_m^{(0)}) = \mathbb{F}_q^\times \cong \mathbf{Z}_{q-1}.$$

Kapitel 13

Elliptische und hyperelliptische Codes

13.1 Elliptische Funktionenkörper und Codes

Definition 13.1. (Elliptische Funktionenkörper)
Ein algebraischer Funktionenkörper $F{:}K$ heißt **elliptisch**, falls er vom Geschlecht $g_{F:K} = 1$ ist und rationale Stellen besitzt, d.h. wenn zusätzlich $\mathbb{P}_{F:K}^{(1)} \neq \emptyset$ gilt.

Notiz 13.2. In elliptischen Funktionenkörpern stimmen Grad und Dimension von Divisoren $\mathfrak{A} \in \mathbb{D}_{F:K}$ mit Grad $\deg(\mathfrak{A}) \geq 1$ stets überein. Dies folgt aus dem Satz von *Riemann-Roch*.

Satz 13.3. (Normalform elliptischer Funktionenkörper)
Es sei $F{:}K$ ein algebraischer Funktionenkörper. Dann sind äquivalent:

(a) *$F{:}K$ ist elliptisch und besitzt eine rationale Stelle $\mathfrak{O}$.*

(b) *$F = K(x, y)$ ist eine galoissche Körpererweiterung von $K(x)$ definiert durch die Relation*

$$y^2 + a_5xy + a_3y = x^3 + a_4x^2 + a_2x + a_0,$$

wobei $(x)_\infty = \mathfrak{O}^2$ und $\bigcap_{\mathfrak{P} \neq \mathfrak{O}} \mathcal{O}_\mathfrak{P} = K[x, y]$ gelten.

Beweis. (a) $\Rightarrow$ (b): Nach dem *Lückensatz von Weierstraß* hat jede rationale Stelle von $F{:}K$ lediglich die Fehlzahl 1 und somit ist jede ganze Zahl $s > 1$ eine Polzahl von $\mathfrak{O}$. Es gibt also zwei Funktionen x_1 und y_1 aus F mit $(x_1)_\infty = \mathfrak{O}^2$ und $(y_1)_\infty = \mathfrak{O}^3$, was $F = K(x_1, y_1)$ zur Folge hat (vgl. Beweis zu Bemerkung 12.10 (2)). Es sind dann $1, x_1, y_1, x_1^2, x_1 \cdot y_1, x_1^3, y_1^2$ linear abhängig in $\mathcal{L}(\mathfrak{O}^6)$, da der Divisor $\mathfrak{O}^6$ Dimension 6 hat, d.h. es besteht eine K-Relation der Form

$$a_6y_1^2 + a_5x_1y_1 + a_3y = b_6x_1^3 + a_4x_1^2 + a_2x + a_0.$$

Es gilt $a_6, b_6 \neq 0$, da die Erweiterungen $F{:}K(x_1)$ und $F{:}K(y_1)$ Körpergrad 2 bzw. Grad 3 besitzen. Multiplizieren wir die Relation mit $a_6^3 b_6^2$ und setzen wir $y := a_6^2 b_6 y_1$ sowie $x := a_6 b_6 x_1$, so erhalten wir (mit neuen Koeffizienten a_i) die Relation aus (b). Die Erweiterung $F{:}K(x)$ ist galoissch, da $\mathrm{Gal}(F{:}K(x))$ den nichttrivialen Automorphismus $y \mapsto -(y + a_5 x + a_3), x \mapsto x$ enthält. Die Gleichheit der Ganzheitsringe $K[x,y]$ und $\bigcap_{\mathfrak{P} \neq \mathfrak{O}} \mathcal{O}_{\mathfrak{P}}$ folgt aus

$$\bigcap_{\mathfrak{P} \neq \mathfrak{O}} \mathcal{O}_{\mathfrak{P}} = \bigcup_{s \in \mathbb{N}} \mathcal{L}(\mathfrak{O}^s) = K[x] + yK[x] = K[x,y].$$

(b) $\Rightarrow$ (a): Nach Voraussetzung ist $\mathfrak{O}$ eine (in $F{:}K(x)$ total verzweigte) rationale Stelle mit $(x)_\infty = \mathfrak{O}^2$ und daher auch mit $(y)_\infty = \mathfrak{O}^3$, da aufgrund der definierenden Relation von F die Gleichungen $[F{:}K(y)] = 3$ und $\mathrm{ord}_{\mathfrak{O}}(y^2 + a_5 xy + a_3 y) = -6$ gelten. Wir müssen zeigen, daß $F{:}K$ Geschlecht 1 hat. Da 2 und 3 und damit alle natürlichen Zahlen außer 1 Polzahlen von $\mathfrak{O}$ sind, gilt nach dem Satz von Weierstraß $g_{F:K} \leq 1$. Wäre $g_{F:K} = 0$ und damit $F{:}K$ ein rationaler Funktionenkörper, so gäbe es eine Variable $t \in F$ mit Nennerdivisor $(t)_\infty = \mathfrak{O}$. Dies führte jedoch wegen $t \in \bigcap_{\mathfrak{P} \neq \mathfrak{O}} \mathcal{O}_{\mathfrak{P}}$ und $t \notin K[x,y]$ zu $\bigcap_{\mathfrak{P} \neq \mathfrak{O}} \mathcal{O}_{\mathfrak{P}} \neq K[x,y]$ im Widerspruch zur Voraussetzung. □

Bemerkung 13.4. *Es sei $F{:}K$ ein elliptischer Funktionenkörper und $\mathfrak{O} \in \mathbb{P}_{F:K}^{(1)}$ eine rationale Stelle. Dann ist die Abbildung*

$$\chi : \begin{cases} \mathbb{P}_{F:K}^{(1)} & \longrightarrow & \mathbb{C}_{F:K}^{0} \\ \mathfrak{P} & \longmapsto & \mathfrak{P}\mathfrak{O}^{-1}\mathbf{H}_{F:K} \end{cases}$$

bijektiv.

Beweis. Injektivität: Werden zwei rationale Stellen $\mathfrak{P}_1, \mathfrak{P}_2$ unter χ auf dieselbe Nullklasse abgebildet, so sind diese äquivalent. Es gibt also eine Funktion $z \in F$ mit Divisor $(z) = \mathfrak{P}_1 \mathfrak{P}_2^{-1}$. Diese ist im linearen Raum $\mathcal{L}(\mathfrak{P}_2) = K$ der Dimension $\dim(\mathfrak{P}_2) = \deg(\mathfrak{P}_2) = 1$ enthalten und somit konstant. Hieraus folgt $\mathfrak{P}_1 = \mathfrak{P}_2$.
Surjektivität: Es sei $\mathbf{C} \in \mathbb{C}_{F:K}^{0}$ eine Nullklasse und $\mathfrak{C} \in \mathbf{C}$ ein Divisor dieser Klasse. Dann ist $\dim(\mathfrak{C}\mathfrak{O}) = \deg(\mathfrak{C}\mathfrak{O}) = \deg(\mathfrak{O}) = 1$. Folglich existiert ein Element z aus dem linearen Raum von $\mathfrak{C}\mathfrak{O}$ und eine rationale Stelle $\mathfrak{P}$, sodaß $(z) = \mathfrak{P}(\mathfrak{C}\mathfrak{O})^{-1}$ bzw. $\mathfrak{C} = \mathfrak{P}\mathfrak{O}^{-1} \cdot (z^{-1})$ gilt. Dann ist $\mathfrak{P}$ das Urbild von $\mathbf{C}$ unter χ. □

Mit dieser Bijektion χ läßt sich die Gruppenstruktur von $\mathbb{C}_{F:K}^{0}$ auf $\mathbb{P}_{F:K}^{(1)}$ übertragen. Als Verknüpfung schreibt man hierfür

$$\oplus : \begin{cases} \mathbb{P}_{F:K}^{(1)} \times \mathbb{P}_{F:K}^{(1)} & \longrightarrow & \mathbb{P}_{F:K}^{(1)} \\ (\mathfrak{P}_1, \mathfrak{P}_2) & \longmapsto & \mathfrak{P}_1 \oplus \mathfrak{P}_2 \end{cases},$$

wobei $\mathfrak{P}_1 \oplus \mathfrak{P}_2$ durch $\frac{\mathfrak{P}_1 \oplus \mathfrak{P}_2}{\mathfrak{O}} \mathbf{H}_{F:K} = \frac{\mathfrak{P}_1 \mathfrak{P}_2}{\mathfrak{O}^2} \mathbf{H}_{F:K}$ definiert ist. Dies ergibt folgendes

Korollar 13.5. *Die rationalen Punkte einer elliptischen Kurve bilden eine abelsche Gruppe.* □

Definition 13.6. (Elliptischer Code)
Ein arithmetischer Code über einem elliptischen Kongruenzfunktionenkörper, also einem elliptischen Funktionenkörper mit endlichem Konstantenkörper, heißt **elliptischer Code**.

Notiz 13.7. Die Parameter eines elliptischen Codes $C{=}C(\mathfrak{A},\mathfrak{G})$ lassen sich leicht eingrenzen. Dazu werden die Aussagen aus Kapitel 1 verwendet.

(a) Entweder ist C pseudorational oder C hat die Minimaldistanz $n-k$.

(b) Ist $\mathfrak{G}$ ein Divisor der Nullklasse, so ist $k \in \{0,1\}$.

(c) Im Fall $0 < \deg(\mathfrak{G}) < n$ hat C die Dimension $k = \dim(\mathfrak{G}) = \deg(\mathfrak{G})$.

(d) $\deg(\mathfrak{G}) = n$ impliziert $n \geq k \geq n-1$.

(e) Aus $\deg(\mathfrak{G}) > n$ folgt $C = \mathbb{F}_q^{\,n}$.

Satz 13.8. (Gewichtsverteilung elliptischer Codes)
Für einen elliptischen $[n,k,d]_q$-Code $C := C(\mathfrak{A},\mathfrak{G})$ gelten:

(a) *Das erzeugende Polynom von C hat die Gestalt*

$$W_C(T) = T^n + \sum_{l=0}^{k-1} \binom{n}{l} (q^{k-l}-1)(T-1)^l + v_k(T-1)^k$$

(b) *Der Koeffizient v_k verschwindet, falls C pseudorational ist. Hat der Code Singletondefekt 1, so ist v_k gleich der Anzahl w_d der Codewörter mit Minimalgewicht:*

$$v_k = w_d = (q-1)\#M_d.$$

Dabei ist M_d die Menge aller zu $\mathfrak{G}$ äquivalenten Teiler $\mathfrak{B}$ von $\mathfrak{A}$ mit Grad $\deg(\mathfrak{B}) = n-d = k$.

Beweis. Wir verwenden die Ergebnisse der Bemerkung 2.22. Das erzeugende Polynom ist $W_C(T) = T^n + \sum_{l=0}^{n-d} v_l (T-1)^l$ mit $v_l = \binom{n}{l}(q^{k-l}-1)$ für die Indices $0 \leq l \leq d^*-1$, wobei d^* den Minimalabstand des dualen Codes $C^* = C^*(\mathfrak{A},\mathfrak{G})$ bezeichne. Der Code C^* ist nach Satz 11.14 wiederum elliptisch. Damit erfüllen C und C^* die Relationen

$$k-1 \leq n-d \leq k \qquad \text{bzw.} \qquad k^*-1 \leq n-d^* \leq k^*$$

zwischen Länge, Dimension und Minimalabstand. Hieraus ergibt sich

$$d^* \geq n-k^* = k \geq n-d,$$

was die Aussage (a) impliziert. Ist C pseudorational, so gilt $k > n-d$ und somit $v_k = 0$. Liegt allerdings Singletondefekt 1 vor, so ist $n-d=k$, und man erhält bei Koeffizientenvergleich mit $W_C(T) = \sum_{i=0}^{n} w_i T^{n-i}$ die Gleichnung $v_k = w_d$. □

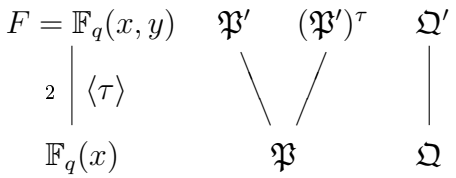
Notiz 13.9. Die Anzahl w_i der Codewörter eines Codes $C(\mathfrak{A},\mathfrak{G})$ vom Gewicht i kann allgemein wie folgt ausgerechnet werden. Es sei M_i die Menge aller Teiler $\mathfrak{B}$ von $\mathfrak{A}$ mit den Eigenschaften: Es gilt $\deg(\mathfrak{B}) = n - i$ und es gibt eine Funktion $u \in \mathcal{L}(\mathfrak{G})$, sodaß $(u)_0\mathfrak{B}^{-1}$ fremd zu $\mathfrak{A}$ und ganz ist. Dann ist $w_i = (q-1)\cdot \#M_i$.

Wie in Kapitel 3 soll ein (pseudorationaler) Code **trivial** heißen, sofern er die Parameter $[n,n,1]_q$, $[n,1,n]_q$ oder $[n,n-1,2]_q$ besitzt. Dies sind bis auf Quasiäquivalenz der gesamte Raum $\mathbb{F}_q^n$, der n-fache Wiederholungscode sowie der Parity-Check-Code. Den Nullcode zählen wir ebenfalls zu den trivialen Codes.

Satz 13.10. (Katsman-Tsfasman)
Ein nichttrivialer pseudorationaler elliptischer Code hat höchstens die Länge $q+2$.

Vorbemerkung: Es sei $M \subseteq \mathbb{P}^{(1)}_{F:\mathbb{F}_q}$ eine Menge rationaler Stellen mit Elementanzahl $\#M \geq q+2$. Dann enthält jeder lineare Raum $\mathcal{L}(\mathfrak{C})$ eines Divisors der Dimension $\dim(\mathfrak{C}) \geq 2$ eine nichtkonstante Funktion mit mindestens zwei (verschiedenen) Nullstellen aus M.
Zum Beweis dieser Bemerkung kann man sich ohne Einschränkung auf ganze Divisoren $\mathfrak{C} \in \mathbb{D}_{F:\mathbb{F}_q}$ beschränken, denn aufgrund $\dim(\mathfrak{C}) \neq 0$ ist $\mathfrak{C}$ äquivalent zu einen ganzen Divisor $\tilde{\mathfrak{C}}$ mit $\mathcal{L}(\mathfrak{C}) \cong \mathcal{L}(\tilde{\mathfrak{C}})$ [Sti93, I.4.5.]. Da $\mathfrak{C}$ mindestens Dimension 2 hat, enthält $\mathcal{L}(\mathfrak{C})$ eine nichtkonstante Funktion z. Die Abbildung $M \to \mathbb{F}_q$, $\mathfrak{R} \mapsto z(\mathfrak{R})$ ist nicht injektiv, da z an mindestens $q+2$ Stellen ausgewertet wird. Folglich gibt es zwei rationale Stellen $\mathfrak{R}_1, \mathfrak{R}_2$ mit $a := z(\mathfrak{R}_1) = z(\mathfrak{R}_2)$, und $z-a$ ist ein nichtverschwindendes Element des Raumes $\mathcal{L}(\mathfrak{C}(\mathfrak{R}_1\mathfrak{R}_2)^{-1})$.

Beweis zu Satz 13.10. Es sei $C := C(\mathfrak{A},\mathfrak{G})$ ein elliptischer Code der Länge $n := \deg(\mathfrak{A}) > q+2$ und Dimension $k \neq 0,1,n-1,n$. Der dazugehörige elliptische Kongruenzfunktionenkörper F ist eine quadratische Körpererweiterung von $\mathbb{F}_q(x)$ mit Galoisgruppe $\mathrm{Gal}(F{:}\mathbb{F}_q(x)) = \langle\tau\rangle$ (vgl. Satz 13.3). Eine rationale Stelle $\mathfrak{P}' \in \mathbb{P}^{(1)}_{F:\mathbb{F}_q}$ in F ist also entweder über einer rationalen Stelle $\mathfrak{P}$ in $\mathbb{F}_q(x)$ verzweigt mit Grad 2 oder sie erfüllt $\mathfrak{P}' \neq (\mathfrak{P}')^\tau$. Der Auswertungsdivisor von C hat somit die Gestalt



$$\mathfrak{A} = \mathfrak{P}_1\mathfrak{P}_1^\tau \cdots \mathfrak{P}_r\mathfrak{P}_r^\tau\mathfrak{Q}_1 \cdots \mathfrak{Q}_s \qquad \text{mit } 2r+s = n \geq q+3.$$

Da $\mathbb{F}_q(x)$ genau $q+1$ rationale Stellen besitzt, gelten $r+s \leq q+1$ und somit $r \geq 2$. Als Goppadivisor eines nichttrivialen Codes erfüllt $\mathfrak{G}$ die Eigenschaft $1 < k = \deg(\mathfrak{G}) = \dim(\mathfrak{G})$. Daher sei $\mathfrak{G}$ ohne Einschränkung ganz. Zudem ist C pseudorational genau dann wenn sein dualer Code C^* pseudorational ist (Bemerkung 3.4). Wegen $\dim C + \dim C^* = n$ können wir schließlich annehmen, daß $\mathfrak{G}$ ein ganzer Divisor vom Grad $\deg(\mathfrak{G}) = k \leq \frac{n}{2}$ ist.

Im folgenden werden wir einen Teiler von $\mathfrak{A}$ konstruieren, der äquivalent zu $\mathfrak{G}$ ist. In diesem Fall nimmt der Code C nach Zusatz 11.3 die untere Schranke für die Minimaldistanz an, d.h. C hat den Singletondefekt 1. Es gibt zwei Fälle:
1.Fall: Es gilt $s \geq 1$ oder C hat Dimension $k \equiv 0 \pmod 2$. Dann gilt $k-2 = 2r'+s'$ mit $s' := \max\{t \leq s : k = 2u+t\}$. Die vorausgesetzten Ungleichungen $n \geq q+3 \geq 5$ und $k \leq n/2$ implizieren $r' \leq r-2$. Der Divisor

$$\mathfrak{B} := \mathfrak{P}_1\mathfrak{P}_1^\tau \cdots \mathfrak{P}_{r'}\mathfrak{P}_{r'}^\tau \mathfrak{Q}_1 \cdots \mathfrak{Q}_{s'}$$

ist ein Teiler von $\mathfrak{A}$ vom Grad $k-2$. Somit hat $\mathfrak{B}^{-1}\mathfrak{G}$ Dimension $\dim(\mathfrak{B}^{-1}\mathfrak{G}) = 2$. Nach der Vorbemerkung erhalten wir also zwei rationale Stellen $\mathfrak{R}_1, \mathfrak{R}_2$ aus der n-elementigen Menge

$$M := \{\mathfrak{P}_1, \mathfrak{P}_1^\tau, \ldots, \mathfrak{P}_r, \mathfrak{P}_r^\tau, \mathfrak{Q}_1^\tau, \ldots, \mathfrak{Q}_{s'}^\tau \mathfrak{Q}_{s'+1}, \ldots, \mathfrak{Q}_s\},$$

sodaß $\mathfrak{G} \sim \mathfrak{B}\mathfrak{R}_1\mathfrak{R}_2$ gilt. Ist $\mathfrak{B}\mathfrak{R}_1\mathfrak{R}_2$ bereits ein Teiler von $\mathfrak{A}$, so sind wir fertig. Andernfalls gibt es paarweise verschiedene Indizes $i_1, i_2 \leq r'$ und $j_1, j_2 \leq s'$, sodaß

$$\mathfrak{R}_1 \in \{\mathfrak{P}_{i_1}, \mathfrak{P}_{i_1}^\tau\} \quad \text{oder} \quad \mathfrak{R}_1 = \mathfrak{Q}_{j_1}^\tau \tag{13.11}$$

$$\text{bzw.} \quad \mathfrak{R}_2 \in \{\mathfrak{P}_{i_2}, \mathfrak{P}_{i_2}^\tau\} \quad \text{oder} \quad \mathfrak{R}_2 = \mathfrak{Q}_{j_2}^\tau \tag{13.12}$$

gilt. Falls nötig, ersetzen wir im Fall 13.11 den Divisor $\mathfrak{B}$ durch den ganzen Divisor

$$\mathfrak{B}' := \mathfrak{B}\mathfrak{P}_{r-1}\mathfrak{P}_{r-1}^\tau(\mathfrak{P}_{i_1}\mathfrak{P}_{i_1}^\tau)^{-1} \quad \text{bzw.} \quad \mathfrak{B}' := \mathfrak{B}\mathfrak{P}_{r-1}\mathfrak{P}_{r-1}^\tau(\mathfrak{Q}_{j_1}\mathfrak{Q}_{j_1}^\tau)^{-1}$$

und im Fall 13.12 den Divisor $\mathfrak{B}'$ durch den ganzen Divisor

$$\mathfrak{B}'' := \mathfrak{B}'\mathfrak{P}_r\mathfrak{P}_r^\tau(\mathfrak{P}_{i_2}\mathfrak{P}_{i_2}^\tau)^{-1} \quad \text{bzw.} \quad \mathfrak{B}'' := \mathfrak{B}'\mathfrak{P}_r\mathfrak{P}_r^\tau(\mathfrak{Q}_{j_2}\mathfrak{Q}_{j_2}^\tau)^{-1}.$$

Wesentlich ist hier, daß $\mathfrak{P}_{r-1}, \mathfrak{P}_{r-1}^\tau, \mathfrak{P}_r$ und $\mathfrak{P}_r^\tau$ keine Teiler von $\mathfrak{B}$ sind und $\mathfrak{B}''$ daher ein Teiler von $\mathfrak{A}$ ist. Ein Divisor in F der Form $\mathfrak{P}\mathfrak{P}^\tau$ ist der Zählerdivisor $(x-a)_0$ für ein $a \in \mathbb{F}_q$. Somit sind die oben verwendeten Divisoren $\mathfrak{P}_a\mathfrak{P}_a^\tau(\mathfrak{P}_b\mathfrak{P}_b^\tau)^{-1}$ Hauptdivisoren. Dies liefert die Äquivalenzkette

$$\mathfrak{G} \sim \mathfrak{B}\mathfrak{R}_1\mathfrak{R}_2 \sim \mathfrak{B}'\mathfrak{R}_1\mathfrak{R}_2 \sim \mathfrak{B}''\mathfrak{R}_1\mathfrak{R}_2$$

zwischen $\mathfrak{G}$ und einem Teiler von $\mathfrak{A}$.
2.Fall: Es bleibt der Fall $s = 0$ und k ungerade. Dann ist $k-2 = 2r'+1$ mit $r' < r$. Wir betrachten die $(n-1)$-elementige Menge

$$M := \{\mathfrak{P}_1, \mathfrak{P}_1^\tau, \ldots, \mathfrak{P}_r, \mathfrak{P}_r^\tau\} \backslash \{\mathfrak{P}_{r'+1}\}.$$

Da $\#M = n-1 \geq q+2$ gilt, ist die Voraussetzung für die Vorbemerkung erfüllt. Der Divisor $\mathfrak{B}^{-1}\mathfrak{G}$ mit

$$\mathfrak{B} = \mathfrak{P}_1\mathfrak{P}_1^\tau \cdots \mathfrak{P}_{r'}\mathfrak{P}_{r'}^\tau \mathfrak{P}_{r'+1}$$

besitzt Dimension $\dim(\mathfrak{B}^{-1}\mathfrak{G}) = 2$. Es gibt also zwei Stellen $\mathfrak{R}_1, \mathfrak{R}_2$ aus M mit $\mathfrak{G} \sim \mathfrak{B}\mathfrak{R}_1\mathfrak{R}_2$. Entweder ist $\mathfrak{B}\mathfrak{R}_1\mathfrak{R}_2$ ein Teiler von $\mathfrak{A}$ oder es ist ohne Einschränkung $\mathfrak{R}_1 \in \{\mathfrak{P}_i, \mathfrak{P}_i^\tau\}$ mit $i \leq r'$. Falls nötig ersetzen wir $\mathfrak{B}$ durch $\mathfrak{B}' := \mathfrak{B}\mathfrak{P}_r\mathfrak{P}_r^\tau(\mathfrak{R}_1\mathfrak{R}_1^\tau)^{-1}$. Dann ist $\mathfrak{G}$ äquivalent zu $\mathfrak{B}'\mathfrak{R}_1\mathfrak{R}_2$. □

Im allgemeinen haben nichttriviale pseudorationale elliptische Codes sogar höchstens die Länge $q+1$. Eine Ausnahme bildet das folgende

Beispiel 13.13. Wir betrachten den elliptischen Kongruenzfunktionenkörper $F = \mathbb{F}_4(x,y)$ mit der definierenden Artin-Schreier Gleichung (vgl. Kapitel 18)

$$y^2 + y = x^3.$$

Anhand der Relation sieht man, daß die Polstelle $\mathfrak{O}$ von x in $F{:}\mathbb{F}_4(x)$ total verzweigt ist. Weiter ergibt sich mit dem *Dedekind Kriterium*, daß die Zählerdivisoren von $x-c$ für $c \in \mathbb{F}_4 = \{0,1,a,b\}$ zerlegt sind, d.h. es ist $(x-c)_0 = \mathfrak{P}_c\mathfrak{P}_c^\tau$, wobei τ den Erzeuger von $\mathrm{Gal}(F{:}\mathbb{F}_4(x))$ bezeichnet. Damit ist

$$\mathbb{P}^{(1)}_{F:\mathbb{F}_4} = \{\mathfrak{P}_0, \mathfrak{P}_0^\tau, \mathfrak{P}_1, \mathfrak{P}_1^\tau, \mathfrak{P}_a, \mathfrak{P}_a^\tau, \mathfrak{P}_b, \mathfrak{P}_b^\tau, \mathfrak{O}\}$$

die Menge aller rationalen Stellen in F. Diese bildet nach Bemerkung 13.4 eine abelsche Gruppe der Ordnung 9 mit neutralem Element $\mathfrak{O}$. Die Gruppenstruktur ist durch die Tafel

$\mathfrak{O}$	$\mathfrak{P}_0$	$\mathfrak{P}_0^\tau$	$\mathfrak{P}_1$	$\mathfrak{P}_1^\tau$	$\mathfrak{P}_a$	$\mathfrak{P}_a^\tau$	$\mathfrak{P}_b$	$\mathfrak{P}_b^\tau$
$\mathfrak{P}_0$	$\mathfrak{P}_0^\tau$	$\mathfrak{O}$	$\mathfrak{P}_a$	$\mathfrak{P}_b^\tau$	$\mathfrak{P}_b$	$\mathfrak{P}_1^\tau$	$\mathfrak{P}_1$	$\mathfrak{P}_a^\tau$
$\mathfrak{P}_0^\tau$		$\mathfrak{P}_0$	$\mathfrak{P}_b$	$\mathfrak{P}_a^\tau$	$\mathfrak{P}_1$	$\mathfrak{P}_b^\tau$	$\mathfrak{P}_a$	$\mathfrak{P}_1^\tau$
$\mathfrak{P}_1$			$\mathfrak{P}_1^\tau$	$\mathfrak{O}$	$\mathfrak{P}_b^\tau$	$\mathfrak{P}_0^\tau$	$\mathfrak{P}_a^\tau$	$\mathfrak{P}_0$
$\mathfrak{P}_1^\tau$				$\mathfrak{P}_1$	$\mathfrak{P}_0$	$\mathfrak{P}_b$	$\mathfrak{P}_0^\tau$	$\mathfrak{P}_a$
$\mathfrak{P}_a$					$\mathfrak{P}_a^\tau$	$\mathfrak{O}$	$\mathfrak{P}_1^\tau$	$\mathfrak{P}_0^\tau$
$\mathfrak{P}_a^\tau$						$\mathfrak{P}_a$	$\mathfrak{P}_0$	$\mathfrak{P}_1$
$\mathfrak{P}_b$							$\mathfrak{P}_b^\tau$	$\mathfrak{O}$
$\mathfrak{P}_b^\tau$								$\mathfrak{P}_b$

gegeben, wobei wir den Leser ermuntern, diese nachzurechnen.
(*Hinweis:* Die Summe $\mathfrak{P} \oplus \mathfrak{Q}$ mit $\mathfrak{P}\mathfrak{Q} \neq \mathfrak{Q}^2$ oder $\mathfrak{P}\mathfrak{Q} \neq (x-c)_0$ für alle $c \in \mathbb{F}_4$ erhält man wie folgt. Bestimmen Sie Koeffizienten $k, l \in \mathbb{F}_4$, sodaß $u = y + l \cdot x + k$ die Nullstellen $\mathfrak{P}$ und $\mathfrak{Q}$ besitzt. Dann ist u Element einer weiteren rationalen Stelle $\mathfrak{R} \neq \mathfrak{O}, \mathfrak{P}, \mathfrak{Q}$. Es folgt dann $\left(\frac{y+l\cdot x+k}{x+x(\mathfrak{R})}\right) = \mathfrak{P}\mathfrak{Q}(\mathfrak{R}^\tau\mathfrak{O})^{-1}$ und somit $\mathfrak{P} \oplus \mathfrak{Q} = \mathfrak{R}^\tau$.)
Der Code $C := C(\mathfrak{A}, \mathfrak{G})$ definiert durch

$$\mathfrak{G} := \mathfrak{P}_0\mathfrak{O}^2 \qquad \text{und} \qquad \mathfrak{A} := \mathfrak{P}_1\mathfrak{P}_1^\tau\mathfrak{P}_a\mathfrak{P}_a^\tau\mathfrak{P}_b\mathfrak{P}_b^\tau$$

ist ein nichttrivialer elliptischer $[6,3]_4$−Code mit Minimaldistanz $d = 3$ oder 4. Nach Zusatz 11.3 gilt $d = 3$ genau dann, falls ein Teiler von $\mathfrak{A}$ äquivalent zu $\mathfrak{G}$ ist. Aufgrund der Gruppenstruktur von $\mathbb{P}^{(1)}_{F:\mathbb{F}_4}$ gibt es für jeden Teiler $\mathfrak{B} = \mathfrak{Q}\mathfrak{Q}_1\mathfrak{Q}_2$ von $\mathfrak{A}$ eine rationale Stelle $\mathfrak{P}$ mit

$$\frac{\mathfrak{B}}{\mathfrak{G}} = \frac{\mathfrak{Q}\mathfrak{Q}_1\mathfrak{Q}_2}{\mathfrak{P}_0\mathfrak{O}^2} \sim \frac{\mathfrak{Q}\mathfrak{P}}{\mathfrak{P}_0\mathfrak{O}}\,.$$

Dann ist $\mathfrak{B}\mathfrak{G}^{-1}$ wegen $\mathcal{L}(\mathfrak{P}_0\mathfrak{O}) = \mathbb{F}_4\langle 1, \frac{y+1}{x}\rangle$ nur für

$$\mathfrak{P}\mathfrak{Q} \in \{\mathfrak{P}_0\mathfrak{O}, (\mathfrak{P}_0^\tau)^2, \mathfrak{P}_a^\tau\mathfrak{P}_b, \mathfrak{P}_1^\tau\mathfrak{P}_a, \mathfrak{P}_1\mathfrak{P}_b^\tau\}$$

ein Hauptdivisor. Wegen $\mathfrak{Q}|\mathfrak{A}$ ist $\mathfrak{P}\mathfrak{Q} \in \{\mathfrak{P}_0\mathfrak{O}, (\mathfrak{P}_0^\tau)^2\}$ nicht möglich. Wäre $\mathfrak{P}\mathfrak{Q} = \mathfrak{P}_a^\tau\mathfrak{P}_b$, so folgte $\mathfrak{Q}_1\mathfrak{Q}_2 = \mathfrak{P}_1\mathfrak{P}_b$ im Fall $\mathfrak{Q} = \mathfrak{P}_b$ bzw. $\mathfrak{Q}_1\mathfrak{Q}_2 = \mathfrak{P}_1^\tau\mathfrak{P}_a^\tau$ im Fall $\mathfrak{Q} = \mathfrak{P}_a^\tau$, was sich mittels der Gruppentafel von $\mathbb{P}^{(1)}_{F:\mathbb{F}_4}$ überprüfen läßt. Da aber alle Primteiler von $\mathfrak{A}$ mit einfacher Ordnung in $\mathfrak{A}$ aufgehen, ist somit $\mathfrak{P}\mathfrak{Q} \neq \mathfrak{P}_a^\tau\mathfrak{P}_b$. Analog schließt man auch die restlichen Fälle aus und es folgt dann $d = 4$ für die Minimaldistanz von C. Insbesondere ist C ist pseudorational mit Länge $q+2$. Eine Generatormatrix des Codes C ist durch

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & a & a & b & b \\ a & b & b & 0 & 0 & a \end{pmatrix}$$

gegeben, die von den Funktionen $1, x, \frac{y+1}{x} + 1$ erzeugt wird.

Die Sonderstellung dieses Beispiels belegt

Zusatz 13.14. (Munuera)
Nichttriviale pseudorationale elliptische Codes der Länge $q+2$ sind $[6,3,4]_4$-Codes.

Beweis. Wir stellen den Nachweis dieser Aussage als Übungsaufgabe 13.16. □

Die *MDS-Vermutung* (vgl. Abschnitt 3.1) ist also für die Klasse der elliptischen Codes bereits bestätigt. Im Abschnitt 13.3 beschäftigen wir uns weiter mit der *MDS-Vermutung.*

Korollar 13.15. *Ein nichttrivialer elliptischer Code über $\mathbb{F}_q$ der Länge $n \geq q+2$ hat Singletondefekt 1, sofern er nicht ein $[6,3,4]_4$-Code ist.* □

Aufgabe 13.16.

(a) Beweisen Sie Zusatz 13.14.

Hinweise: Übertragen Sie den Beweis zu Satz 13.10 für $n = q+2$ soweit es möglich ist und betrachten Sie die Ausnahmefälle. Der Beweis genügt nicht im 1.Fall, wenn $r' = r-1$ gilt. Zeigen Sie dann, daß es auch in diesen Fall keine pseudorationalen Codes gibt! Im 2.Fall gibt es nur dann pseudorationale Codes, falls $n = q+2$ gerade ist. Zeigen Sie, daß dann $k = 3$ und $q = 4$ folgen!

(b) Berechnen Sie alle elliptischen $[6,3,4]_4$-Codes bis auf Quasiäquivalenz.

13.2 Hyperelliptische Funktionenkörper

Definition 13.17. (Hyperelliptische Funktionenkörper und Divisoren)
Ein algebraischer Funktionenkörper $F{:}K$ vom Geschlecht $g_{F:K} \geq 2$ heißt **hyperelliptisch**, falls F eine quadratische Körpererweiterung eines rationalen Funktionenkörpers $K(x)$ ist. Einen Divisor nennen wir **hyperelliptisch**, wenn er Grad und Dimension 2 besitzt.

Bemerkung 13.18. (Existenz hyperelliptischer Divisoren)
Ein algebraischer Funktionenkörper $F{:}K$ vom Geschlecht $g_{F:K} \geq 2$ ist genau dann hyperelliptisch, falls er einen hyperelliptischen Divisor besitzt.

Beweis. Sei ein hyperelliptischer Divisor $\mathfrak{H}$ gegeben. Da $\mathcal{L}(\mathfrak{H})$ nicht der Nullraum ist, gibt es einen zu $\mathfrak{H}$ äquivalenten ganzen Divisor $\mathfrak{N}$ mit $\mathcal{L}(\mathfrak{N}) \cong \mathcal{L}(\mathfrak{H})$. Somit existiert eine nichtkonstante Funktion $x \in \mathcal{L}(\mathfrak{N})$ mit Poldivisor $(x)_\infty = \mathfrak{Q}|\mathfrak{N}$. Wegen $g_{F:K} \geq 2$ ist nur $\mathfrak{Q} = \mathfrak{N}$ möglich und daher ist $F{:}K(x)$ eine quadratische Erweiterung vermöge

$$[F{:}K(x)] = \deg(x)_\infty = \deg(\mathfrak{N}) = \deg(\mathfrak{H}) = 2.$$

Ist umgekehrt eine quadratische Körpererweiterung $F{:}K(x)$ gegeben, so hat der Polstellendivisor $\mathfrak{H} = (x)_\infty$ den Grad $\deg(\mathfrak{H}) = [F{:}K(x)] = 2$ und aufgrund $K\langle 1, x\rangle \leq \mathcal{L}(\mathfrak{H})$ mindestens die Dimension 2. Nach dem Satz von *Clifford* gilt zusätzlich

$$\dim(\mathfrak{H}) \leq 1 + \frac{\deg(\mathfrak{H})}{2} = 2,$$

woraus die Behauptung folgt. □

Satz 13.19. (Normalform hyperelliptischer Funktionenkörper)
Es seien $g \geq 2$ und $F{:}K$ ein algebraischer Funktionenkörper mit ungerader Charakteristik. Dann sind äquivalent:

(a) *$F{:}K$ ist hyperelliptisch mit Geschlecht g.*

(b) *Es ist $F = K(x, y)$ mit der Relation $y^2 = h(x)$, wobei das Polynom h quadratfrei ist und Grad $2g+1$ oder $2g+2$ besitzt. Insbesondere ist $F{:}K(x)$ galoissch.*

Beweis. (a) ⇒ (b): Ist $F{:}K$ hyperelliptisch, so gibt es einen ganzen Divisor $\mathfrak{H}$ mit $\deg(\mathfrak{H}) = \dim(\mathfrak{H}) = 2$ und eine Variable $x \in \mathcal{L}(\mathfrak{H})$ mit $[F{:}K(x)] = \deg(x)_\infty = \deg(\mathfrak{H}) = 2$. Die Divisoren $\mathfrak{H}^g$ und $\mathfrak{H}^{g+1}$ haben Grad $2g$ bzw. $2g+2$ und besitzen somit nach dem Satz von Riemann-Roch die Dimension

$$\begin{aligned} \dim(\mathfrak{H}^g) &= \deg(\mathfrak{H}^g) + 1 - g = g + 1 \\ \text{bzw.} \quad \dim(\mathfrak{H}^{g+1}) &= \deg(\mathfrak{H}^{g+1}) + 1 - g = g + 3. \end{aligned}$$

Es gibt somit eine Variable $y \notin K(x)$, sodaß die linearen Räume die Gestalt

$$\begin{aligned} \mathcal{L}(\mathfrak{H}^g) &= K\langle 1, x, \ldots, x^g \rangle \\ \text{bzw.} \quad \mathcal{L}(\mathfrak{H}^{g+1}) &= K\langle 1, x, \ldots, x^{g+1}, y \rangle \end{aligned}$$

haben. Wegen $K(x,y) \neq K(x)$ gilt dann $F = K(x,y)$. Die folgenden $3g+6$ Elemente

$$1, x, \ldots, x^{2g+2}, y, yx, \ldots, yx^{g+1} \text{ und } y^2$$

liegen im linearen Raum $\mathcal{L}(\mathfrak{H}^{2g+2})$. Da dessen Dimension aber lediglich $\dim(\mathfrak{H}^{2g+2}) = 3g+5$ beträgt, sind diese Elemente K-linear abhängig. Also existieren Polynome f_{g+1}, f_{2g+2} vom Grad $\deg(f_i) \leq i$ mit

$$y^2 + f_{g+1}(x)y + f_{2g+2}(x) = 0.$$

Substituiert man y durch $y - f_{g+1}(x)/2$ (was aufgrund $\mathrm{char}(F) \neq 2$ möglich ist), so erhält man ein Polynom $h \in K[T]$ vom Grad $\deg(h) \leq 2g+2$, das wegen $y \notin \mathcal{L}(\mathfrak{H}^g)$ auch $\deg(h) \geq 2g+1$ erfüllt, sodaß

$$y^2 = h(x)$$

gilt. Angenommen, das Polynom h sei nicht quadratfrei, d.h. es gelte $y^2 = q^2\tilde{h}$ mit $\deg(q) \geq 1$. Dann ist die Variable y/q gemäß

$$\mathrm{ord}_{\mathfrak{H}}(y/q) = \mathrm{ord}_{\mathfrak{H}}(y) - \mathrm{ord}_{\mathfrak{H}}(q) = g + 1 - \deg(q) \leq g$$

ein Element von $\mathcal{L}(\mathfrak{H}^g)$, was im Widerspruch zu $\mathcal{L}(\mathfrak{H}^g) \leq K[x]$ steht.
(b) $\Rightarrow$ (a): Aufgrund der Quadratfreiheit des Polynoms h ist F eine quadratische Erweiterung von $K(x)$. Außerdem folgt, daß die Primteiler des Zählerdivisors $(h(x))_0$ mit Grad 2 verzweigt sind. Nach *Dedekinds Differentensatz* bedeutet dies für den Grad der Differente $\deg(\mathfrak{D}_{F:K(x)}) \geq \deg(h(x))$. Mit der *Hurwitzschen Relativgeschlechtformel* folgt hieraus

$$\begin{aligned} g_{F:K} - 1 &= 1/2 \ \deg(\mathfrak{D}_{F:K(x)}) + [F{:}K(x)](g_{K(x):K} - 1) \\ &= 1/2 \ \deg(\mathfrak{D}_{F:K(x)}) - 2 \\ &\geq 1/2 \ \deg(h(x)) - 2 \\ &> g - 2 \end{aligned}$$

und damit $g_{F:K} \geq g \geq 2$. Somit ist $F{:}K$ hyperelliptisch. Angenommen, es sei $\tilde{g} := g_{F:K} > g$. Dann gilt $\mathcal{L}(\mathfrak{H}^{\tilde{g}}) \geq \mathcal{L}(\mathfrak{H}^{g+1})$, wobei $\mathfrak{H}$ wie oben den Polstellendivisor von x bezeichne. Es ist also y Element des linearen Raumes $\mathcal{L}(\mathfrak{H}^{\tilde{g}})$, der wegen $\dim(\mathfrak{H}^{\tilde{g}}) = \tilde{g}+1$ die Gestalt $\mathcal{L}(\mathfrak{H}^{\tilde{g}}) = K\langle 1, x, \ldots, x^{\tilde{g}} \rangle$ hat (vgl. ersten Teil des Beweises). Aus diesem Widerspruch ergibt sich $g_{F:K} = g$. □

Aufgabe 13.20. Beweisen Sie, daß für einen hyperelliptischen Funktionenkörper $F{:}K$ vom Geschlecht g gelten:

(a) Es gibt genau einen rationalen Teilkörper R mit Index $[F{:}R] = 2$ und dieser enthält jeden rationalen Teilkörper $K(z)$ mit $[F{:}K(z)] \leq g$.

(b) Es ist $R = K(x)$, wobei x ein Element des linearen Raumes $\mathcal{L}(\mathfrak{W})$ eines ganzen kanonischen Divisors $\mathfrak{W} \in \mathbf{W}_{F:K}$ ist. Man nennt R den **Quotientenkörper der ganzen Differentiale**.

Korollar 13.21. (Spezielle Divisoren hyperelliptischer Funktionenkörper)
Es seien $F{:}K$ ein hyperelliptischer Funktionenkörper vom Geschlecht g, R der dazugehörige Quotientenkörper der ganzen Differentiale, τ der zyklische Erzeuger der Galoisgruppe $\mathrm{Gal}(F{:}R)$ *und $\mathfrak{H}$ ein ganzer hyperelliptischer Divisor.*

(a) *Es sei $\mathfrak{C} = \prod_{i=1}^{s} \mathfrak{P}_i$ ein Produkt von paarweise über R nicht konjugierter Primstellen mit Trägheitsindex 1 in $F{:}R$, d.h. die Primteiler $\mathfrak{P}$ von $\mathfrak{C}$ sind entweder verzweigt oder zerlegt in $F{:}R$ und $\mathfrak{P}^\tau$ ist kein Teiler von $\mathfrak{C}\mathfrak{P}^{-1}$. Zudem sei $\mathfrak{H}$ kein Teiler von $\mathfrak{C}$. Dann hat jeder Divisor der Gestalt $\mathfrak{H}^r\mathfrak{C}$ mit $r + \deg(\mathfrak{C}) \leq g - 1$ und $r \geq 0$ die Dimension $\dim(\mathfrak{H}^r\mathfrak{C}) = r + 1$.*

(b) *Die Äquivalenzklassen der speziellen Divisoren in F besitzen Repräsentanten der Form $\mathfrak{H}^r\mathfrak{C}$ mit $r + \deg(\mathfrak{C}) \leq g - 1$ und $\mathfrak{C}$ in der Gestalt wie in* (a).

Beweis. (a) Es ist $\mathcal{L}(\mathfrak{H}) = K\langle 1, x\rangle$ und $\mathcal{L}(\mathfrak{H}^g) = K\langle 1, x, \ldots, x^g\rangle$ wie im Beweis zu Satz 13.19. Also gilt

$$\mathcal{L}(\mathfrak{H}^r) = K\langle 1, x, \ldots, x^r\rangle \leq K[x] \qquad \text{für } 1 \leq r \leq g.$$

Für einen Primdivisor $\mathfrak{P} \in \mathbb{P}_{F:K}$ vom Grad s ist $\mathfrak{P}\mathfrak{P}^\tau\mathfrak{H}^{-s}$ der Hauptdivisor eines Polynoms in x. Folglich ist $\mathfrak{C}\mathfrak{C}^\tau$ äquivalent zu $\mathfrak{H}^{\deg(\mathfrak{C})}$ und es bezeichne $f(x)$ die Funktion aus R mit Divisor $\mathfrak{C}\mathfrak{C}^\tau\mathfrak{H}^{-\deg(\mathfrak{C})}$. Es gilt daher

$$\mathcal{L}(\mathfrak{H}^r\mathfrak{C}) \leq \mathcal{L}(\mathfrak{H}^r\mathfrak{C}\mathfrak{C}^\tau) \cong \mathcal{L}(\mathfrak{H}^{r+\deg(\mathfrak{C})}) \leq K[x],$$

wobei die letzte Inklusion aus $r+\deg(\mathfrak{C}) \leq g-1$ folgt. Für eine Funktion $z \in \mathcal{L}(\mathfrak{H}^r\mathfrak{C})$ ist $z \cdot f(x)$ also ein Polynom in $\mathcal{L}(\mathfrak{H}^{r+\deg(\mathfrak{C})}) \leq K[x]$. Somit ist z eine rationale Funktion in x. Aufgrund seiner Gestalt besitzt der Divisor $\mathfrak{C}$ allerdings keine Teiler des Polstellendivisors von z und folglich enthält $\mathcal{L}(\mathfrak{H}^r\mathfrak{C})$ ausschließlich Polynome und $\mathcal{L}(\mathfrak{H}^r\mathfrak{C})\backslash\mathcal{L}(\mathfrak{H}^r)$ ist leer. Das zeigt $\dim(\mathfrak{H}^r\mathfrak{C}) = r + 1$.

(b) Es sei $\mathfrak{S}$ ein ganzer spezieller Divisor. Abgesehen vom Teiler $\mathfrak{H}^s$ mit $s = \mathrm{ord}_{\mathfrak{H}}(\mathfrak{S})$ läßt sich $\mathfrak{S}$ in drei Faktoren $\mathfrak{A}, \mathfrak{B}$ und $\mathfrak{C}$ zerlegen, wobei $\mathfrak{A} = \prod \mathfrak{P}_i\mathfrak{P}_i^\tau$ das Produkt von in $F{:}R$ verzweigter oder zerlegter und $\mathfrak{B} = \prod \mathfrak{R}_i$ das Produkt von in $F{:}R$ träger Primstellen sei. Es gelten

$$\mathfrak{P}_i\mathfrak{P}_i^\tau \sim \mathfrak{H}^{\deg(\mathfrak{P}_i)} \qquad \text{und} \qquad \mathfrak{R}_i \sim \mathfrak{H}^{\frac{1}{2}\deg(\mathfrak{R}_i)}.$$

Der Divisor $\mathfrak{C}$ habe die Gestalt wie in (a). Der spezielle Divisor $\mathfrak{S}$ ist also äquivalent zu $\mathfrak{H}^r\mathfrak{C}$ mit $r = s + \frac{1}{2}\deg(\mathfrak{A}\mathfrak{B})$.

Im Fall $\deg(\mathfrak{S}) \leq g-1$ ist offensichtlich $r + \deg(\mathfrak{C}) \leq g-1$ erfüllt. Andernfalls ist $\deg(\mathfrak{S}) \geq g$ und $\dim(\mathfrak{S}) > 0$. Aufgrund $\deg(\mathfrak{H}^{g-1}) = 2g-2$ und $\dim(\mathfrak{H}^{g-1}) = g$ ist $\mathfrak{H}^{g-1}$ ein kanonischer Divisor und es folgt nach dem Satz von *Riemann-Roch*

$$\dim(\mathfrak{H}^{g-1}\mathfrak{S}^{-1}) = i(\mathfrak{S}) > 0.$$

Die Äquivalenzklasse von $\mathfrak{H}^{g-1}\mathfrak{S}^{-1}$ mit Grad $\deg(\mathfrak{H}^{g-1}\mathfrak{S}^{-1}) \leq g-1$ enthält also einen ganzen Divisor $\tilde{\mathfrak{S}}$ (vgl. [Sti93, I.4.5.]), der natürlich ebenfalls speziell ist. Nach dem bereits Bewiesenen erhalten wir somit die Äquivalenzkette

$$\mathfrak{H}^{g-1}\mathfrak{S}^{-1} \sim \tilde{\mathfrak{S}} \sim \mathfrak{H}^{\tilde{r}}\tilde{\mathfrak{C}},$$

wobei $\tilde{r} + \deg(\tilde{\mathfrak{C}}) \leq g-1$ gilt. Das zeigt schließlich

$$\mathfrak{S} \sim \frac{\mathfrak{H}^{g-1}\tilde{\mathfrak{C}}^{\tau}}{\mathfrak{H}^{\tilde{r}}\tilde{\mathfrak{C}}\tilde{\mathfrak{C}}^{\tau}} \sim \mathfrak{H}^{g-1-(\tilde{r}+\deg(\tilde{\mathfrak{C}}))}\tilde{\mathfrak{C}}^{\tau}$$

mit $g-1-(\tilde{r}+\deg(\tilde{\mathfrak{C}})) + \deg(\tilde{\mathfrak{C}}^{\tau}) = g-1-\tilde{r} \leq g-1$. □

13.3 Hyperelliptische Codes

Definition 13.22. (Hyperelliptischer Code)
Ein arithmetischer Code über einem hyperelliptischen Kongruenzfunktionenkörper heißt **hyperelliptischer Code**.

Notiz 13.23. Für einen hyperelliptischen $[n,k,d]_q$-Code $C = C(\mathfrak{A},\mathfrak{G})$ mit $\deg(\mathfrak{G}) < \deg(\mathfrak{A})$ gelten:

(a) Die Länge des Codes ist höchstens $\min\{2q+2, q+1+2g\sqrt{q}\}$.

(b) C hat Dimension $k = \dim(\mathfrak{G})$ und es gelten die Schranken

$$\deg(\mathfrak{G}) - g + 1 \leq k \leq \deg(\mathfrak{G}) + 1.$$

(c) Der Minimalabstand d ist durch

$$n-k+1-g \leq d \leq n-k+1$$

beschränkt.

Die Teile (b) und (c) wiederholen lediglich die Ergebnisse des 1. Kapitels. Für Teil (a) betrachtet man die Schranken für die Anzahl $\#\mathbb{P}^{(1)}_{F:K}$ der rationalen Stellen im zugrunde liegenden hyperelliptischen Funktionenkörper $F{:}K$ und damit für den Grad eines Auswertungsdivisors. Einerseits gilt die *Hasse-Weil-Schranke* $q+1+2g\sqrt{q}$. Andererseits ist F eine quadratische Erweiterung eines rationalen Funktionenkörpers R, das heißt $\#\mathbb{P}^{(1)}_{F:K}$ ist durch $2(q+1)$ beschränkt (vgl. auch Beweis zu Satz 13.10).

Satz 13.24. (Reiter) *Die Länge eines nichttrivialen pseudorationalen hyperelliptischen Codes beträgt höchstens $q+2$. Ist der Goppadivisor speziell, so ist die Länge sogar durch $q+1$ beschränkt.*

Vorbemerkung: Es seien $C = C(\mathfrak{A}, \mathfrak{G})$ ein arithmetischer Code und k seine Dimension. Besitzt $\mathfrak{A}$ einen Teiler $\mathfrak{B}$ vom Grad k mit

$$\dim(\mathfrak{B}^{-1}\mathfrak{G}) > \dim(\mathfrak{A}^{-1}\mathfrak{G}),$$

so gibt es eine Funktion x aus $\mathcal{L}(\mathfrak{B}^{-1}\mathfrak{G})\backslash\mathcal{L}(\mathfrak{A}^{-1}\mathfrak{G})$. Das zugehörige Codewort $\boldsymbol{x}$ hat Gewicht $w(\boldsymbol{x}) \leq n-k$. Also ist der Code C in diesen Fall nicht pseudorational.

Beweis zu Satz 13.24. Es sei C ein nichttrivialer, hyperelliptischer Code mit Auswertungsdivisor $\mathfrak{A} = \prod_{i=1}^{n} \mathfrak{P}_i$. Weiter seien F der zugehörige hyperelliptische Funktionenkörper, R der Quotientenkörper der ganzen Differentiale mit $[F{:}R] = 2$ und $\mathrm{Gal}(F{:}R) = \{\mathrm{id}, \tau\}$ sowie $\mathfrak{H}$ ein ganzer hyperelliptischer Divisor.

Wir nehmen zunächst an, daß C einen speziellen Goppadivisor $\mathfrak{G}$ mit Dimension $r+1$ besitzt. Da C kein trivialer Code ist, gilt $r \geq 0$. Nach Korollar 13.21 ist also $\mathfrak{G}$ äquivalent zum Divisor $\mathfrak{H}^r\mathfrak{C}$, wobei $\mathfrak{C}$ ein Produkt von paarweise über R nicht konjugierter Primdivisoren mit Trägheitsindex 1 in $F{:}R$ ist. Wir nehmen weiterhin an, daß C mindestens Länge $q+2$ hat. Da F eine galoissche Erweiterung von R ist, sind wenigstens zwei Primteiler des Auswertungsdivisors $\mathfrak{A}$ zueinander konjugiert. O.E. gilt also $\mathfrak{P}_2 = \mathfrak{P}_1^{\tau}$ (mit $\mathfrak{P}_1 \neq \mathfrak{P}_2$). Der Divisor $\mathfrak{P}_1\mathfrak{P}_2\mathfrak{H}^{-1}$ ist der Hauptdivisor einer Funktion aus R. Es gilt somit die Äquivalenzkette $\mathfrak{G} \sim \mathfrak{H}^r\mathfrak{C} \sim \mathfrak{H}^{r-1}\mathfrak{C}\mathfrak{P}_1\mathfrak{P}_2$. Wegen

$$\dim(\mathfrak{G}) = \dim(\mathfrak{H}^r\mathfrak{C}) = 1 + \dim(\mathfrak{H}^{r-1}\mathfrak{C}) = 1 + \dim(\mathfrak{P}_1^{-1}\mathfrak{P}_2^{-1}\mathfrak{G})$$

und

$$\dim(\mathfrak{P}_1^{-1}\cdots\mathfrak{P}_k^{-1}\mathfrak{G}) \geq \dim(\mathfrak{P}_1^{-1}\mathfrak{P}_2^{-1}\mathfrak{G}) - (k-2) = \dim(\mathfrak{G}) - (k-1) > \dim(\mathfrak{A}^{-1}\mathfrak{G})$$

ist die Voraussetzung der Vorbemerkung erfüllt. Also ist der hyperelliptische Code $C(\mathfrak{A}, \mathfrak{G})$ mit speziellen Goppadivisor $\mathfrak{G}$ allenfalls dann pseudorational, falls er höchstens Länge $q+1$ hat.

Nun wenden wir uns dem Fall eines nicht-speziellen Goppadivisors $\mathfrak{G}$ zu. Wir nehmen an, C habe die Länge $n \geq q+3$. Wie wir wissen, ist $C = C(\mathfrak{A}, \mathfrak{G})$ genau dann pseudorational, wenn der duale Code $C^*(\mathfrak{A}, \mathfrak{G}) = C(\mathfrak{A}, \mathfrak{G}^*)$ pseudorational ist. Nach dem bisher gezeigten können $C(\mathfrak{A}, \mathfrak{G})$ und $C(\mathfrak{A}, \mathfrak{G}^*)$ nur dann pseudorational sein, wenn $\mathfrak{G}$ und $\mathfrak{G}^* = (\delta)\mathfrak{A}\mathfrak{G}^{-1}$ nicht speziell (d.h. normale Goppa-Divisoren) sind. Wir nehmen diesen Fall an. Es gilt dann $\dim(\mathfrak{A}^{-1}\mathfrak{G}) = \dim((\delta)(\mathfrak{G}^*)^{-1}) = i(\mathfrak{G}^*) = 0$, d.h. der Code $C(\mathfrak{A}, \mathfrak{G})$ hat Dimension

$$k = \dim(\mathfrak{G}) = \deg(\mathfrak{G}) - g + 1$$

nach Satz 11.2 und dem Satz von *Riemann-Roch*. Nun verläuft der Beweis völlig analog zum Beweis im elliptischen Fall (Satz 13.10) mit einer Ausnahme. Bei der Definition des Teilers $\mathfrak{B}$ von $\mathfrak{A}$ im ersten Fall gilt nun in allgemeinen nicht mehr $\dim(\mathfrak{B}^{-1}\mathfrak{G}) = 2$. Für den problemlosen Übertrag des Beweises ist also noch der Nachweis für $\dim(\mathfrak{B}^{-1}\mathfrak{G}) \geq 2$ im hyperelliptischen Fall zu erbringen.
Der Divisor $\mathfrak{B}$ hat nach Definition Grad $k-2$. Somit gilt nach obigem für den Quotienten $\mathfrak{B}^{-1}\mathfrak{G}$

$$\deg(\mathfrak{B}^{-1}\mathfrak{G}) = \deg(\mathfrak{G}) - (k-2) = \dim(\mathfrak{G}) + g - 1 - k + 2 = g + 1.$$

Hieraus folgt für die Dimension dieses Divisors nach dem Satz von Riemann-Roch

$$\dim(\mathfrak{B}^{-1}\mathfrak{G}) \geq \deg(\mathfrak{B}^{-1}\mathfrak{G}) - g + 1 = 2. \qquad \square$$

Die *MDS-Vermutung* scheint also auch für die Klasse der hyperelliptischen Codes zu gelten, wobei noch auszuschließen ist, daß es hyperelliptische pseudorationale Codes der Länge $q+2$ geben kann. Die "nächsthöhere" Klasse von Codes erhält man über **trigonalen Funktionenkörper**. Diese Funktionenkörper haben mindestens Geschlecht 3 und besitzen einen rationalen Teilkörper vom Index 3. Es ist also eine naheliegende und offene Fragestellung, ob sich die *MDS-Vermutung* auch für die Klasse der trigonalen Codes beweisen läßt. Eine umfassende Charakterisierung von trigonalen Funktionenkörpern und deren Standardcodes (sowie der hyperelliptischen Standardcodes) findet man in der Diplomarbeit von Daniel Bierbrauer [Bie06].

Beispiel 13.25. Den (elliptischen) $[6,3,4]_4-$Code aus Beispiel 13.13 erhalten wir auch als hyperelliptischen Code. Dazu betrachten wir den hyperelliptischen Funktionenkörper $F = \mathbb{F}_4(x,y)$ mit der Artin-Schreier Gleichung

$$y^2 + y = x^5 + x^3 + x = x(x+a)^2(x+b)^2.$$

Nur der Nennerdivisor von x ist in $F{:}\mathbb{F}_4(x)$ verzweigt und es gilt $d_{\mathfrak{O}}(F{:}\mathbb{F}_4(x)) = 6$ für seinen Differentenexponenten (vgl. 18.2). Daher hat F das Geschlecht 2. Desweiteren besitzt die Artin-Schreier Gleichung die rationalen Punkte

$$\begin{array}{rccccccc}
(x,y) = & (0,0) & \leftrightarrow & \mathfrak{P}_0, & (0,1) & \leftrightarrow & \mathfrak{P}_0^\tau \\
& (1,a) & \leftrightarrow & \mathfrak{P}_1, & (1,b) & \leftrightarrow & \mathfrak{P}_1^\tau \\
& (a,0) & \leftrightarrow & \mathfrak{P}_a, & (a,1) & \leftrightarrow & \mathfrak{P}_a^\tau \\
& (b,0) & \leftrightarrow & \mathfrak{P}_b, & (b,1) & \leftrightarrow & \mathfrak{P}_b^\tau.
\end{array}$$

(Auch hier bezeichne τ den zyklischen Erzeuger von $\mathrm{Gal}(F{:}\mathbb{F}_4(x))$.) Folglich besitzt auch dieser Funktionenkörper 9 rationale Stellen gegeben durch

$$\mathbb{P}^{(1)}_{F:\mathbb{F}_4} = \{\mathfrak{P}_0, \mathfrak{P}_0^\tau, \mathfrak{P}_1, \mathfrak{P}_1^\tau, \mathfrak{P}_a, \mathfrak{P}_a^\tau, \mathfrak{P}_b, \mathfrak{P}_b^\tau, \mathfrak{O}\}.$$

Durch $C := C(\mathfrak{A}, \mathfrak{G})$ mit

$$\mathfrak{G} := \mathfrak{P}_0\mathfrak{O}^3 \qquad \text{und} \qquad \mathfrak{A} := \mathfrak{P}_1\mathfrak{P}_1^\tau\mathfrak{P}_a\mathfrak{P}_a^\tau\mathfrak{P}_b\mathfrak{P}_b^\tau$$

ist dann ein pseudorationaler $[6,3,4]_4-$Code definiert. Wie in Beispiel 13.13 gilt

$$\mathcal{L}(\mathfrak{G}) = \mathbb{F}_4 \left\langle 1, \frac{1}{x}, \frac{y+1}{x} \right\rangle .$$

Der Code C besitzt die Erzeugermatrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & b & b & a & a \\ b & a & b & 0 & a & 0 \end{pmatrix} .$$

Man weist ohne Mühe nach, daß dieser Code zu dem in Beispiel 13.13 äquivalent ist.

Aufgabe 13.26. Zeigen Sie, daß man über die folgenden Konstruktionen hyperelliptische MDS-Codes erhält:

(a) Es sei $F = \mathbb{F}_5(x,y)$ durch $y^2 = x^5 - x + 1$ definiert. Den rationalen Punkten (x,y) dieser Gleichung seien wie folgt die rationalen Stellen $\mathfrak{P}_0, \ldots, \mathfrak{P}_4$ von F zugeordnet:

$$\mathfrak{P}_0 \leftrightarrow (0,1),\ \mathfrak{P}_1 \leftrightarrow (1,1),\ \mathfrak{P}_2 \leftrightarrow (2,1),\ \mathfrak{P}_3 \leftrightarrow (3,1), \mathfrak{P}_4 \leftrightarrow (4,1).$$

Desweiteren sei $\tau : x \mapsto x, \mapsto -y$ der zyklische Erzeuger von $\mathrm{Gal}(F{:}\mathbb{F}_5(x))$. Zeigen Sie, daß $C(\mathfrak{A}, \mathfrak{G})$ mit

$$\mathfrak{A} := \mathfrak{P}_2\mathfrak{P}_2^\tau\mathfrak{P}_3\mathfrak{P}_3^\tau\mathfrak{P}_4\mathfrak{P}_4^\tau \quad \text{und} \quad \mathfrak{G} := \mathfrak{P}_0\mathfrak{P}_1\mathfrak{O}^2$$

ein $[6,3,4]_5-$Code ist.

(b) Es sei $F = \mathbb{F}_7(x,y)$ mit $y^2 = x^5 - x^3 + x^2 + 1$ gegeben. Ordnen Sie wie in Aufgabenteil (a) den rationalen Punkten dieser Gleichung den rationalen Stellen von F zu und zeigen Sie:

Der quasi-arithmetische Code $C(\mathfrak{A}, \mathfrak{G})$ mit

$$\mathfrak{A} := \mathfrak{P}_0\mathfrak{P}_0^\tau\mathfrak{P}_2\mathfrak{P}_2^\tau\mathfrak{P}_4\mathfrak{P}_4^\tau\mathfrak{P}_5\mathfrak{P}_5^\tau \quad \text{und} \quad \mathfrak{G} := \mathfrak{P}_0\mathfrak{P}_1\mathfrak{P}_3\mathfrak{O}^2$$

ist ein hyperelliptischer $[8,3,6]_7-$Code.

Kapitel 14

Selbstduale arithmetische Codes

14.1 Quasiselbstduale Codes

Definition 14.1. (Quasiselbstdualer Code)
Ein Code $C \leq \mathbb{F}_q^n$ heißt **quasiselbstdual**, falls für einen Vektor $\boldsymbol{a} \in (\mathbb{F}_q^\times)^n$ gilt:

$$C^\perp = \boldsymbol{a} \times C = \{(a_1 c_1, \ldots, a_n c_n) : \boldsymbol{c} \in C\}.$$

Satz 14.2. (Kriterium für Quasiselbstdualität)
Es sei $C = C(\mathfrak{A}, \mathfrak{G})$ ein arithmetischer Code über $F{:}\mathbb{F}_q$ der Länge $n > 2g_{F:\mathbb{F}_q} - 2$. Weiter sei der Quotient $\mathfrak{A}^{-1}\mathfrak{G}^2$ ein kanonischer Divisor, d.h. es gibt ein Differential δ mit Divisor $(\delta) = \mathfrak{A}^{-1}\mathfrak{G}^2$. Dann ist C quasiselbstdual, und es gilt

$$C^\perp = (\mathrm{Res}_{\mathfrak{P}_1}(\delta), \ldots, \mathrm{Res}_{\mathfrak{P}_n}(\delta)) \times C.$$

Insbesondere ist C selbstdual, falls δ Residuum 1 bei allen Primteilern von $\mathfrak{A}$ hat.

Beweis. Es bezeichne g das Geschlecht von $F{:}\mathbb{F}_q$. Als Element der kanonischen Klasse $\mathbf{W}_{F:\mathbb{F}_q}$ hat $\mathfrak{A}^{-1}\mathfrak{G}^2$ den Grad $2g-2$. Wegen $n > 2g-2$ bedeutet dies für den Grad des Goppadivisors

$$2g - 2 < \deg(\mathfrak{G}) = g - 1 + \frac{n}{2} < n.$$

Insbesondere ist $\mathfrak{G}$ ein normaler Goppa-Divisor. Die Dimension des Codes ist somit

$$\dim(C) = \dim(\mathfrak{G}) = \deg(\mathfrak{G}) - (g-1) = \frac{n}{2}.$$

Nach Voraussetzung gilt $(\delta) = \mathfrak{A}^{-1}\mathfrak{G}^2$. Aufgrund von $\mathrm{ord}_{\mathfrak{P}}(\delta) = \mathrm{ord}_{\mathfrak{P}}(\mathfrak{A}^{-1}\mathfrak{G}^2) = -1$ ist $\mathrm{Res}_{\mathfrak{P}}(\delta) \neq 0$ für jeden Teiler $\mathfrak{P}$ von $\mathfrak{A}$. Der Vektor $\boldsymbol{a} := (\mathrm{Res}_{\mathfrak{P}_1}(\delta), \ldots, \mathrm{Res}_{\mathfrak{P}_n}(\delta))$ ist also in $(\mathbb{F}_q^\times)^n$ enthalten. Für zwei Variablen $x, y \in \mathcal{L}(\mathfrak{G})$ ist $xy\delta$ ein Differential aus $\Delta(\mathfrak{A}^{-1})$ und es folgt nach dem *Residuensatz*

$$< \boldsymbol{a} \times \boldsymbol{x}, \boldsymbol{y} >= \sum_{\mathfrak{P}|\mathfrak{A}} \mathrm{Res}_{\mathfrak{P}}(\delta) x(\mathfrak{P}) y(\mathfrak{P}) = \sum_{\mathfrak{P} \in \mathbb{P}_{F:\mathbb{F}_q}} \mathrm{Res}_{\mathfrak{P}}(xy\delta) = 0.$$

Es ist also $\boldsymbol{a} \times C$ ist ein Untercode des dualen Codes $C^\perp$. Aus Dimensionsgründen folgt schließlich $\boldsymbol{a} \times C = C^\perp$. □

Das folgende Beispiel zeigt, daß Selbstdualität auch ohne die Voraussetzungen in Satz 14.2 auftreten kann.

Beispiel 14.3. Wir betrachten erneut den elliptischen Kongruenzfunktionenkörper $F = \mathbb{F}_4(x, y)$ aus Beispiel 13.13 mit der definierenden Artin-Schreier Relation

$$y^2 + y = x^3.$$

Es ist dann $g_{F:\mathbb{F}_4} = 1$ und

$$\mathbb{P}^{(1)}_{F:\mathbb{F}_4} = \{\mathfrak{P}_0, \mathfrak{P}_0^\tau, \mathfrak{P}_1, \mathfrak{P}_1^\tau, \mathfrak{P}_a, \mathfrak{P}_a^\tau, \mathfrak{P}_b, \mathfrak{P}_b^\tau, \mathfrak{O}\}$$

mit $\mathrm{Gal}(F{:}\mathbb{F}_4(x)) = \langle\tau\rangle$ und $(x - c) = \mathfrak{P}_c\mathfrak{P}_c^\tau\mathfrak{O}^{-2}$ für $c \in \mathbb{F}_4 = \{0, 1, a, b\}$.
Es seien $\mathfrak{A} := \prod_{c\in\mathbb{F}_4} \mathfrak{P}_c$ der Auswertungsdivisor und $\mathfrak{G} := \mathfrak{O}^2$ der Goppadivisor des elliptischen Codes $C := C(\mathfrak{A}, \mathfrak{G})$. Der Raum $\mathcal{L}(\mathfrak{G})$ wird von 1 und x erzeugt (nach Notiz 13.2) und es ist daher

$$C = \mathbb{F}_4\langle(1, 1, 1, 1), (0, 1, a, b)\rangle.$$

Die drei Skalarprodukte der beiden Basisvektoren verschwinden allesamt aufgrund $1{+}1{+}1{+}1 = 0 = 1{+}a{+}b = 1^2{+}a^2{+}b^2$. Somit ist $C = C(\mathfrak{A}, \mathfrak{G})$ ein selbstdualer Code der Dimension 2 obwohl der Quotient $\mathfrak{A}^{-1}\mathfrak{G}^2$ kein kanonischer Divisor ist. Denn wäre $\mathfrak{A}^{-1}\mathfrak{G}^2$ kanonisch, d.h. es gilt $\mathfrak{A}^{-1}\mathfrak{G}^2 \in \mathbf{W}_{F:\mathbb{F}_4} = \mathbf{H}_{F:\mathbb{F}_4}$, so gäbe es eine Funktion $z \in F$ mit Divisor $(z) = \mathfrak{A}\mathfrak{G}^{-2} = \mathfrak{A}\mathfrak{O}^{-4}$. Dann ist z eine $\mathbb{F}_4$-Linearkombination der $\mathcal{L}(\mathfrak{O}^4)-$erzeugenden Funktionen $1, x, x^2, y$. Aufgrund $\mathrm{ord}_\mathfrak{O}(1), \mathrm{ord}_\mathfrak{O}(x), \mathrm{ord}_\mathfrak{O}(y) < 4$ ist also o.E.

$$z = x^2 + a_3y + a_2x + a_0$$

mit $a_i \in \mathbb{F}_4$. Es ist $a_0 = 0$ aufgrund $z(\mathfrak{P}_0) = x(\mathfrak{P}_0) = y(\mathfrak{P}_0) = 0$. Weiter gilt $a_2 \neq 0$, da $\mathfrak{P}_0^2$ den Nullstellendivisor von $x^2 + a_3y$ nicht aber $(z)_0$ teilt. Ebenso ist $a_3 \neq 0$, da die Funktion $x(x + a_2)$ den Divisor $\mathfrak{P}_0\mathfrak{P}_0^\tau\mathfrak{P}_c\mathfrak{P}_c^\tau\mathfrak{O}^{-4}$ mit $c \in \{1, a, b\}$ besitzt. Es ergibt sich also die Gleichung

$$0 = z(\mathfrak{P}_c) = x(x + a_2)(\mathfrak{P}_c) + a_3y(\mathfrak{P}_c) = a_3y(\mathfrak{P}_c),$$

die im Widerspruch zu $\mathrm{ord}_{\mathfrak{P}_c}(y) = 0$ steht.

14.2 Ein Kriterium für Selbstdualität

Satz 14.4. (Reiter) *Es sei $C(\mathfrak{A}, \mathfrak{G})$ ein arithmetischer Code über $F{:}\mathbb{F}_q$ der Länge $n \geq 2g_{F:\mathbb{F}_q} + 2$ mit ganzem Goppadivisor $\mathfrak{G}$. Dann ist der Code $C(\mathfrak{A}, \mathfrak{G})$ genau dann selbstdual, wenn es ein Differential $\delta \in \Delta_{F:\mathbb{F}_q}$ mit Divisor $(\delta) = \mathfrak{A}^{-1}\mathfrak{G}^2$ und $\mathrm{Res}_\mathfrak{P}(\delta) = 1$ für alle Primteiler $\mathfrak{P}$ von $\mathfrak{A}$ gibt.*

Zum Beweis des Satzes benötigen wir eine allgemeinere Form des Lemma 12.17.

Lemma 14.5. *Es seien $C(\mathfrak{A},\mathfrak{G})$ und $C(\mathfrak{A},\tilde{\mathfrak{G}})$ zwei identische Codes über $F{:}\mathbb{F}_q$, deren Goppadivisoren $\mathfrak{G},\tilde{\mathfrak{G}}$ die Ungleichungen $2g_{F:\mathbb{F}_q}\leq\deg(\mathfrak{G}),\deg(\tilde{\mathfrak{G}})\leq n-2$ erfüllen. Zudem sei $\mathfrak{G}$ ganz. Dann sind $\mathfrak{G}$ und $\tilde{\mathfrak{G}}$ äquivalent, und es gibt eine Funktion $u\in F$ mit Divisor $(u)=\mathfrak{G}\tilde{\mathfrak{G}}^{-1}$ sowie $u(\mathfrak{P})=1$ für alle Primteiler $\mathfrak{P}$ von $\mathfrak{A}$.*

Beweis. Es seien $C := C(\mathfrak{A},\mathfrak{G})$ und $\tilde{C} := C(\mathfrak{A},\tilde{\mathfrak{G}})$. Da $\mathfrak{G}$ ganz ist, enthält sein linearer Raum $\mathcal{L}(\mathfrak{G})$ die konstanten Funktionen und es gilt $1\in\mathcal{L}(\mathfrak{G})$. Somit besitzen C und aufgrund $C=\tilde{C}$ auch $\tilde{C}$ das Codewort $(1,\ldots,1)$. Es gibt also eine Variable $u\in\mathcal{L}(\tilde{\mathfrak{G}})$ mit

$$(1,\ldots,1)=(u(\mathfrak{P}_1),\ldots,u(\mathfrak{P}_n)).$$

Daher hat der Divisor von u die Gestalt $(u)=\mathfrak{U}\tilde{\mathfrak{G}}^{-1}$ mit einem ganzen und zu $\mathfrak{A}$ teilerfremden Divisor $\mathfrak{U}$. Hieraus folgt die Gleichheit der arithmetischen Codes

$$C(\mathfrak{A},\mathfrak{G})=C(\mathfrak{A},\tilde{\mathfrak{G}})=C(\mathfrak{A},\mathfrak{U}).$$

Wir zeigen, daß $\mathfrak{G}$ und $\mathfrak{U}$ gleich sind. Wegen $\mathfrak{U}\sim\tilde{\mathfrak{G}}$ folgt dann die Behauptung des Satzes.
Den größten gemeinsamen Teiler von $\mathfrak{G}$ und $\mathfrak{U}$ bezeichnen wir mit $\mathfrak{B}$ und es sei $\mathfrak{C} := (\mathfrak{A}\mathfrak{B})^{-1}\mathfrak{G}\mathfrak{U}$. Wir nehmen zunächst an, daß $\dim(\mathfrak{C})>0$ gilt. Da $\mathfrak{B}$ ganz ist, folgt nach dem Satz von *Clifford*

$$\dim(\mathfrak{B})+\dim(\mathfrak{C})\leq 1+\dim(\mathfrak{B}\mathfrak{C})=1+\dim(\mathfrak{A}^{-1}\mathfrak{G}\mathfrak{U}).$$

Aufgrund $\deg(\mathfrak{A}^{-1}\mathfrak{U})\leq -2$ und $2g\leq\deg(\mathfrak{G})$ gilt

$$\dim(\mathfrak{A}^{-1}\mathfrak{G}\mathfrak{U})\leq\dim(\mathfrak{G})-2$$

und damit

$$r:=\dim(\mathcal{L}(\mathfrak{G})/\mathcal{L}(\mathfrak{B}))=\dim(\mathfrak{G})-\dim(\mathfrak{B})>\dim(\mathfrak{C})>0.$$

Wir betrachten ein Vertretersystem $\{x_1,\ldots,x_r\}$ einer Basis von $\mathcal{L}(\mathfrak{G})/\mathcal{L}(\mathfrak{B})$ und zugehörige Funktionen $u_1,\ldots,u_r\in\mathcal{L}(\mathfrak{U})$ mit $u_i(\mathfrak{P})=x_i(\mathfrak{P})$ für $i=1,\ldots,r$ und $\mathfrak{P}|\mathfrak{A}$. Dann liegen die Elemente x_i-u_i im Raum $\mathcal{L}(\mathfrak{C})$. Aufgrund $r>\dim(\mathfrak{C})$ gibt es eine nichttriviale Linearkombination $\sum_{i=1}^{r}a_i(x_i-u_i)=0$. Es gilt somit

$$0\neq\sum_{i=1}^{r}a_ix_i=\sum_{i=1}^{r}a_iu_i\in\mathcal{L}(\mathfrak{G})\cap\mathcal{L}(\mathfrak{U})=\mathcal{L}(\mathfrak{B})$$

im Widerspruch zur Definition der x_i. Es ist also $\dim(\mathfrak{C})=0$.
Hieraus folgt nun die Gleichheit von $\mathfrak{G}$ und $\mathfrak{U}$. Weil die Codes C und $\tilde{C}$ gleich sind, gibt es zu jeder Funktion $x\in\mathcal{L}(\mathfrak{G})$ ein $y\in\mathcal{L}(\mathfrak{U})$ mit

$$\boldsymbol{x}=(x(\mathfrak{P}_1),\ldots,x(\mathfrak{P}_n))=(y(\mathfrak{P}_1),\ldots,y(\mathfrak{P}_n))=\boldsymbol{y}.$$

Also ist $x-y\in\mathcal{L}(\mathfrak{C})=\{0\}$, woraus $\mathcal{L}(\mathfrak{G})\leq\mathcal{L}(\mathfrak{U})$ folgt. Die entgegengesetze Inklusion zeigt man analog und es gilt somit $\mathcal{L}(\mathfrak{G})=\mathcal{L}(\mathfrak{U})$. Aufgrund der Voraussetzung $2g\leq\deg(\mathfrak{G}),\deg(\tilde{\mathfrak{G}})$ sind $\mathfrak{G}$, $\tilde{\mathfrak{G}}$ und somit auch $\mathfrak{U}$ nicht speziell, was schließlich $\mathfrak{G}=\mathfrak{U}$ zur Folge hat. □

Beweis zu Satz 14.4. Wir brauchen nur die Hinrichtung zu zeigen, da die Rückrichtung aus Satz 14.2 folgt. Es sei also $C = C(\mathfrak{A}, \mathfrak{G})$ ein selbstdualer Code der Länge $n \geq 2g + 2$. Dann hat C Dimension $\frac{n}{2}$ und es folgt

$$\dim(\mathfrak{G}) - \dim(\mathfrak{A}^{-1}\mathfrak{G}) = \dim(C) = \frac{n}{2} \geq g + 1.$$

Nach dem Satz von *Clifford* ist $\mathfrak{G}$ somit nicht-speziell. Die obige Ungleichung wird dann mit dem Satz von *Riemann-Roch* zu

$$i(\mathfrak{A}^{-1}\mathfrak{G}) = \dim(\mathfrak{G}) - \dim(\mathfrak{A}^{-1}\mathfrak{G}) \geq g + 1.$$

Es folgen $\deg(\mathfrak{A}^{-1}\mathfrak{G}) < 0$ und $\dim(\mathfrak{A}^{-1}\mathfrak{G}) = 0$, da Spezialitätsindizes für Divisoren positiven Grades stets durch das Geschlecht des Funktionenkörpers nach oben beschränkt sind. Das zeigt $\frac{n}{2} = \dim(\mathfrak{G}) = \deg(\mathfrak{G}) - (g - 1)$ und

$$2g \leq \deg(\mathfrak{G}) \leq n - 2.$$

Als selbstdualer Code erfüllt $C(\mathfrak{A}, \mathfrak{G})$ nach Kapitel 11 die Gleichheit $C(\mathfrak{A}, \mathfrak{G}) = C(\mathfrak{A}, \mathfrak{G}^*)$ mit dem dualen Goppadivisor $\mathfrak{G}^* = (\delta)\mathfrak{A}\mathfrak{G}^{-1}$, wobei δ ein Differential mit Residuen $\mathrm{Res}_{\mathfrak{P}}(\delta) = 1$ bei den Primteilern $\mathfrak{P}$ von $\mathfrak{A}$ ist. Der Grad von $\mathfrak{G}^*$ ist ebenfalls durch $2g \leq \deg(\mathfrak{G}^*) \leq n - 2$ beschränkt und es folgt aus Lemma 14.5

$$\mathfrak{G} = (u)\mathfrak{G}^* = (u)(\delta)\mathfrak{A}\mathfrak{G}^{-1} \qquad \text{mit } u(\mathfrak{P}) = 1 \text{ für } \mathfrak{P}|\mathfrak{A}.$$

Dann ist $\mathfrak{A}^{-1}\mathfrak{G}^2$ der kanonische Divisor von $\tilde{\delta} := u\delta$ und es gilt $\mathrm{Res}_{\mathfrak{P}}(\tilde{\delta}) = 1$ für alle Primteiler $\mathfrak{P}$ von $\mathfrak{A}$. □

Zusatz 14.6. *Unter der Voraussetzung $n \geq 6g_{F:\mathbb{F}_q} + 2$ gilt der Satz 14.4 auch für nicht ganze Goppadivisoren $\mathfrak{G}$.*

Beweis. Der Beweis sei dem Leser zur Übung überlassen. □

14.3 Ein Existenzsatz für selbstduale Codes in Charakteristik 2

Bemerkung 14.7. (Hecke) *In einem Kongruenzfunktionenkörper $F{:}\mathbb{F}_q$ gibt es eine Klasse von Divisoren $\mathbf{D} \in \mathbb{C}_{F:\mathbb{F}_q}$ mit $\mathbf{D}^2 = \mathbf{W}_{F:\mathbb{F}_q}$.*

Beweis für Charakteristik 2. Es sei $F{:}\mathbb{F}_q$ ein Funktionenkörper der Charakteristik 2. Für ein exaktes Differential dx von F unterscheidet sich ein beliebiger kanonischer Divisor von (dx) nur durch Multiplikation mit einem Hauptdivisor. Es ist also nur zu zeigen, daß jeder Primdivisor $\mathfrak{P}$ mit quadratischer Ordnung in (dx) aufgeht. Sei $\mathfrak{P} \in \mathbb{P}_{F:\mathbb{F}_q}$ ein Primdivisor und $t \in \mathfrak{P}$ ein Primelement. Dann besitzt x die Laurententwicklung $x = \sum_{i \geq i_0} a_i t^i$. Die Differentation beider Seiten ergibt

$$dx = \sum_{i \geq i_0} a_i \cdot i \cdot t^{i-1} dt = \sum_{j \geq j_0} (2j + 1) \cdot a_{2j+1} \cdot t^{2j} dt$$

aufgrund der Charakteristik von F. Also geht $\mathfrak{P}$ mit Ordnung $2j_0$ in (dx) auf. Da $\mathfrak{P} \in \mathbb{P}_{F:\mathbb{F}_q}$ beliebig gewählt werden kann, ist (dx) das Quadrat eines Divisors $\mathfrak{D}$. Somit gilt $\mathbf{W}_{F:\mathbb{F}_q} = [\mathfrak{D}^2] = [\mathfrak{D}]^2$, wobei $[\mathfrak{D}]$ die von $\mathfrak{D}$ erzeugte Divisorenklasse in $\mathbb{C}_{F:\mathbb{F}_q}$ sei. □

Satz 14.8. (Scharlau) *Es sei F:$\mathbb{F}_q$ ein Kongruenzfunktionenkörper und $\mathbf{C} \in \mathbb{C}_{F:\mathbb{F}_q}$ eine Divisorenklasse. Der Auswertungsdivisor $\mathfrak{A}$ sei ein Element der Klasse $\mathbf{C}^2$. Dann gelten:*

(a) *Es gibt es einen zu $\mathfrak{A}$ fremden Divisor $\mathfrak{G} \in \mathbb{D}_{F:\mathbb{F}_q}$, sodaß der arithmetische Code $C(\mathfrak{A}, \mathfrak{G})$ quasiselbstdual ist.*

(b) *Im Falle der Chararistik 2 gibt es sogar einen Divisor $\mathfrak{G}$, für den der Code $C(\mathfrak{A}, \mathfrak{G})$ selbstdual ist.*

Beweis. (a) Es seien $\mathfrak{A} = \mathfrak{P}_1 \cdots \mathfrak{P}_n \in \mathbf{C}^2$ sowie $\mathfrak{D} \in \mathbf{D}$ mit $\mathbf{D}^2 = \mathbf{W}_{F:\mathbb{F}_q}$ (vgl. obige Bemerkung 14.7). Nach dem *schwachen Approximationssatz* gibt es einen Divisor $\mathfrak{G} \in \mathbf{C} \cdot \mathbf{D}$, der fremd zu $\mathfrak{A}$ ist. Dann ist $C := C(\mathfrak{A}, \mathfrak{G})$ ein wohldefinierter arithmetischer Code und es gilt $\mathfrak{A}^{-1}\mathfrak{G}^2 \sim \mathfrak{D}^2$, d.h. $\mathfrak{A}^{-1}\mathfrak{G}^2$ ist ein kanonischer Divisor. Somit gelten $\dim(\mathfrak{A}^{-1}\mathfrak{G}) = \dim(\mathfrak{D}^2\mathfrak{G}^{-1}) = i(\mathfrak{G})$, $\deg(\mathfrak{G}) = \frac{n}{2} + g - 1$ und

$$\dim(C(\mathfrak{A}, \mathfrak{G})) = \dim(\mathfrak{G}) - \dim(\mathfrak{A}^{-1}\mathfrak{G}) = \dim(\mathfrak{G}) - i(\mathfrak{G}) = \deg(\mathfrak{G}) - g + 1 = \frac{n}{2}.$$

In dieser Situation läßt sich nun genauso wie im Beweis zu Satz 14.2 auf die Quasiselbstdualität von C schließen.
(b) Nun beschränken uns auf den Fall der Charakteristik 2. Es sei $\boldsymbol{a} = (a_1, \ldots, a_n)$ der Vektor aus $\mathbb{F}_q^n$ mit

$$C^* = \boldsymbol{a} \times C(\mathfrak{A}, \mathfrak{G}).$$

Da der Frobeniusendomorphismus auf $\mathbb{F}_q$ ein Automorphismus ist, gibt es Konstanten $b_i \in \mathbb{F}_q$ mit $a_i = b_i^2$. Nach dem *schwachen Approximationssatz* existiert desweiteren eine Funktion $u \in F^\times$ mit $u(\mathfrak{P}_\mathrm{i}) = b_i$ für alle Primteiler $\mathfrak{P}_i$ von $\mathfrak{A}$. Wir definieren dann $\tilde{\mathfrak{G}} := (u)^{-1}\mathfrak{G}$. Für alle Funktionen $z \in \mathcal{L}(\mathfrak{G})$ ist $\tilde{z} = uz$ eine Funktion aus $\mathcal{L}(\tilde{\mathfrak{G}})$, d.h. es gilt $C(\mathfrak{A}, \tilde{\mathfrak{G}}) = \boldsymbol{b} \times C(\mathfrak{A}, \mathfrak{G})$. Für $\tilde{\boldsymbol{x}} = \boldsymbol{b} \times \boldsymbol{x}$, $\tilde{\boldsymbol{y}} = \boldsymbol{b} \times \boldsymbol{y} \in C(\mathfrak{A}, \tilde{\mathfrak{G}})$ gelten

$$< \tilde{\boldsymbol{x}}, \tilde{\boldsymbol{y}} > = < \boldsymbol{b} \times \boldsymbol{x}, \boldsymbol{b} \times \boldsymbol{y} > = < \boldsymbol{a} \times \boldsymbol{x}, \boldsymbol{y} > = \ 0,$$

also ist $C(\mathfrak{A}, \tilde{\mathfrak{G}})$ selbstorthogonal. Das beweist Aussage (b). □

Die Voraussetzung des Satzes von *Scharlau* kann in Charakteristik 2 tatsächlich erfüllt werden.

Korollar 14.9. *Es gibt arithmetische selbstduale binäre Codes.*
Solche Codes können über Funktionenkörper F:$\mathbb{F}_q$ (der Charakteristik 2) erzeugt werden, deren Geschlecht g und Anzahl rationaler Stellen N die Ungleichung $N > g + 1$ erfüllen. Ihre Länge beträgt hierbei mindestens $N - g - 1$.

Die Existenz solcher Funktionenkörper ist gesichert. Als Beispiel dienen die *Hermiteschen Funktionenkörper* $F = \mathbb{F}_{q^2}(x,y)$ mit der erzeugenden Relation $x^{q+1}+y^{q+1}=1$, die wir in Kapitel 17 studieren werden. Diese Funktionenkörper nehmen die *Hasse-Weil-Schranke* an und erfüllen somit

$$N = 2g\sqrt{q^2} + q^2 + 1 > g + 1.$$

Zum Beweis des Korollars benötigen wir eine Anleihe aus der algebraischen Geometrie.

Bemerkung 14.10. *Es sei $F{:}\mathbb{F}_q$ ein Funktionenkörper der Charakteristik p vom Geschlecht g. Dann ist die Nullklassenfaktorgruppe $\mathbb{C}^0_{F:\mathbb{F}_q}/(\mathbb{C}^0_{F:\mathbb{F}_q})^p$ eine elementarabelsche p-Gruppe vom Rang $r \leq g$.*

Ohne Beweis. (siehe bspw. [Mum86, II.5, Seite 64, Prop.(4)])

Beweis zu Korollar 14.9. Nach obiger Anleihe bilden die Divisorenklassen vom Grad 0 modulo zweiter Potenzen eine elementarabelsche 2-Gruppe vom Rang $r \leq g$, d.h. es gilt

$$\mathbb{C}_2^0 := \mathbb{C}^0_{F:\mathbb{F}_q}/(\mathbb{C}^0_{F:\mathbb{F}_q})^2 = \mathbf{Z}_2^r.$$

Sind $\mathfrak{P}_1, \ldots, \mathfrak{P}_N$ sämtliche rationale Stellen von $F{:}\mathbb{F}_q$, so erzeugen die Nullklassen $[\mathfrak{P}_i\mathfrak{P}_N^{-1}]$ in $\mathbb{C}_2^0$ eine Untergruppe U vom Rang $s \leq r$. Ohne Einschränkung seien $[\mathfrak{P}_1\mathfrak{P}_N^{-1}], \ldots, [\mathfrak{P}_s\mathfrak{P}_N^{-1}]$ die Erzeuger von U. Das Produkt der restlichen Nullklassen hat in $\mathbb{C}_2^0$ die Darstellung

$$\prod_{i=s+1}^{N-1} [\mathfrak{P}_i\mathfrak{P}_N^{-1}] = \prod_{i=1}^{s} [\mathfrak{P}_i\mathfrak{P}_N^{-1}]^{e_i} \qquad \text{mit } e_i \in \{0,1\}.$$

Nach eventueller Umnummerierung gilt also

$$\prod_{i=\tilde{s}+1}^{N-1} [\mathfrak{P}_i\mathfrak{P}_N^{-1}] = 1 \in \mathbb{C}_2^0$$

mit $\tilde{s} \leq s \leq g$. Die Nullklasse $[\mathfrak{A}\mathfrak{P}_n^{-n}]$ mit $\mathfrak{A} := \prod_{i=\tilde{s}+1}^{N-1} \mathfrak{P}_i$ und $n = N-1-\tilde{s}$ ist also ein zweite Potenz, d.h. es gilt

$$\mathfrak{A}\mathfrak{P}_N^{-n} \sim \mathfrak{D}^2 = \mathfrak{B}^2\mathfrak{C}^{-2} \qquad \text{mit ganzen Divisoren } \mathfrak{A}, \mathfrak{B}, \mathfrak{C}.$$

Folglich ist n eine gerade Zahl und $\mathfrak{A}$ ist äquivalent zu einem quadratischen Divisor. Außerdem hat $\mathfrak{A}$ aufgrund $\deg(\mathfrak{A}) = N-1-\tilde{s} \geq N-1-g$ einen positiven Grad. Hiermit ist die Voraussetzung des Satzes von *Scharlau* erfüllt und es gibt daher einen selbstdualen arithmetischen Code über $F{:}\mathbb{F}_q$ mit Auswertungsdivisor $\mathfrak{A}$. □

Kapitel 15

Decodierung arithmetischer Codes

15.1 Der Basis-Decodieralgorithmus

Im praktischen Gebrauch eines Codes entsteht die folgende Situation: Sender und Empfänger einigen sich auf einen arithmetischen $[n,k,d]_q$-Code $C^* := C^*(\mathfrak{A},\mathfrak{G})$. Der Sender schickt ein Codewort $\boldsymbol{x}$ über einen möglicherweise nicht fehlerfreien Kanal an seinen Kommunikationspartner, der am anderen Ende des Kanals den Vektor $\boldsymbol{y} \in \mathbb{F}_q^n$ empfängt. Der Basis-Decodieralgorithmus ermöglicht nun dem Empfänger bis zu $e^* := \lfloor(\deg(\mathfrak{G}) - 2g + 1)/2\rfloor$ Fehler zu korrigieren. Gesucht wird hierbei ein **Fehlervektor** $\boldsymbol{e} \in \mathbb{F}_q^n$ vom Gewicht $w(\boldsymbol{e}) \leq e^*$ und ein Codewort $\boldsymbol{x'} \in C^*$, sodaß $\boldsymbol{y} = \boldsymbol{x'} + \boldsymbol{e}$ gilt. Der Fehlervektor $\boldsymbol{e}$ und das Codewort $\boldsymbol{x'}$ sind eindeutig bestimmt, über ihre Existenz läßt sich aber keine allgemeine Aussage treffen. Sind nun bei der Übertragung nicht mehr als e^* Fehler aufgetreten, so gelten $\boldsymbol{x} = \boldsymbol{x'}$ und

$$\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}.$$

Von dieser Annahme werden wir in diesem Kapitel ausgehen.

Definition 15.1. Es sei $F{:}\mathbb{F}_q$ ein Kongruenzfunktionenkörper vom Geschlecht g, $C := C(\mathfrak{A},\mathfrak{G})$ ein arithmetischer Code über $F{:}\mathbb{F}_q$ der Länge n mit dualem Code $C^* := C(\mathfrak{A},\mathfrak{G}^*) = C^*(\mathfrak{A},\mathfrak{G})$. Dann heißen die Zahlen

$$k_C^* := n - \deg(\mathfrak{G}) + g - 1 \leq \dim(C^*)$$
$$d_C^* := \deg(\mathfrak{G}) - 2g + 2 \leq d(C^*)$$

garantierte Dimension bzw. **garantierte Minimaldistanz** von C^*.
Die Bilinearform

$$[\,\cdot\,,\,\cdot\,] : \begin{cases} \mathbb{F}_q^n \times \mathcal{L}(\mathfrak{G}) & \longrightarrow & \mathbb{F}_q \\ (\boldsymbol{y}, z) & \longmapsto & \sum_{i=1}^{n} y_i z(\mathfrak{P}_i) \end{cases}$$

heißt **Syndrom**. Es sei $\mathfrak{H} \in \mathbb{D}_{F:\mathbb{F}_q}$ ein Hilfsdivisor und $u_1,\ldots,u_k$ eine Basis von $\mathcal{L}(\mathfrak{H})$, $v_1,\ldots,v_l$ eine Basis von $\mathcal{L}(\mathfrak{H}^{-1}\mathfrak{G})$ sowie $z_1,\ldots,z_m$ eine Basis von $\mathcal{L}(\mathfrak{G})$. Für

einen Vektor $\boldsymbol{y} \in \mathbb{F}_q^n$ heißen dann

$$s_{ij}(\boldsymbol{y}) := [\boldsymbol{y}, u_i v_j]$$

Syndrome von $\boldsymbol{y}$. Man beachte, daß die $s_{ij}(\boldsymbol{y})$ wohldefiniert sind, da $u_i v_j \in \mathcal{L}(\mathfrak{G})$ gilt.

Für die folgenden Bemerkungen 15.2, 15.4 und 15.6 gelte für $\boldsymbol{y} \in \mathbb{F}_q^n$

$$\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$$

mit einem Codewort $\boldsymbol{x} \in C^*$ und einem Fehlervektor $\boldsymbol{e} \in \mathbb{F}_q^n$. Dabei sei $w(\boldsymbol{e}) \leq e^*$.

Bemerkung 15.2. *Für alle $z \in \mathcal{L}(\mathfrak{G})$ gilt*

$$[\boldsymbol{y}, z] = [\boldsymbol{e}, z].$$

Beweis. Die Codewörter $\boldsymbol{x} \in C^*$ und $\boldsymbol{z} = (z(\mathfrak{P}_1), \ldots, z(\mathfrak{P}_n)) \in C$ sind orthogonal zueinander, daher gilt $[\boldsymbol{y} - \boldsymbol{e}, z] = [\boldsymbol{x}, z] = \sum_{i=1}^n x_i z(\mathfrak{P}_i) = < \boldsymbol{x}, \boldsymbol{z} > = 0$. □

Es seien $I_{\boldsymbol{y}} := \{1 \leq i \leq n : e_i \neq 0\}$ die **Indexmenge der Fehlerpositionen**, $\mathfrak{T}_{\boldsymbol{y}} := \prod_{i \in I_{\boldsymbol{y}}} \mathfrak{P}_i$ sowie $t_{\boldsymbol{y}} := \deg(\mathfrak{T}_{\boldsymbol{y}})$. Die nichtverschwindenden Elemente aus $\mathcal{L}(\mathfrak{T}_{\boldsymbol{y}}^{-1}\mathfrak{H})$ nennt man dann **fehlerlokalisierende Funktionen zu $\boldsymbol{y}$**. Weiter werde mit $H_{\boldsymbol{y}}$ der Lösungsraum des linearen Gleichungssystems

$$\sum_{i=1}^{k} s_{ij}(\boldsymbol{y}) X_i = 0 \qquad \text{für } j = 1, \ldots, l \tag{15.3}$$

bezeichnet. Es gilt die

Bemerkung 15.4.

(a) *Die Abbildung $\lambda : \mathcal{L}(\mathfrak{T}_{\boldsymbol{y}}^{-1}\mathfrak{H}) \hookrightarrow H_{\boldsymbol{y}}, u = \sum_{i=1}^k x_i u_i \mapsto (x_1, \ldots, x_k)$ ist ein injektiver Homomorphismus.*

(b) *λ ist ein Isomorphismus, falls $(\mathfrak{T}_{\boldsymbol{y}}\mathfrak{H})^{-1}\mathfrak{G}$ Spezialitätsindex 0 hat.*

Beweis. (a) Es sei $u \in \mathcal{L}(\mathfrak{T}_{\boldsymbol{y}}^{-1}\mathfrak{H})$. Als Element von $\mathcal{L}(\mathfrak{H})$ hat u eine eindeutige Darstellung $u = \sum_{i=1}^k x_i u_i$ mit $x_i \in \mathbb{F}_q$. Die Funktionen uv_j für $j = 1, \ldots, l$ gehören zu $\mathcal{L}(\mathfrak{T}_{\boldsymbol{y}}^{-1}\mathfrak{G})$, d.h. es ist $uv_j(\mathfrak{P}_i) = 0$ für alle Fehlerpositionen $i \in I_{\boldsymbol{y}}$. Im Falle $e_i \neq 0$ ist also $uv_j(\mathfrak{P}_i) = 0$. Daher gilt für $j = 1, \ldots, l$

$$\sum_{i=1}^{k} x_i s_{ij}(\boldsymbol{y}) = \sum_{i=1}^{k} x_i [\boldsymbol{y}, u_i v_j] = [\boldsymbol{y}, uv_j] = [\boldsymbol{e}, uv_j] = \sum_{i=1}^{n} e_i (uv_j)(\mathfrak{P}_i) = 0.$$

Hieraus folgen Wohldefiniertheit und Injektivität von λ; die Homomorphie ist offensichtlich.

(b) Es sei nun zusätzlich $(\mathfrak{T}_{\boldsymbol{y}}\mathfrak{H})^{-1}\mathfrak{G}$ kein spezieller Divisor. Wir nehmen an, daß λ nicht surjektiv ist. Dann gibt es eine Lösung $(x_1,\ldots,x_k) \in H_{\boldsymbol{y}}$ des Gleichungssytems (15.3), für welche die Funktion $u := \sum_{i=1}^{k} x_i u_i \in \mathcal{L}(\mathfrak{H})$ nicht Element des Raumes $\mathcal{L}(\mathfrak{T}_{\boldsymbol{y}}^{-1}\mathfrak{H})$ ist. Also gibt es einen Primteiler $\mathfrak{P}_r$ von $\mathfrak{T}_{\boldsymbol{y}}$ mit $\mathrm{ord}_{\mathfrak{P}_r}(u) < -\mathrm{ord}_{\mathfrak{P}_r}(\mathfrak{T}_{\boldsymbol{y}}^{-1}\mathfrak{H})$. Da $(\mathfrak{T}_{\boldsymbol{y}}\mathfrak{H})^{-1}\mathfrak{G}$ nach Voraussetzung Spezialitätsindex 0 hat, ist die Menge $\mathcal{L} := \mathcal{L}(\mathfrak{P}_r(\mathfrak{T}_{\boldsymbol{y}}\mathfrak{H})^{-1}\mathfrak{G})\backslash\mathcal{L}((\mathfrak{T}_{\boldsymbol{y}}\mathfrak{H})^{-1}\mathfrak{G})$ nicht leer. Ist $v \in \mathcal{L}$, so ist uv eine Funktion aus $\mathcal{L}(\mathfrak{T}_{\boldsymbol{y}}^{-1}\mathfrak{P}_r\mathfrak{G})$, d.h. das Syndrom $[\boldsymbol{e}, uv]$ ist wohldefiniert und es gilt

$$[\boldsymbol{e}, uv] = e_r(uv(\mathfrak{P}_r)) \neq 0.$$

Andererseits hat v wegen $\mathcal{L} \leq \mathcal{L}(\mathfrak{H}^{-1}\mathfrak{G})$ die Darstellung $v = \sum_{j=1}^{l} a_j v_j$. Als Lösung des Gleichungssystems (15.3) erfüllt $(x_1,\ldots,x_k)$ nun

$$0 = \sum_{j=1}^{l} a_j \sum_{i=1}^{k} x_i[\boldsymbol{y}, u_i v_j] = [\boldsymbol{y}, uv] = [\boldsymbol{e}, uv].$$

Dies ergibt einen Widerspruch zur Annahme, daß λ nicht surjektiv ist. □

Korollar 15.5. (a) *Unter der Voraussetzung* $\dim(\mathfrak{H}) > t_{\boldsymbol{y}}$ *ist der Lösungsraum* $H_{\boldsymbol{y}}$ *nicht trivial.*
(b) *Im Falle* $\deg(\mathfrak{H}^{-1}\mathfrak{G}) > t_{\boldsymbol{y}} + 2g - 2$ *gilt* $H_{\boldsymbol{y}} \cong \mathcal{L}(\mathfrak{T}_{\boldsymbol{y}}^{-1}\mathfrak{H})$. □

Bemerkung 15.6. *Es sei* $\deg(\mathfrak{H}^{-1}\mathfrak{G}) \geq 2g$ *und* $u = \sum_{i=1}^{k} x_i u_i \in \mathcal{L}(\mathfrak{T}_{\boldsymbol{y}}^{-1}\mathfrak{H})$ *eine fehlerlokalisierende Funktion zu* $\boldsymbol{y}$. *Weiter bezeichne*

$$J_u := \{1 \leq i \leq n : (uv_j)(\mathfrak{P}_i) = 0 \text{ für } j = 1,\ldots,l\}.$$

Dann besitzt das inhomogene lineare Gleichungssystem

$$\sum_{i \in J_u} z_r(\mathfrak{P}_i) T_i = [\boldsymbol{y}, z_r] \qquad \text{für } r = 1,\ldots,m \tag{15.7}$$

genau eine Lösung, nämlich $(e_i)_{i \in J_u}$.

Beweis. Existenz: Aufgrund $u(\mathfrak{P}_i) = 0$ für jeden Index $i \in I_{\boldsymbol{y}}$ ist $I_{\boldsymbol{y}}$ in der Menge J_u enthalten. Es ist also für $r = 1,\ldots,m$

$$\sum_{i \in J_u} e_i z_r(\mathfrak{P}_i) = \sum_{i=1}^{n} e_i z_r(\mathfrak{P}_i) = [\boldsymbol{e}, z_r] = [\boldsymbol{y}, z_r].$$

Eindeutigkeit: Es sei $\boldsymbol{f}$ eine zweite Lösung von (15.7). Dann löst $\boldsymbol{e} - \boldsymbol{f}$ das homogene lineare Gleichungssystem $\sum_{i \in J_u} z_r(\mathfrak{P}_i) T_i = 0$ für $r = 1,\ldots,m$. Definiert man $\boldsymbol{h} := (h_1,\ldots,h_n)$ mittels

$$h_i := \begin{cases} e_i - f_i & \text{für } i \in J_u \\ 0 & \text{sonst} \end{cases},$$

so ist $[\boldsymbol{h}, z_r] = 0$ für alle Basisfunktionen $z_r \in \mathcal{L}(\mathfrak{G})$. Also ist $\boldsymbol{h}$ ein Codewort aus C^* vom Gewicht $w(\boldsymbol{h}) \leq \#J_u$. Wir schätzen die Mächtigkeit von J_u ab: Ist $u(\mathfrak{P}) = 0$ für einen Primteiler $\mathfrak{P}$ von $\mathfrak{A}$, so gilt nach der Dreicksungleichung $\mathrm{ord}_{\mathfrak{P}}(u_i) \geq 1$ für $i = 1, \ldots, k$ und damit $\mathrm{ord}_{\mathfrak{P}}(\mathfrak{H}) \geq 1$, da $u_1, \ldots, u_k$ den Raum $\mathcal{L}(\mathfrak{H})$ aufspannen. Ist stattdessen $v_j(\mathfrak{P}) = 0$ für alle Basisvariablen $v_j \in \mathcal{L}(\mathfrak{H}^{-1}\mathfrak{G})$, so gilt ebenfalls $\mathrm{ord}_{\mathfrak{P}}(\mathfrak{H}) \geq 1$, da $\mathfrak{G}$ fremd zu $\mathfrak{A}$ ist. Demnach ist im jeden Fall $\#J_u \leq \deg(\mathfrak{H})$ und damit nach Voraussetzung

$$w(\boldsymbol{h}) \leq \#J_u \leq \deg(\mathfrak{H}) < \deg(\mathfrak{G}) - 2g + 2 = d_C^* \leq d(C^*).$$

Also ist $\boldsymbol{h}$ vom Gewicht 0 und somit $\boldsymbol{e} = \boldsymbol{f}$. □

Basis-Decodieralgorithmus 15.8. (für $C^* := C^*(\mathfrak{A}, \mathfrak{G})$)

(0) Wähle eine Zahl $1 \leq t \leq e^*$ und einen Hilfsdivisor $\mathfrak{H} \in \mathbb{D}_{F:\mathbb{F}_q}$ mit $\dim(\mathfrak{H}) > t$ und $\deg(\mathfrak{H}^{-1}\mathfrak{G}) > t + 2(g-1)$.

(1) Berechne Basen $u_1, \ldots, u_k$ von $\mathcal{L}(\mathfrak{H})$, $v_1, \ldots, v_l$ von $\mathcal{L}(\mathfrak{H}^{-1}\mathfrak{G})$ sowie $z_1, \ldots, z_m$ von $\mathcal{L}(\mathfrak{G})$.

(2) Berechne für den Vektor $\boldsymbol{y} \in \mathbb{F}_q^n$ die Syndrome $s_{ij}(\boldsymbol{y}) = [\boldsymbol{y}, u_i v_j]$ sowie $[\boldsymbol{y}, z_r]$.

(3) Finde eine nichttriviale Lösung des Gleichungssytem $\sum_{i=1}^{k} s_{ij}(\boldsymbol{y}) X_i = 0$ $(j = 1, \ldots, l)$ und bilde mit dem Lösungsvektor $(x_1, \ldots, x_k)$ die fehlerlokalisierende Funktion $u := \sum_{i=1}^{k} x_i u_i$.

(4) Finde alle Teiler $\mathfrak{P}_i$ des Auswertungsdivisors $\mathfrak{A}$ mit $(uv_j)(\mathfrak{P}_i) = 0$ für alle $j = 1, \ldots, l$ und damit die Indexmenge J_u.

(5) Löse das Gleichungssystem $\sum_{i \in J_u} z_r(\mathfrak{P}_i) T_i = [\boldsymbol{y}, z_r] (r = 1, \ldots, m)$. Mit der Lösung $(e_i)_{i \in J_u}$ bilde schließlich den Fehlervektor $\boldsymbol{e} = (e_1, \ldots, e_n)$ mit $e_i := 0$ für alle $i \notin J_u$.

Anmerkung 15.9. Ist der Hilfsdivisor $\mathfrak{H}$ fremd zu $\mathfrak{A}$, so genügt statt Schritt (4) die Vorgehensweise

(4*) Finde alle Teiler $\mathfrak{P}_i$ von $\mathfrak{A}$ mit $u(\mathfrak{P}_i) = 0$ und bilde damit J_u.

Wir erhalten schließlich folgenden

Satz 15.10. *Es sei $C^* = C^*(\mathfrak{A}, \mathfrak{G})$ ein dualer arithmetischer Code über $F{:}\mathbb{F}_q$. Weiter seien $e^* := \lfloor (d_C^* - 1)/2 \rfloor, 1 \leq t \leq e^*$ und $\mathfrak{H}$ ein Divisor mit $\dim(\mathfrak{H}) > t$ und $\deg(\mathfrak{H}^{-1}\mathfrak{G}) > t + 2(g-1)$. Dann korrgiert der Basis-Decodieralgorithmus bis zu t Fehler.* □

Korollar 15.11. (a) *Mit dem Basis-Decodieralgorithmus können bis zu*

$$t^* := -1 + \max\{\min\{\dim(\mathfrak{H}), \deg(\mathfrak{H}^{-1}\mathfrak{G}) - 2g + 2)\} : \mathfrak{H} \textit{ Hilfsdivisor}\}$$

Fehler korrigiert werden.

(b) *Es gilt* $t^* \geq \lfloor \frac{d_C^* - 1 - g}{2} \rfloor$.

Beweis. Es ist nur (b) zu zeigen. Sei $\mathfrak{P}$ ein rationale Stelle. Dann ist $\mathfrak{H} := \mathfrak{P}^{t^*+g}$ ein Hilfsdivisor mit $\dim(\mathfrak{H}) \geq t^* - 1$. Gemäß der Definition von t^* gilt

$$t^* \geq -1 + \deg(\mathfrak{H}^{-1}\mathfrak{G}) - 2g + 2 = \deg(\mathfrak{G}) - t^* - 3g + 1,$$

was $2t^* \geq \deg(\mathfrak{G}) - 3g + 1 = d_C^* - g - 1$ zur Folge hat. □

15.2 Der modifizierte Decodieralgorithmus

Definition 15.12. Es sei $C^* := C^*(\mathfrak{A}, \mathfrak{G})$ ein dualer arithmetischer Code über $F{:}\mathbb{F}_q$ mit einem Goppadivisor der Gestalt $\mathfrak{G} = \mathfrak{Q}^a$. Dann bezeichnen

$$s(\mathfrak{Q}) := \max\{\lfloor(\deg(\mathfrak{Q}^{i+1}) + 1)/2\rfloor - \dim(\mathfrak{Q}^i) : i \in \mathbb{Z}\} \qquad \text{und}$$

$$b := \min\{i \in \mathbb{N} : \text{Das Gleichungssystem (15.3) ist lösbar für } \mathfrak{H} = \mathfrak{Q}^i\}.$$

Bemerkung 15.13. *Für* $t_{\boldsymbol{y}} \leq e^* - s(\mathfrak{Q})$ *ist der Divisor* $\mathfrak{T}_{\boldsymbol{y}}^{-1}\mathfrak{Q}^{a-b}$ *nicht speziell. Insbesondere gilt dann* $H_{\boldsymbol{y}} \cong \mathcal{L}(\mathfrak{T}_{\boldsymbol{y}}^{-1}\mathfrak{Q}^b)$.

Beweis. Wir nehmen an, $\mathfrak{T}_{\boldsymbol{y}}^{-1}\mathfrak{Q}^{a-b}$ sei speziell, d.h. für einen kanonischen Divisor $\mathfrak{W} \in \mathbf{W}_{F:\mathbb{F}_q}$ gelte $\dim(\mathfrak{W}\mathfrak{T}_{\boldsymbol{y}}\mathfrak{Q}^{b-a}) = i(\mathfrak{T}_{\boldsymbol{y}}^{-1}\mathfrak{Q}^{a-b}) > 0$. Dann gibt es einen ganzen Divsor $\mathfrak{B}$, der äquivalent zu $\mathfrak{W}\mathfrak{T}_{\boldsymbol{y}}\mathfrak{Q}^{b-a}$ ist. Für diesen gilt

$$\mathcal{L}(\mathfrak{T}_{\boldsymbol{y}}^{-1}\mathfrak{Q}^{b-1}) \cong \mathcal{L}(\mathfrak{B}^{-1}\mathfrak{W}\mathfrak{Q}^{2b-a-1}).$$

Nach der Definition von b ist $\dim(\mathfrak{T}_{\boldsymbol{y}}^{-1}\mathfrak{Q}^{b-1}) = 0$ und somit $\dim(\mathfrak{B}^{-1}\mathfrak{W}\mathfrak{Q}^{2b-a-1}) = 0$, was nach dem Satz von *Riemann-Roch*

$$\deg(\mathfrak{B}) \geq \dim(\mathfrak{W}\mathfrak{Q}^{2b-a-1}) = \dim(\mathfrak{Q}^{a-2b+1}) - (a - 2b + 1)\deg(\mathfrak{Q}) + g - 1$$

zur Folge hat. Die Definition der Zahl $s(\mathfrak{Q})$ führt auf die Abschätzung

$$\begin{aligned}\dim(\mathfrak{Q}^{a-2b+1}) &\geq \left\lfloor \frac{(a-2b+2)\deg(\mathfrak{Q}) + 1}{2} \right\rfloor - s(\mathfrak{Q}) \\ &= \left\lfloor \frac{a\ \deg(\mathfrak{Q}) + 1 - 2g}{2} \right\rfloor + g - (b-1)\deg(\mathfrak{Q}) - s(\mathfrak{Q}) \\ &= e^* + g - (b-1)\deg(\mathfrak{Q}) - s(\mathfrak{Q}).\end{aligned}$$

Damit läßt sich schließlich ein Widerspruch herleiten, denn es folgt hieraus

$$\begin{aligned}\deg(\mathfrak{B}) &\geq e^* + g - (b-1)\deg(\mathfrak{Q}) - s(\mathfrak{Q}) - (a-2b+1)\deg(\mathfrak{Q}) + g - 1 \\ &= e^* - s(\mathfrak{Q}) + 2g - 1 - (a-b)\deg(\mathfrak{Q}) \\ &\geq t_{\boldsymbol{y}} + 2g - 1 - (a-b)\deg(\mathfrak{Q}) = \deg(\mathfrak{T}_{\boldsymbol{y}}\mathfrak{W}\mathfrak{Q}^{b-a}) + 1 = \deg(\mathfrak{B}) + 1.\end{aligned}$$

Folglich war die Annahme $i(\mathfrak{T}_{\boldsymbol{y}}^{-1}\mathfrak{Q}^{a-b}) > 0$ falsch. □

Bemerkung 15.14. *Für $t_{\boldsymbol{y}} \leq e^* - s(\mathfrak{Q})$ und $\mathfrak{H} := \mathfrak{Q}^b$ besitzt das Gleichungssystem (15.7) eine eindeutige Lösung.*

Beweis. Der Existenzbeweis unterscheidet sich nicht von dem zu Bemerkung 15.6. Es ist also nur die Eindeutigkeit der Lösung zu zeigen. Seien also $\boldsymbol{e}$ und $\boldsymbol{f}$ Lösungen von (15.7). Genauso wie im Beweis zu Bemerkung 15.6 wird dann $\boldsymbol{h} := (h_1, \ldots, h_n)$ definiert durch

$$h_i := \begin{cases} e_i - f_i & \text{falls } i \in J_u \\ 0 & \text{sonst} \end{cases}$$

und ist ein Codewort aus C^* vom Gewicht

$$w(\boldsymbol{h}) \leq \#J_u \leq \deg(\mathfrak{H}) = \deg(\mathfrak{Q}^b).$$

Aufgrund der Konstruktion von b ist $\dim(\mathfrak{T}_{\boldsymbol{y}}^{-1}\mathfrak{Q}^{b-1}) = 0$, woraus $\dim(\mathfrak{Q}^{b-1}) \leq t_{\boldsymbol{y}}$ folgt. Mit der Voraussetzung $t_{\boldsymbol{y}} \leq e^* - s(\mathfrak{Q})$ und der Definiton von $s(\mathfrak{Q})$ ergibt sich daraus

$$\lfloor(\deg(\mathfrak{Q}^b) + 1)/2\rfloor \leq s(\mathfrak{Q}) + \dim(\mathfrak{Q}^{b-1}) \leq s(\mathfrak{Q}) + t_{\boldsymbol{y}} \leq e^*.$$

Somit hat $\boldsymbol{h}$ wegen $w(\boldsymbol{h}) = \deg(\mathfrak{Q}^b) \leq 2e^* = 2\lfloor(d_C^* - 1)/2\rfloor \leq d_C^* - 1$ Gewicht 0. Je zwei Lösungen $\boldsymbol{e}$ und $\boldsymbol{f}$ des Gleichungssytems (15.7) sind also gleich. □

Modifizierter Decodieralgorithmus 15.15. (für $C^* := C^*(\mathfrak{A}, \mathfrak{Q}^a)$)

(I) Man bestimme die Zahl b, indem man die Schritte (1) – (3) des Algorithmus (15.8) für $\mathfrak{H} = \mathfrak{Q}, \mathfrak{Q}^2, \mathfrak{Q}^3, \ldots$ solange durchführt, bis das Gleichungssystem (15.3) für $\mathfrak{H} = \mathfrak{Q}^b$ lösbar ist.

(II) Mit dem Hilfsdivisor $\mathfrak{H} = \mathfrak{Q}^b$ führe man die Schritte (4*) und (5) durch.

Mit den Bemerkungen 15.13 und 15.14 erhält man nun den

Satz 15.16. *Es sei $C^* = C^*(\mathfrak{A}, \mathfrak{G})$ ein dualer arithmetischer Code mit Goppadivisor $\mathfrak{G} = \mathfrak{Q}^a$. Dann können mit dem modifizierten Decodieralgorithmus bis zu $e^* - s(\mathfrak{Q})$ Fehler korrigiert werden.* □

Korollar 15.17. *Die Zahl $s(\mathfrak{Q})$ ist beschränkt durch*

$$\left\lfloor \frac{\deg(\mathfrak{Q}) - 1}{2} \right\rfloor \leq s(\mathfrak{Q}) \leq \left\lfloor \frac{\deg(\mathfrak{Q}) + g - 1}{2} \right\rfloor.$$

Beweis. Als Maximum der Menge $\{\lfloor(\deg(\mathfrak{Q}^{i+1}) + 1)/2\rfloor - \dim(\mathfrak{Q}^i)\rfloor : i \in \mathbb{Z}\}$ erfüllt $s(\mathfrak{Q})$ die erste Ungleichung $s(\mathfrak{Q}) \geq \lfloor(\deg(\mathfrak{Q}^1)+1)/2\rfloor - \dim(\mathfrak{Q}^0) = \lfloor(\deg(\mathfrak{Q})+1)/2\rfloor$. Für natürliche Zahlen i mit $\dim(\mathfrak{Q}^i) > 0$ gilt $\deg(\mathfrak{Q}^i) - 2\dim(\mathfrak{Q}^i) \leq g - 2$, was aus der Definition des Geschlechts folgt. Also gilt für hinreichend große Zahlen

$$\deg(\mathfrak{Q}^{i+1}) + 1 - 2\dim(\mathfrak{Q}^{\mathrm{i}}) \leq \deg(\mathfrak{Q}) + g - 1.$$

Das zeigt die zweite Abschätzung. □

Anmerkung 15.18. Die obere Schranke für $s(\mathfrak{Q})$ kann für spezielle Divisoren verbessert werden (vergleiche z.B. die folgende Bemerkung 15.19).

15.3 Decodierung elliptischer und hyperelliptischer Codes

Bemerkung 15.19. *Es sei $F{:}\mathbb{F}_q$ ein elliptischer oder hyperelliptischer Funktionenkörper. Dann ist $s(\mathfrak{H}) = 0$ für hyperelliptische Divisoren $\mathfrak{H} \in \mathbb{D}_{F:\mathbb{F}_q}$.*

Beweis. Wegen $\deg(\mathfrak{H}) = \dim(\mathfrak{H}) = 2$ gilt $\lfloor(\deg(\mathfrak{H}^{i+1})+1)/2\rfloor - \dim(\mathfrak{H}^i) = (i+1) - \dim(\mathfrak{H}^i) \leq 0$. Mit $i = 0$ folgt dann die Behauptung. □

Aufgabe 15.20. Es seien $F{:}\mathbb{F}_q$ ein Kongruenzfunktionenkörper und $\mathfrak{H} \in \mathbb{D}_{F:\mathbb{F}_q}$ ein Divisor mit $s(\mathfrak{H}) = 0$. Zeigen Sie:

(a) Entweder gilt $g_{F:\mathbb{F}_q} \leq 1$ oder es ist $F{:}\mathbb{F}_q$ hyperelliptisch.

(b) Der Divisor $\mathfrak{H}$ (oder $\mathfrak{H}^2$) ist ein hyperelliptischer Divisor.

Kapitel 16

Arithmetische Teilkörpercodes

In diesen Kapitel betrachten wir die Teilkörpercodes, die durch den Körperabstieg von $\mathbb{F}_q$ nach $\mathbb{F}_r \leq \mathbb{F}_q$ aus arithmetischen Codes über $\mathbb{F}_q$ konstruiert werden. Dabei seien q, r Primzahlpotenzen von p mit $q = r^m$. Die Galoisgruppe $\mathrm{Gal}(\mathbb{F}_q{:}\mathbb{F}_r)$ wird erzeugt vom Frobeniusautomorphismus $\phi : a \mapsto a^r$. Für einen Code $C \leq \mathbb{F}_q^n$ bezeichne $C|_{\mathbb{F}_r}$ wie in Kapitel 4 den auf $\mathbb{F}_r$ *eingeschränkten Code* $C \cap \mathbb{F}_r$ und $\mathrm{Tr}_{\mathbb{F}_q:\mathbb{F}_r}(C)$ den *Spurcode* von C, der durch die Abbildung $\mathrm{Tr}_{\mathbb{F}_q:\mathbb{F}_r} : (x_1, \ldots, x_n) \mapsto (\mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_r}(x_1), \ldots, \mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_r}(x_n))$ erzeugt wird. Wenn keine Mißverständnisse möglich sind, schreiben wir auch abkürzend $\mathrm{Tr}(C)$ für den Spurcode. Genauso wie die Spurabbildung erweitern wir den Frobeniusautomorphismus auf Codewörter via $\phi((x_1, \ldots, x_n)) = (\phi(x_1), \ldots, \phi(x_n))$.

16.1 Dimension arithmetischer Teilkörpercodes

Mit den Bezeichnungen der Einleitung gilt folgende Verschärfung des Korollars 4.16 aus Teil I.

Bemerkung 16.1. *Sind sowohl B als auch $\phi(B)$ Teilcodes von C, so gilt*

$$\dim_{\mathbb{F}_r}(\mathrm{Tr}(C)) - \dim_{\mathbb{F}_r}(B|_{\mathbb{F}_r}) \leq m \cdot (\dim_{\mathbb{F}_q}(C) - \dim_{\mathbb{F}_q}(B)).$$

Beweis. Die Abbildung $\psi : B \to C, \boldsymbol{x} \mapsto \phi(\boldsymbol{x}) - \boldsymbol{x}$ ist linear mit Kern $B|_{\mathbb{F}_r}$. Das Bild $\psi(B)$ liegt im Kern der Spurabbildung $\mathrm{Tr} : C \to C|_{\mathbb{F}_r}$, da für alle Elemente $a \in \mathbb{F}_q$ die Gleichung $\mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_r}(\phi(a) - a) = 0$ gilt. Somit ergibt sich mit der Dimensionformel für lineare Abbildungen

$$\begin{aligned}
\dim_{\mathbb{F}_r}(\mathrm{Tr}(C)) &= \dim_{\mathbb{F}_r}(C) - \dim_{\mathbb{F}_r}(\mathrm{Kern}(\mathrm{Tr})) \\
&\leq \dim_{\mathbb{F}_r}(C) - \dim_{\mathbb{F}_r}(\psi(B)) \\
&= \dim_{\mathbb{F}_r}(C) - (\dim_{\mathbb{F}_r}(B) - \dim_{\mathbb{F}_r}(\mathrm{Kern}(\psi))) \\
&= m \cdot (\dim_{\mathbb{F}_q}(C) - \dim_{\mathbb{F}_q}(B)) + \dim_{\mathbb{F}_r}(\mathrm{Kern}(\psi)).
\end{aligned}$$

Das zeigt die Behauptung. □

Zusammen mit dem Satz von *Delsarte* (4.15) ergibt sich unmittelbar

Korollar 16.2. *Sind B und $\phi(B)$ Teilcodes des dualen Codes $C^* = C^\perp$ von C, so gilt die Ungleichung*

$$\dim_{\mathbb{F}_r}(C|_{\mathbb{F}_r}) + \dim_{\mathbb{F}_r}(B|_{\mathbb{F}_r}) \geq m \cdot (\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(B)) - (m-1) \cdot n.$$

Beweis. Nach dem Satz von *Delsarte* gilt $C|_{\mathbb{F}_r} = \mathrm{Tr}\left(C^\perp\right)^\perp$. Dann folgt mit der obigen Bemerkung

$$\begin{aligned}\dim_{\mathbb{F}_r}(C|_{\mathbb{F}_r}) &= \dim_{\mathbb{F}_r}\left(\mathrm{Tr}\left(C^\perp\right)^\perp\right)\\ &= n - \dim_{\mathbb{F}_r}(\mathrm{Tr}\left(C^\perp\right))\\ &\geq n - (\ \dim_{\mathbb{F}_r}(B|_{\mathbb{F}_r}) + m \cdot (\dim_{\mathbb{F}_q}(C^\perp) - \dim_{\mathbb{F}_q}(B))\ ).\end{aligned}$$

Wegen $\dim_{\mathbb{F}_q}(C^\perp) = n - \dim_{\mathbb{F}_q}(C)$ ist das schon die behauptete Ungleichung. □

Satz 16.3. (Dimension arithmetischer Teilkörpercodes)
Es seien F:$\mathbb{F}_q$ ein algebraischer Funktionenkörper und $C = C(\mathfrak{A}, \mathfrak{G})$ ein arithmetischer Code über F mit $\deg(\mathfrak{A}) > \deg(\mathfrak{G})$. Weiter sei $\mathfrak{H} \in \mathbb{D}_{F:\mathbb{F}_q}$ ein Divisor, für den sowohl $\mathfrak{H}^{-1}\mathfrak{G}$ als auch $\mathfrak{H}^{-r}\mathfrak{G}$ ganz sind. Ist $\mathfrak{H}$ selbst ganz, so sei $\varepsilon = 1$ und sonst sei $\varepsilon = 0$. Dann gelten:

(a) *Der Spurcode von C besitzt die Dimension*

$$\dim_{\mathbb{F}_r}(\mathrm{Tr}(C)) \leq m \cdot (\dim(\mathfrak{G}) - \dim(\mathfrak{H})) + \varepsilon.$$

(b) *Die Einschränkung des dualen Codes $C^* = C^*(\mathfrak{A}, \mathfrak{G})$ auf $\mathbb{F}_r$ hat Dimension*

$$\dim_{\mathbb{F}_r}(C^*|_{\mathbb{F}_r}) \geq n - m \cdot (\dim(\mathfrak{G}) - \dim(\mathfrak{H})) - \varepsilon.$$

Beweis. (a) Da sowohl $\mathfrak{H}^{-1}\mathfrak{G}$ als auch $\mathfrak{H}^{-r}\mathfrak{G}$ ganz sind, ist jede Funktion $x \in \mathcal{L}(\mathfrak{H})$ und ihre r-te Potenz x^r in $\mathcal{L}(\mathfrak{G})$ enthalten, d.h. sowohl $\boldsymbol{x}$ als auch $\boldsymbol{x^r}$ sind Codewörter aus C. Bezeichnet B den arithmetischen Code $C(\mathfrak{A}, \mathfrak{H})$, so ist neben B auch $\phi(B)$ ein Teilcode von C. Wegen $\deg(\mathfrak{H}) \leq \deg(\mathfrak{G}) < \deg(\mathfrak{A})$ haben die Codes B und C nach Korollar 11.4 Dimension $\dim(\mathfrak{H})$ bzw. $\dim(\mathfrak{G})$ über $\mathbb{F}_q$. Aus obiger Bemerkung 16.1 folgern wir nun

$$\dim_{\mathbb{F}_r}(\mathrm{Tr}(C)) \leq m \cdot (\dim(\mathfrak{G}) - \dim(\mathfrak{H})) + \dim_{\mathbb{F}_r}(B|_{\mathbb{F}_r}).$$

Wir zeigen nun, daß $\dim_{\mathbb{F}_r}(B|_{\mathbb{F}_r}) = \varepsilon$ gilt. Es sei $\boldsymbol{x}$ ein Codewort aus $B|_{\mathbb{F}_r}$ mit der zugehörigen Funktion $x \in \mathcal{L}(\mathfrak{H})$. Dann sind x, x^r und $x^r - x$ Elemente des Raumes $\mathcal{L}(\mathfrak{G})$ und es folgt wegen $x(\mathfrak{P}_\mathrm{i}) \in \mathbb{F}_r$ die Gleichung $(x^r - x)(\mathfrak{P}_i) = 0$ für alle Primteiler $\mathfrak{P}_i$ von $\mathfrak{A}$. Also ist $x^r - x$ eine Funktion aus $\mathcal{L}(\mathfrak{A}^{-1}\mathfrak{G})$ und als solche nach Voraussetzung die Nullfunktion. Somit ist x konstant und es gilt

$$\dim_{\mathbb{F}_r}(B|_{\mathbb{F}_r}) = \dim_{\mathbb{F}_r}(\mathcal{L}(\mathfrak{H}) \cap \mathbb{F}_r) = \varepsilon.$$

(b) Nach dem Satz von *Delsarte* gilt $\dim_{\mathbb{F}_r}(C^*|_{\mathbb{F}_r}) = n - \dim_{\mathbb{F}_r}(\mathrm{Tr}(C))$, womit Aussage (b) aus (a) folgt. □

Anmerkung 16.4. Man beachte, daß es stets ein Divisor $\mathfrak{H}$ gibt, der die Voraussetzung zu Satz 16.3 erfüllt. Hat der Goppadivisor $\mathfrak{G}$ nämlich die Gestalt $\mathfrak{N}^{-1}\mathfrak{B}^r\mathfrak{C}$ mit ganzen Divisoren $\mathfrak{B}, \mathfrak{C}, \mathfrak{N}$, so kann man $\mathfrak{H} = \mathfrak{N}^{-1}\mathfrak{B}$ wählen.

Satz 16.3 ist eine Verschärfung von Korollar 4.16, wie das folgende Beispiel zeigt.

Beispiel 16.5. (Klassische Goppa-Codes)
Wir erinnern an die Definition der klassischen Goppa-Codes aus Kapitel 10. Für ein normiertes Polynom $g(X) \in \mathbb{F}_q[X]$ und den Vektor $\boldsymbol{a} = (a_1, \ldots, a_n)$ mit paarweise verschiedenen Koeffizienten a_i aus $\mathbb{F}_q$ und $g(a_i) \neq 0$ ist der klassische Goppa-Code $\Gamma(\boldsymbol{a}, g)$ definiert durch

$$\Gamma(\boldsymbol{a}, g) := \left\{ (x_1, \ldots, x_r) \in \mathbb{F}_r^{\,n} : \sum_{i=1}^{n} \frac{x_i}{X - a_i} \equiv 0 \pmod{g(X)} \right\}.$$

$\Gamma(\boldsymbol{a}, g)$ tritt als Teilkörpercode $\tilde{\Gamma}(\boldsymbol{a}, g)|_{\mathbb{F}_r}$ von

$$\tilde{\Gamma}(\boldsymbol{a}, g) := \left\{ (x_1, \ldots, x_r) \in \mathbb{F}_q^{\,n} : \sum_{i=1}^{n} \frac{x_i}{X - a_i} \equiv 0 \pmod{g(X)} \right\}$$

auf. Dieses Beispiel können wir mit der Theorie der arithmetischen Codes behandeln. Es sei $\mathbb{F}_q(x)$ ein rationaler Funktionenkörper und es bezeichne $(x - a_i) = \mathfrak{P}_i\mathfrak{P}_\infty^{-1}$ für $i = 1, \ldots, n$ sowie $(g(x)) = \mathfrak{G}\mathfrak{P}_\infty^{-\deg(g)}$. Wir zeigen, daß mit dem Auswertungsdivisor $\mathfrak{A} := \prod_{i=1}^{n} \mathfrak{P}_i$ und dem Goppadivisor $\tilde{\mathfrak{G}} := \mathfrak{G}\mathfrak{P}_\infty^{-1}$

$$\tilde{\Gamma}(\boldsymbol{a}, g) = C^*(\mathfrak{A}, \tilde{\mathfrak{G}}) \qquad \text{und} \qquad \Gamma(\boldsymbol{a}, g) = C^*(\mathfrak{A}, \tilde{\mathfrak{G}})|_{\mathbb{F}_r}$$

gelten. Der duale arithemtische Code $C^*(\mathfrak{A}, \tilde{\mathfrak{G}})$ besteht nämlich aus den Codewörtern

$$(\mathrm{Res}_{\mathfrak{P}_1}(\delta), \ldots, \mathrm{Res}_{\mathfrak{P}_n}(\delta)) \qquad \text{für Differentiale } \delta \in \Delta(\mathfrak{A}^{-1}\tilde{\mathfrak{G}}).$$

Für $i = 1, \ldots, n$ ist $\frac{dx}{x - a_i}$ ein Differential aus $\Delta(\mathfrak{A}^{-1}\mathfrak{P}_\infty^{-1}) \leq \Delta(\mathfrak{A}^{-1}\tilde{\mathfrak{G}})$. Nach dem Satz von *Riemann-Roch* gilt $\dim(\Delta(\mathfrak{A}^{-1}\mathfrak{P}_\infty^{-1})) = i(\mathfrak{A}^{-1}\mathfrak{P}_\infty^{-1}) = -\deg(\mathfrak{A}^{-1}\mathfrak{P}_\infty^{-1}) - 1 = n$ und somit

$$\Delta(\mathfrak{A}^{-1}\mathfrak{P}_\infty^{-1}) = \left\langle \frac{dx}{x - a_i} : i = 1, \ldots, n \right\rangle.$$

Folglich gilt dann

$$\Delta(\mathfrak{A}^{-1}\tilde{\mathfrak{G}}) = \left\{ \sum_{i=1}^{n} \frac{x_i dx}{x - a_i} : \boldsymbol{x} \in \mathbb{F}_q^{\,n} \text{ mit } \sum_{i=1}^{n} \frac{x_i}{x - a_i} \equiv 0 \pmod{g(x)} \right\}.$$

Das Residuum des Differentials $\delta = \sum_{i=1}^{n} \frac{x_i}{x - a_i}$ an der Stelle $\mathfrak{P}_i = (x - a_i)_0$ ist dann $\mathrm{Res}_{\mathfrak{P}_i}(\delta) = x_i$ für $i = 1, \ldots, n$, was die Gleichheit von $\tilde{\Gamma}(\boldsymbol{a}, g)$ und $C^*(\mathfrak{A}, \tilde{\mathfrak{G}})$ beweist.

Nach Korollar 4.16 ist die Dimension von $\Gamma(\boldsymbol{a}, g)$ nach unten beschränkt durch $n - m \cdot \dim_{\mathbb{F}_q}(\tilde{\Gamma}(\boldsymbol{a}, g)^{\perp})$ bzw. durch $n - m \cdot \dim_{\mathbb{F}_q}(C(\mathfrak{A}, \tilde{\mathfrak{G}}))$. Aus $\dim_{\mathbb{F}_q}(C(\mathfrak{A}, \tilde{\mathfrak{G}})) = \dim(\tilde{\mathfrak{G}}) = \deg(\tilde{\mathfrak{G}}) + 1 = \deg(g)$ folgt daher

$$\dim_{\mathbb{F}_r}(\Gamma(\boldsymbol{a}, g)) \geq n - m \deg(g).$$

Dies ist das gleiche Ergebnis wie von Satz 10.5 aus Teil I. Wir nehmen nun an, daß sich das Polynom $g(X)$ in $\mathbb{F}_q[X]$ zu $g(X) = b(X)^r c(X)$ zerlegen läßt. Dann hat der Divisor $\tilde{\mathfrak{B}} = \mathfrak{B}\mathfrak{P}_\infty^{-1}$ mit $\mathfrak{B} = (b(x))_0$ die Dimension $\deg(b)$ und es gilt mit Satz 16.3 (b) die schärfere Ungleichung

$$\dim_{\mathbb{F}_r}(\Gamma(\boldsymbol{a}, g)) \geq n - m(\dim(\tilde{\mathfrak{G}}) - \dim(\tilde{\mathfrak{B}})) = n - m(\deg(g) - \deg(b)).$$

16.2 Distanz arithmetischer Teilkörpercodes

Satz 16.6. *Es seien $F{:}\mathbb{F}_q$ ein algebraischer Funktionenkörper vom Geschlecht g und $q = r^m$ mit $m > 1$. Der Goppadivisor $\mathfrak{G}$ des arithmetischen Codes $C(\mathfrak{A}, \mathfrak{G})$ habe die Form $\mathfrak{N}^{-1}\mathfrak{B}^r\mathfrak{C}$ mit ganzen Divisoren $\mathfrak{B}, \mathfrak{C}, \mathfrak{N} \in \mathbb{D}_{F:\mathbb{F}_q}$ und $\mathfrak{H} := \mathfrak{N}^{-1}\mathfrak{B}$ habe mindestens Grad $2g - 1$. Ist $\mathfrak{E}$ das Produkt aller Primteiler $\mathfrak{Q}$ von $\mathfrak{C}$ mit Ordnung $\mathrm{ord}_{\mathfrak{Q}}(\mathfrak{C}) \equiv -1 \pmod r$, so gilt*

$$C^*(\mathfrak{A}, \mathfrak{G})|_{\mathbb{F}_r} = C^*(\mathfrak{A}, \mathfrak{G}\mathfrak{E})|_{\mathbb{F}_r} \qquad \textit{mit } \mathfrak{E} := \prod_{\substack{\mathfrak{Q} \in \mathbb{P}_{F:\mathbb{F}_q} \\ \mathrm{ord}_{\mathfrak{Q}}(\mathfrak{C}) \equiv -1 \pmod r}} \mathfrak{Q}.$$

Beweis. Nach dem Satz von *Delsarte* genügt es, $\mathrm{Tr}(C(\mathfrak{A}, \mathfrak{G})) = \mathrm{Tr}(C(\mathfrak{A}, \mathfrak{G}\mathfrak{E}))$ zu zeigen. Die Inklusion $\mathrm{Tr}(C(\mathfrak{A}, \mathfrak{G})) \leq \mathrm{Tr}(C(\mathfrak{A}, \mathfrak{G}\mathfrak{E}))$ ist offensichtlich wegen der Ganzheit von $\mathfrak{E}$. Es bleibt die umgekehrte Richtung zu zeigen. Wegen $\deg(\mathfrak{H}) > 2g-2$ gilt nach dem Satz von *Riemann-Roch* $\dim(\mathfrak{H}\mathfrak{E}) = \deg(\mathfrak{H}\mathfrak{E}) - g + 1 = \dim(\mathfrak{H}) + \deg(\mathfrak{E})$. Es sei $s := \deg(\mathfrak{E})$ und $\{u_1, \ldots, u_s\}$ ein Vertretersystem einer Basis von $\mathcal{L}(\mathfrak{H}\mathfrak{E})$ modulo $\mathcal{L}(\mathfrak{H})$. Wir ergänzen dieses System mit $\{v_1, \ldots, v_t\}$ zu einer Basis von $\mathcal{L}(\mathfrak{G})$. Es ist also $s + t = \dim(\mathfrak{G})$. Da für alle Teiler $\mathfrak{Q}$ von $\mathfrak{E}$

$$\mathrm{ord}_{\mathfrak{Q}}(\mathfrak{C}\mathfrak{E}^{1-r}) = \mathrm{ord}_{\mathfrak{Q}}(\mathfrak{C}) + (1 - r) \geq 0$$

gilt, ist $(\mathfrak{H}\mathfrak{E})^{-r}\mathfrak{G}\mathfrak{E} = \mathfrak{N}^{r-1}\mathfrak{C}\mathfrak{E}^{1-r}$ ein ganzer Divisor. Somit ist $\mathcal{L}((\mathfrak{H}\mathfrak{E})^r)$ in $\mathcal{L}(\mathfrak{G}\mathfrak{E})$ enthalten. Die Funktionen $u_1, \ldots, u_s, v_1, \ldots, v_t, u_1^r, \ldots, u_s^r$ erzeugen daher einen $\mathbb{F}_r$-Unterraum von $\mathcal{L}(\mathfrak{G}\mathfrak{E})$. Wären diese linear abhängig, so gäbe es eine Linearkombination

$$z := \sum_{i=1}^{s} a_i u_i^r = \sum_{i=1}^{s} b_i u_i + \sum_{j=1}^{t} c_j v_j \ \in \mathcal{L}(\mathfrak{G})$$

mit $z \neq 0$. Dabei ist z das Bild der Variablen $u := \sum_{i=1}^{s} \phi^{-1}(a_i) u_i$ aus $\mathcal{L}(\mathfrak{H}\mathfrak{E}) \backslash \mathcal{L}(\mathfrak{H})$ unter der Frobeniusabbildung ϕ. Andererseits folgte aus $z = u^r \in \mathcal{L}(\mathfrak{G}) = \mathcal{L}(\mathfrak{N}^{-1}\mathfrak{B}^r\mathfrak{C})$, daß u Element des Raumes $\mathcal{L}(\mathfrak{N}^{-1}\mathfrak{B}) = \mathcal{L}(\mathfrak{H})$ ist, da nach Voraussetzung in $\mathfrak{C}$ keine

r-te Potenz aufgeht. Somit wären $u = 0$ und $z = 0$ im Widerspruch zur Annahme. Also sind die Funktionen $u_1, \ldots, u_s, v_1, \ldots, v_t, u_1^r, \ldots, u_s^r$ linear unabhängig in $\mathcal{L}(\mathfrak{GE})$. Desweiteren erzeugen sie diesen Raum, da nach dem Satz von *Riemann-Roch* $\dim(\mathfrak{GE}) = \dim(\mathfrak{G}) + s$ gilt. Der Code $C(\mathfrak{A}, \mathfrak{GE})$ hat also die Basiselemente $\boldsymbol{u_1}, \ldots, \boldsymbol{u_s}, \boldsymbol{v_1}, \ldots, \boldsymbol{v_t}, \boldsymbol{u_1^r}, \ldots, \boldsymbol{u_s^r}$. Die Codewörter $\boldsymbol{u_1}, \ldots, \boldsymbol{u_s}, \boldsymbol{v_1}, \ldots, \boldsymbol{v_t}$ sind auch in $C(\mathfrak{A}, \mathfrak{G})$ enthalten. Also gilt

$$C(\mathfrak{A}, \mathfrak{GE}) \leq C(\mathfrak{A}, \mathfrak{G}) + \phi\left(C(\mathfrak{A}, \mathfrak{G})\right),$$

woraus schließlich die gewünschte Ungleichung

$$\mathrm{Tr}(C(\mathfrak{A}, \mathfrak{GE})) \leq \mathrm{Tr}(C(\mathfrak{A}, \mathfrak{G})) + \mathrm{Tr}(\phi\left(C(\mathfrak{A}, \mathfrak{G})\right)) = \mathrm{Tr}(C(\mathfrak{A}, \mathfrak{G}))$$

folgt. □

Der Code $C^*(\mathfrak{A}, \mathfrak{GE})$ hat nach Satz 11.2 Minimaldistanz $d^* \geq \deg(\mathfrak{GE}) - 2g + 2$, was natürlich auch auf seine Einschränkung auf $\mathbb{F}_r$ zutrifft. Somit folgt aus obigem Satz 16.6 das

Korollar 16.7. *Für die Minimaldistanz des auf $\mathbb{F}_r$ eingeschränkten Codes $C^*(\mathfrak{A}, \mathfrak{G})|_{\mathbb{F}_r}$ gilt*

$$d(C^*(\mathfrak{A}, \mathfrak{G})|_{\mathbb{F}_r}) \geq \deg(\mathfrak{G}) + \deg(\mathfrak{E}) - 2g + 2. \qquad \square$$

Beispiel 16.8. (Klassische Goppa-Codes)
Korollar 16.7 liefert ebenfalls eine Verschärfung für die Parameter der klassischen Goppa-Codes. Mit den Bezeichnungen aus Beispiel 16.5 gilt zunächst für die Minimaldistanz von $\Gamma(\boldsymbol{a}, g)$

$$\begin{aligned} d(\Gamma(\boldsymbol{a}, g)) &\geq d(\tilde{\Gamma}(\boldsymbol{a}, g)) = d(C^*(\mathfrak{A}, \tilde{\mathfrak{G}})) \\ &\geq \deg(\tilde{\mathfrak{G}}) - 2g_{\mathbb{F}_q(x)} + 2 = \deg(g) + 1, \end{aligned}$$

was mit Satz 10.5 übereinstimmt. Gilt allerdings $g(X) = h(X)^{r-1}$ für ein quadratfreies Polynom $h(X) \in \mathbb{F}_q[X]$, so kann man die Minimaldistanz von $\Gamma(\boldsymbol{a}, g)$ besser abschätzen. Dazu bezeichne $\mathfrak{E} = (h(x))_0$. Dann gelten $\mathfrak{G} = \mathfrak{E}^{r-1}$ und $\tilde{\mathfrak{G}} = \mathfrak{E}^{r-1}\mathfrak{P}_\infty^{-1}$. Wir können $\mathfrak{H} = \mathfrak{P}_\infty^{-1}$ wählen, da sowohl $\mathfrak{H}^{-1}\tilde{\mathfrak{G}}$ als auch $\mathfrak{H}^{-r}\tilde{\mathfrak{G}}$ ganz sind. Desweiteren hat $\mathfrak{H}$ Grad $\deg(\mathfrak{H}) = -1 > 2g_{\mathbb{F}_q(x)} - 2$ und daher folgt mit Korollar 16.7

$$\begin{aligned} d(\Gamma(\boldsymbol{a}, g)) &\geq \deg(\tilde{\mathfrak{G}}) + \deg(\mathfrak{E}) + 2 = \deg(g) - 1 + \deg(h) + 2 \\ &= r\deg(h) + 1 = \frac{r}{r-1}\deg(g) + 1. \end{aligned}$$

Dies liefert eine bessere Abschätzung der Minimaldistanz von $\Gamma(\boldsymbol{a}, g)$.

Aufgabe 16.9. Es seien $r = 3$ und $q = 27$ sowie $F = \mathbb{F}_{27}(x, y)$ definiert durch

$$y^2 = x^3 - x^2 - 1.$$

(a) Zeigen Sie: F besitzt 38 rationale Stellen, d.h. die Kurve $y^2 = x^3 - x^2 - 1$ über $\mathbb{F}_{27}$ ist "maximal".

(b) Es seien die Standardcodes $C_m = C(\mathfrak{A}, \mathfrak{O}^m)$ definiert durch den in $F{:}\mathbb{F}_{27}(x)$ total verzweigten Polstellendivisor $\mathfrak{O}$ von x und dem Auswertungsdivisor $\mathfrak{A} = \prod_{\mathfrak{P} \neq \mathfrak{O}} \mathfrak{P}$ (Produkt aller rationalen Stellen $\mathfrak{P} \neq \mathfrak{O}$ von $F{:}\mathbb{F}_{27}$) sowie $1 \leq m \leq 16$. Berechnen Sie die Dimension und Distanz der Teilkörpercodes $C_m|_{\mathbb{F}_3}$ und vergleichen Sie die Ergebnisse mit denen der Sätze 16.3 und 16.6.

Untersuchen Sie analog Standardcodes der folgenden Funktionenkörper:

(1) $r = 2, q = 16$ und $F = \mathbb{F}_{16}(x, y)$ mit $y^2 + y = x^3 + x + 1$,

(2) $r = 5, q = 25$ und $F = \mathbb{F}_{25}(x, y)$ mit $y^2 = x^6 + 1$.

16.3 Parameter klassischer Goppa-Codes*

In diesen Abschnitt beschränken wir uns auf den Fall $r = p$ prim und $q = p^m$. Desweiteren greifen wir auf Ergebnisse der Artin-Schreier-Theorie (Satz 18.2) und der *Serre-Schranke* (Satz 19.4) vor.

Definition 16.10. (Ausgeartete Funktion)
Es sei $F{:}K$ ein algebraischer Funktionenkörper der Charakteristik p. Eine Funktion $z \in F$ der Gestalt

$$z = u^p - u + a$$

mit $u \in F$ und $a \in K$ nennen wir **ausgeartete Funktion**.

Notiz 16.11. Es sei $z = u^p - u + a$ eine ausgeartete Funktion. Dann hat das Codewort $\boldsymbol{z} = (z(\mathfrak{P}_1), \ldots, z(\mathfrak{P}_n))$ unter der (erweiterten) Spurabbildung $\mathrm{Tr}_{\mathbb{F}_q:\mathbb{F}_p}$ das Bild

$$\mathrm{Tr}_{\mathbb{F}_q:\mathbb{F}_p}((z(\mathfrak{P}_1), \ldots, z(\mathfrak{P}_n))) = b \cdot (1, \ldots, 1)$$

mit $b = \mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_p}(a)$.

Bemerkung 16.12. *Es seien $F = \mathbb{F}_q(x)$ ein rationaler Funktionenkörper und $z \in F$ eine nicht-ausgeartete Funktion. Den Zerfällungskörper von $f(T) = T^p - T - z$ über F bezeichnen wir mit E_z. Dann gelten:*

(a) *Die Körpererweiterung $E_z{:}F$ ist geometrisch mit zyklischer Galoisgruppe vom Grad p.*

(b) *Es sei $\mathfrak{P} \in \mathbb{P}^{(1)}_{F:\mathbb{F}_q}$ eine rationale Stelle in F mit $z(\mathfrak{P}) \neq \infty$.*

Dann ist $\mathfrak{P}$ in $E_z{:}F$ $\left\{\begin{matrix} \textit{träge} \\ \textit{voll zerlegt} \end{matrix}\right\}$, falls $\left\{\begin{matrix} \mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_p}(z(\mathfrak{P})) \neq 0 \\ \mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_p}(z(\mathfrak{P})) = 0 \end{matrix}\right\}$ gilt.

(c) *Es seien $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ paarweise verschiedene rationale Stellen in F. Dann hat das Codewort $(z(\mathfrak{P}_1), \ldots, z(\mathfrak{P}_n))$ unter der Spurabbildung $\mathrm{Tr}_{\mathbb{F}_q:\mathbb{F}_p}$ das Gewicht*

$$w_z := w(\mathrm{Tr}_{\mathbb{F}_q:\mathbb{F}_p}((z(\mathfrak{P}_1), \ldots, z(\mathfrak{P}_n))) = n - \frac{N_1(E_z) - s_z}{p}$$

mit $0 \leq s_z \leq p(q+1-n)$, wobei $N_1(E_z) = \#\mathbb{P}^{(1)}_{E_z:\mathbb{F}_q}$ die Anzahl aller rationalen Stellen in E_z bezeichne.

Beweis. Die Aussage (a) folgt aus dem Hauptsatz der Artin-Schreier Theorie, den wir in allgemeinerer Form in Kapitel 18 (Satz 18.2) beweisen werden.
(b) Es sei $\mathfrak{P}$ eine rationale Stelle in F mit $z(\mathfrak{P}) \neq \infty$. Dann ist $c := z(\mathfrak{P}) \in \mathbb{F}_q$ eine Konstante von F und $f_c(X) = X^p - X - c$ ein Polynom über $\mathbb{F}_q$. Nach *Hilberts Satz 90* [Lan02] verschwindet $\mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_p}(c)$ genau dann, wenn $c = b^p - b$ für ein $b \in \mathbb{F}_q$ gilt. Da dann mit b für alle Konstanten $a \in \mathbb{F}_p$ auch $b + a$ Nullstellen von f_c sind, ist f_c entweder irreduzibel oder zerfällt komplett in verschiedene Linearfaktoren. Nach dem *Dedekind-Kriterium* entsprechen hierbei die irreduziblen Faktoren von $f_c = f_{z(\mathfrak{P})}$ umkehrbar eindeutig den Primteilern von $\mathfrak{P}$ in E_z. Gilt also $\mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_p}(c) = 0$, so zerfällt f_c komplett in Linearfaktoren und es ist $\mathfrak{P}$ voll zerlegt in E_z. Im anderen Fall gilt $\mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_p}(c) \neq 0$ und somit ist f_c irreduzibel und $\mathfrak{P}$ träge in $E_z{:}F$.
(c) Es sei $\mathbb{S} \subset \mathbb{P}^{(1)}_{F:\mathbb{F}_q}$ die Menge aller rationalen Stellen in F außer $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$. Dann hat $\mathbb{S}$ die Mächtigkeit $s = q + 1 - n$. Desweiteren sei $\mathbb{S}_z \subset \mathbb{P}^{(1)}_{E_z:\mathbb{F}_q}$ die Menge aller rationalen Stellen in E_z, die als Erweiterung einer Stelle aus $\mathbb{S}$ auftreten, d.h. es ist $\mathbb{S}_z = \{\mathfrak{P} \in \mathbb{P}^{(1)}_{E_z:\mathbb{F}_q} : \mathfrak{P}|_F \in \mathbb{S}\}$. Die Kardinalität s_z von $\mathbb{S}_z$ ist dann beschränkt durch $s_z \leq ps$. Das Wort $\mathrm{Tr}((z(\mathfrak{P}_1), \ldots, z(\mathfrak{P}_n)))$ hat Gewicht

$$w_z = n - \#\{\mathfrak{P}_i : 1 \leq i \leq n, \mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_p}(z(\mathfrak{P}_i)) = 0\}.$$

Nach Aussage (b) ist die Anzahl aller $\mathfrak{P}_i$ mit $\mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_p}(z(\mathfrak{P}_i)) = 0$ aber genau

$$\frac{1}{p}\#\{\ \mathfrak{P} \in \mathbb{P}^{(1)}_{E_z:\mathbb{F}_q} : \mathfrak{P}|_F \in \{\mathfrak{P}_1, \ldots, \mathfrak{P}_n\}\ \} = \frac{1}{p}\ (N_1(E_z) - s_z).$$

Das zeigt unsere Behauptung. □

Korollar 16.13. *Es seien $z \in F = K(t)$ eine nicht-ausgeartete Funktion aus $\mathcal{L}(\mathfrak{G})$ mit $\mathfrak{G} = \mathfrak{N}^{-1}\mathfrak{B}$ sowie $\mathfrak{E} := \prod_{\mathfrak{P}|\mathfrak{B}} \mathfrak{P}$ das Produkt aller Primteiler von $\mathfrak{B}$. Dann gilt für das Geschlecht von $E_z{:}\mathbb{F}_q$ die obere Schranke*

$$g_{E_z:\mathbb{F}_q} \leq \frac{p-1}{2}\ (\deg(\mathfrak{B}\mathfrak{E}) - 2).$$

Beweis. Nach der Theorie der Artin-Schreier-Erweiterungen gilt für die Differente $\mathfrak{D}(E_z{:}F)$ der Körpererweiterung $E_z{:}F$

$$\mathfrak{D}(E_z{:}F) = \left(\prod\nolimits_{\mathfrak{P}|(z)_\infty} \mathfrak{P}^{\mathrm{ord}_{\mathfrak{P}}(z)+1}\right)^{p-1}.$$

Wegen $(z)_\infty | \mathfrak{B}$ ist dieser Divisor ein Teiler von $(\mathfrak{B}\mathfrak{E})^{p-1}$. Somit erhalten wir die Ungleichung

$$\deg(\mathfrak{D}(E_z{:}F)) \leq (p-1)\ \deg(\mathfrak{B}\mathfrak{E}).$$

Nach dem Satz von *Hurwitz* hat E_z das Geschlecht $g_{E_z:\mathbb{F}_q} = \frac{1}{2}\ \deg(\mathfrak{D}(E_z{:}F)) - p + 1$. Setzt man die gefundene Ungleichung für den Grad der Differente ein, so folgt die Behauptung. □

Für den Beweis des folgenden Satzes greifen wir auf die Schranke von *Serre* zurück. Diese besagt, daß für einen Kongruenfunktionenkörper $F{:}\mathbb{F}_q$ stets die Abschätzung

$$|N_1(F) - (q+1)| \leq g_{F:\mathbb{F}_q} \lfloor 2\sqrt{q} \rfloor$$

gilt. Dies werden wir später in Abschnitt 19.1 (Satz 19.4) beweisen.

Satz 16.14. *Es sei $C = C(\mathfrak{A}, \mathfrak{G})$ ein rationaler Code über $\mathbb{F}_q$ der Länge n mit Goppadivisor $\mathfrak{G} = \mathfrak{N}^{-1}\mathfrak{B}$. Weiter sei $\mathfrak{E} := \prod_{\mathfrak{P}|\mathfrak{B}} \mathfrak{P}$ das Produkt aller Primteiler von $\mathfrak{B}$. Dann gilt für die Minimaldistanz des Spurcodes von C die untere Schranke*

$$d(\mathrm{Tr}(C)) \geq n - \frac{q+1}{p} - \frac{p-1}{2p} \cdot (\deg(\mathfrak{B}\mathfrak{E}) - 2) \cdot \lfloor 2\sqrt{q} \rfloor.$$

Beweis. Es sei $\boldsymbol{x}$ ein (nichttriviales) Wort des Spurcodes $\mathrm{Tr}(C)$ vom Gewicht $w(\boldsymbol{x}) \notin \{0, n\}$. Nach Notiz 16.11 wird $\boldsymbol{x}$ von einer nicht-ausgearteten Funktion $z \in \mathcal{L}(\mathfrak{G})$ erzeugt, d.h. es ist $\boldsymbol{x} = \mathrm{Tr}(\boldsymbol{z})$. Mit den Bezeichnungen aus Bemerkung 16.12 (c) gelten dann $w(\boldsymbol{x}) = w_z$ und

$$N_1(E_z) = p \cdot (n - w_z) + s_z.$$

Durch Verwendung der *Serre-Schranke* erhalten wir die Ungleichung

$$|p \cdot (n - w_z) + s_z - (q+1)| = |N_1(E_z) - (q+1)| \ \leq\ g_{E_z:\mathbb{F}_q} \lfloor 2\sqrt{q} \rfloor.$$

Mit der Abschätzung des Geschlechts aus Korollar 16.13 läßt sich dies zu

$$\left| (w_z - n) + \frac{(q+1) - s_z}{p} \right| \leq \frac{p-1}{2p} \cdot (\deg(\mathfrak{B}\mathfrak{E}) - 2) \cdot \lfloor 2\sqrt{q} \rfloor$$

umformen. Wir bezeichnen die rechte Seite mit A. Dann gilt mit dieser Abschätzung für das Gewicht von $\boldsymbol{x}$

$$w(\boldsymbol{x}) = w_z \geq n - \frac{(q+1) - s_z}{p} - A = n - \frac{q+1}{p} - A + \frac{s_z}{p}.$$

Einzig der Summand s_z/p ist von der Wahl des Codewortes $\boldsymbol{x}$ abhängig. Da dieser positiv ist, folgt somit die behauptete Abschätzung für die Minimaldistanz des Spurcodes. □

Die untere Schranke aus Satz 16.3 bzw. aus Beispiel 16.5 ist oft scharf. Das zeigt

Satz 16.15. *Es sei $\Gamma(\boldsymbol{a}, g)$ ein klassischer Goppa-Code mit $\boldsymbol{a} \in \mathbb{F}_q^q$ (d.h. $\boldsymbol{a}$ enthält alle Körperelemente von $\mathbb{F}_q$) und $g(X) \in \mathbb{F}_q[X]$ ein normiertes Polynom vom Grad $\deg(g) \geq 2$ ohne Linearfaktoren in $\mathbb{F}_q[X]$. Desweiteren habe $g(X)$ die Form $g(X) = b(X)^p c(X)$, wobei $c(X)$ keine p-ten Potenzen enthalte. Das Polynom $f(X)$ sei das Produkt aller Primteiler von $g(X)$. Gilt dann*

$$2(q+1) > (\deg(g \cdot f) - 2)\lfloor 2\sqrt{q} \rfloor,$$

so hat $\Gamma(\boldsymbol{a}, g)$ die Dimension

$$\dim(\Gamma(\boldsymbol{a}, g)) = q - m(\deg(g) - \deg(b)).$$

Beweis. Wir verwenden die Bezeichnungen aus Beispiel 16.5, d.h. es sind $\mathfrak{P}_\infty = (x)_\infty$, $\mathfrak{G} = (g(x))_0$ und $\tilde{\mathfrak{G}} = \mathfrak{G}\mathfrak{P}_\infty^{-1}$. Desweiteren sei $\mathfrak{A} = \prod_{\mathfrak{P} \neq \mathfrak{P}_\infty} \mathfrak{P}$ das Produkt aller rationalen Stellen aus $\mathbb{F}_q(x)$ außer $\mathfrak{P}_\infty$. Es gelten dann nach 16.5 und dem Satz von *Delsarte*

$$\Gamma(\boldsymbol{a}, g)^\perp = \left(C^*(\mathfrak{A}, \tilde{\mathfrak{G}})|_{\mathbb{F}_p}\right)^\perp = \mathrm{Tr}(C(\mathfrak{A}, \tilde{\mathfrak{G}})).$$

Der Code $\Gamma(\boldsymbol{a}, g)^\perp$ ist also das Bild der aus der Auswertungs- und Spurabbildung zusammengesetzten Abbildung $S : \mathcal{L}(\tilde{\mathfrak{G}}) \twoheadrightarrow C(\mathfrak{A}, \tilde{\mathfrak{G}}) \twoheadrightarrow \mathrm{Tr}(C(\mathfrak{A}, \tilde{\mathfrak{G}}))$ und besitzt die Dimension

$$\dim\left(\Gamma(\boldsymbol{a}, g)^\perp\right) = \dim_{\mathbb{F}_p}(S(\mathcal{L}(\tilde{\mathfrak{G}}))) = \dim_{\mathbb{F}_p}(\mathcal{L}(\tilde{\mathfrak{G}})) - \dim_{\mathbb{F}_p}(\mathrm{Kern}(S)).$$

Wir werden zeigen, daß $\mathrm{Kern}(S)$ isomorph zum linearen Raum $\mathcal{L}(\tilde{\mathfrak{B}})$ mit $\tilde{\mathfrak{B}} := \mathfrak{B}\mathfrak{P}_\infty^{-1}$ und $\mathfrak{B} := (b(x))_0$ ist. Dann folgt die Behauptung des Satzes unmittelbar aus

$$\dim\left(\Gamma(\boldsymbol{a}, g)^\perp\right) = \dim_{\mathbb{F}_p}(\mathcal{L}(\tilde{\mathfrak{G}})) - \dim_{\mathbb{F}_p}(\mathcal{L}(\tilde{\mathfrak{B}})) = m(\deg(g) - \deg(b)).$$

Es genügt also, die Bijektivität der $\mathbb{F}_p-$linearen Abbildung

$$\psi : \left\{ \begin{array}{ccc} \mathcal{L}(\tilde{\mathfrak{B}}) & \longrightarrow & \mathrm{Kern}(S) \leq \mathcal{L}(\tilde{\mathfrak{G}}) \\ u & \longmapsto & u^p - u \end{array} \right.$$

zu zeigen. Man beachte, daß ψ nach *Hilberts Satz 90* wohldefiniert ist. Offensichtlich gilt $u^p - u = 0$ genau dann, wenn u eine Konstante aus $\mathbb{F}_p$ ist. Wegen $\mathcal{L}(\tilde{\mathfrak{B}}) \cap \mathbb{F}_p = \{0\}$ ist dies nur für $u = 0$ möglich, was die Injektivität von ψ zeigt.
Zum Beweis der Surjektivität zeigen wir zunächst, daß $\mathrm{Kern}(S)$ nur ausgeartete Funktionen enthält. Dazu nehmen wir an, daß $z \in \mathrm{Kern}(S) \leq \mathcal{L}(\tilde{\mathfrak{G}})$ eine nichtausgeartete Funktion ist. Wegen $z(\mathfrak{P}_\infty) \neq \infty$ und $\mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_p}(z(\mathfrak{P}_\infty)) = 0$ ist dann $\mathfrak{P}_\infty$ nach Bemerkung 16.12 (b) voll zerlegt in $E_z{:}\mathbb{F}_q(x)$, wobei E_z den Zerfällungskörper von $T^p - T - z$ über $\mathbb{F}_q(x)$ bezeichne. Dann gilt weiter $0 = w_z = q - \frac{N_1(E_z) - p}{p}$ nach 16.12 (c) und somit

$$N_1(E_z) = p(q+1).$$

Desweiteren ist das Geschlecht von $E_z{:}\mathbb{F}_q$ nach Korollar 16.13 beschränkt durch

$$g_{E_z:\mathbb{F}_q} \leq \frac{p-1}{2}\,(\deg(\mathfrak{G}(f(x))_0) - 2) = \frac{p-1}{2}\,(\deg(g \cdot f) - 2).$$

Mit der Schranke von *Serre* folgt dann

$$(p-1)(q+1) = N_1(E_z) - (q+1) \leq g_{E_z:\mathbb{F}_q}\lfloor 2\sqrt{q}\rfloor = \frac{p-1}{2}\,(\deg(g \cdot f) - 2)\lfloor 2\sqrt{q}\rfloor$$

beziehungsweise

$$2(q+1) \leq (\deg(g \cdot f) - 2)\lfloor 2\sqrt{q}\rfloor,$$

was der Voraussetzung des Satzes widerspricht. Also ist jedes Element aus $\mathrm{Kern}(S)$ eine ausgeartete Funktion.

Es sei also $z = u_1^p - u_1 + a$ eine Funktion aus $\mathrm{Kern}(S)$ mit $u_1 \in \mathbb{F}_q(x)$ und $a \in \mathbb{F}_q$. Aus $S(z) = 0$ folgt insbesondere $\mathrm{Spur}_{\mathbb{F}_q:\mathbb{F}_p}(a) = 0$. Nach *Hilberts Satz 90* existiert ein $b \in \mathbb{F}_q$ mit $a = b^p - b$ und somit gilt $z = u^p - u$ mit $u := u_1 + b$. Aus $u^p - u \in \mathcal{L}(\mathfrak{G})$ folgt mit der Dreiecksungleichung für diskrete Bewertungen $u^p \in \mathcal{L}(\mathfrak{G})$ und somit $u \in \mathcal{L}(\mathfrak{B})$. Wegen

$$\prod_{c \in \mathbb{F}_p} (u - c) = u^p - u = z \in \mathcal{L}(\mathfrak{G}\mathfrak{P}_\infty^{-1})$$

ist $\mathfrak{P}_\infty$ Nullstelle eines der Faktoren $u - c$ mit $c \in \mathbb{F}_p$. Dieser ist dann ein Urbild von z unter ψ. □

Kapitel 17

Hermitesche Codes

17.1 Hermitesche Funktionenkörper

Definition 17.1. (Hermitescher Funktionenkörper)
Ein algebraischer Kongruenzfunktionenkörper $F = K(x, y)$ über $K = \mathbb{F}_{q^2}$ mit der definierenden Relation

$$x^{q+1} + y^{q+1} = 1.$$

heißt **Hermitescher Funktionenkörper vom Exponenten $q+1$** oder auch **unitärer Fermatkörper**.

Satz 17.2. (Eigenschaften Hermitescher Funktionenkörper)
Für einen Hermiteschen Funktionenkörper $F = K(x, y)$ vom Exponenten $q + 1$ gelten:

(a) *Das Geschlecht von F:K beträgt $g = \frac{q(q-1)}{2}$.*

(b) *Der Modul der ganzen Differentiale wird erzeugt von den Differentialen der Form $x^r y^{s-q} dx$ mit $0 \leq r, s, r + s \leq q - 2$, d.h. es ist*

$$\Delta_{F:K}(1) = K \left\langle \, x^r y^{s-q} dx : 0 \leq r, s, r + s \leq q - 2 \, \right\rangle .$$

(c) *Die Anzahl der rationalen Stellen in F:K beträgt*

$$\#\mathbb{P}_{F:K}^{(1)} = q^3 + 1.$$

Insbesondere ist F:K maximal (bzgl. der Hasse-Weil-Schranke).

(d) *Die Automorphismengruppe* $\mathrm{Aut}(F{:}K)$ *enthält eine zu* $\mathbf{PGU}_3(K)$ *isomorphe Untergruppe der Mächtigkeit $q^3(q^3 + 1)(q^2 - 1)$.*

Beweis. (a) Die erzeugende Relation des Hermiteschen Funktionenkörpers läßt sich schreiben als

$$y^{q+1} = 1 - x^{q+1} = \prod_{i=0}^{q} (w^i - x)$$

mit einer primitiven $(q+1)$-ten Einheitswurzel $w \in K$. Also ist F eine Kummererweiterung von $K(x)$. Aus der Theorie der Kummererweiterungen folgt, daß lediglich die Nullstellen von $x^{q+1}+1$ verzweigt sind (vgl. Anhang). Die (einzige) Nullstelle $\mathfrak{P}_i$ von $x - w^i$ ist total und zahm verzweigt und besitzt nach dem *Dedekindschen Differentensatz* den Differentenexponenten q. Die Differente von $F{:}K(x)$ setzt sich also zusammen zu

$$\mathfrak{D}(F{:}K(x)) = \prod_{i=0}^{q} \mathfrak{P}_i^q.$$

Für das Geschlecht von $F{:}K$ gilt gemäß der *Hurwitzschen Relativgeschlechtformel*

$$g_{F:K(x)} = 1 - [F{:}K(x)] + \frac{\deg(\mathfrak{D}(F{:}K(x)))}{2} = -q + \frac{q(q+1)}{2} = \frac{q(q-1)}{2}.$$

(b) Nach der *Differentialdivisorformel* hat der kanonische Divisor von $y^{-q}dx$ die Gestalt

$$(y^{-q}dx) = (y)^{-q}\mathfrak{D}(F{:}K(x))(x)_\infty^{-2} = (\mathfrak{P}_0 \cdots \mathfrak{P}_q)^{-q}(x)_\infty^q \mathfrak{D}(F{:}K(x))(x)_\infty^{-2} = (x)_\infty^{q-2}.$$

Folglich sind alle Differentiale $x^r y^{s-q}dx$ mit $r, s \geq 0$ und $r + s \leq q-2$ ganz und linear unabhängig. Da die Anzahl der Paare $(r,s) \in \mathbb{N} \times \mathbb{N}$ mit $r+s \leq q-2$, nämlich $\frac{q(q-1)}{2}$, mit der Dimension $g_{F:K}$ des Vektorraums der ganzen Differentiale $\Delta(1)$ übereinstimmt, folgt hieraus die Behauptung.

(c) Eine rationale Stelle $\mathfrak{P}$ in F ist eine Erweiterung einer rationalen Stelle $\mathfrak{Q}$ in $K(x)$, d.h. es ist $\mathfrak{P}$ eine Pol- oder Nullstelle von $x - a$ für eine Konstante $a \in K$. Die rationalen Stellen von F treten also als Primteiler von $x^{q^2} - x$ auf, die wir im folgenden untersuchen werden.

1.Fall: $\mathfrak{P}$ ist eine Nullstelle von $x - w$ mit einer $(q+1)$-ten Einheitswurzel $w \in K$. Dann ist $\mathfrak{P}$ nach dem Beweis von Aussage (a) die einzige Nullstelle von $x - w$ und total verzweigt in $F{:}K(x)$. Insgesamt liefern die Nullstellen von $x^{q+1}+1$ also genau $q+1$ rationale Stellen in F.

2.Fall: $\mathfrak{P}$ ist eine Nullstelle von $x - a$ mit $a^{q+1} \neq 1$. Es bezeichne $\mathfrak{Q} = \mathfrak{P} \cap K(x)$ die Reduktion von $\mathfrak{P}$ auf $K(x)$. Das Minimalpolynom $g(T) = T^{q+1} + x^{q+1} - 1$ von y über $K(x)$ hat Koeffizienten im Bewertungsring von $\mathfrak{Q}$. Daher läßt sich anhand der Zerlegung von $g(T)$ modulo $\mathfrak{Q}$ mit dem *Dedekind-Kriterium* das Zerlegungsverhalten von $\mathfrak{Q}$ in $F{:}K(x)$ ablesen. Es gilt in diesem Fall

$$g(T) \equiv T^{q+1} + a^{q+1} - 1 \equiv \prod_{i=0}^{q} (T - w^i b) \pmod{\mathfrak{Q}}$$

mit einer $(q+1)$-ten Einheitswurzel $w \in K$ und $b^{q+1} = a^{q+1} - 1$. (Die Elemente b und w sind Urbilder von $a^{q+1} - 1$ und 1 der surjektiven Normabbildung von $K{:}\mathbb{F}_q$.) Da die Linearfaktoren von $g(T) \pmod{\mathfrak{Q}}$ paarweise verschieden sind, hat dies die volle Zerlegung von $\mathfrak{Q}$ in $F{:}K(x)$ zur Folge und es ist $\mathfrak{P}$ eine von insgesamt $q+1$

Nullstellen von $x-a$. Die Nullstellen von $(x^{q^2}-x)/(x^{q+1}-1)$ liefern also genau $(q^2-(q+1))\cdot(q+1) = q^3-2q-1$ weitere rationale Stellen in F.
3.Fall: $\mathfrak{P}$ ist eine Polstelle von x. Wir setzen $\mathfrak{Q} = \mathfrak{P}\cap K(x)$ und $z := \frac{y}{x}$. Dann wird F auch von x und z erzeugt und das Minimalpolynom $h(T) = T^{q+1}+1-\frac{1}{x^{q+1}}$ von z über $K(x)$ liefert eine Gleichung von z über dem Bewertungsring von $\mathfrak{Q}$. Modulo $\mathfrak{Q}$ zerfällt $h(T) \equiv T^{q+1}-1 \pmod{\mathfrak{Q}}$ komplett in paarweise verschiedene Linearfaktoren. Somit hat $\mathfrak{Q}$ wie im zweiten Fall nach dem *Dedekind-Kriterium* ebenfalls $q+1$ rationale Fortsetzungen in F. Zusammen mit den ersten beiden Fällen zählen wir also insgesamt q^3+1 rationale Stellen in F. Im Vergleich mit der *Hasse-Weil-Schranke* ergibt sich

$$\#\mathbb{P}^{(1)}_{F:K} = q^3+1 = 2\sqrt{q^2}g_{F:K}+q^2+1,$$

d.h. die *Hasse-Weil-Schranke* wird von Hermiteschen Funktionenkörpern erreicht.

(d) Der Fermatkörper F ist isomorph zum rationalen Funktionenkörper $K(\mathfrak{X})$ der projektiven Kurve

$$\mathfrak{X} = \{(x_0:x_1:x_2) : x_0^{q+1}+x_1^{q+1}+x_2^{q+1}=0\} \subset \mathbb{P}^{(2)}(K)$$

vermöge $x \mapsto b\frac{x_1}{x_0}$ und $y \mapsto b\frac{x_2}{x_0}$, wobei b eine primitive $2(q+1)$-te Einheitswurzel in K (respektive eine primitve $(q+1)$-te Einheitswurzel im Fall $\mathrm{char}(K)=2$) bezeichnet. Wir zeigen, daß

$$\varphi : \left\{ \begin{array}{ccc} \mathbf{U}_3(K) & \longrightarrow & \mathrm{Aut}(K(\mathfrak{X}){:}K) \\ A=(a_{ij})_{0\le i,j\le 2} & \longmapsto & \varphi_A : x_i \mapsto \sum_{j=0}^2 a_{ij}x_j \end{array} \right.$$

eine Operation der unitären Matrizen $A\in\mathbf{U}_3(K)$ auf $K(\mathfrak{X})$ definiert. Es ist

$$\sum_{i=0}^2 \varphi(x_i)^{q+1} = \sum_{i=0}^2 \left(\sum_{j=0}^2 a_{ij}x_j\right)\left(\sum_{i=0}^2 a_{ik}x_k\right)^q = \sum_{0\le i,j,k\le 2} a_{ij}a_{ik}^q x_j x_k^q.$$

Eine unitäre Matrix $A\in\mathbf{U}_3(K)$ erfüllt $A^TA^q = \mathrm{id}$ (vgl. [Hup67, II.10.]). Somit gelten $a_{ij}a_{ik}^q = \delta_{jk}$ für $i=0,1,2$, wobei δ_{ik} das Kroeneckersymbol bezeichne. Es folgt dann

$$\sum_{i=0}^2 \varphi(x_i)^{q+1} = \sum_{0\le j,k\le 2}\left(\sum_{i=0}^2 a_{ij}a_{ik}^q\right)x_jx_k^q = \sum_{i=0}^2 x_i^{q+1}.$$

Also läßt die durch φ definierte Operation das projektive Modell von F invariant. Dies induziert die Operation

$$\overline{\varphi} : \left\{ \begin{array}{ccc} \mathbf{U}_3(K) & \longrightarrow & \mathrm{Aut}(F{:}K) \\ A & \longmapsto & \overline{\varphi}_A : x \mapsto b\frac{\varphi(x_1)}{\varphi(x_0)}, y \mapsto b\frac{\varphi(x_2)}{\varphi(x_0)} \end{array} \right.$$

von $\mathbf{U}_3(K)$ auf $F{:}K$. Der Kern des Homomorphismus $\overline{\varphi}$ wird erzeugt von den Matrizen der Gestalt $a\cdot(\delta_{ij})$, d.h. von den Vielfachen der Einheitsmatrix. Das zeigt schließlich $\mathrm{Aut}(F{:}K) \ge \mathbf{U}_3(K)/\mathrm{Z}(\mathbf{U}_3(K)) = \mathbf{PGU}_3(K)$. □

Anmerkung 17.3. Die Automorphismengruppe eines Hermiteschen Funktionenkörpers operiert 2-transitiv auf der Menge $\mathbb{P}^{(1)}_{F:K}$ seiner rationalen Stellen.

17.2 Hermitesche Codes und Dualisierung

Zum Studium Hermitescher Codes ist die Artin-Schreier-Normalform Hermitescher Funktionenkörper besonders zweckmäßig.

Bemerkung 17.4. (Artin-Schreier-Normalform)
Es sei F:K ein Hermitescher Funktionenkörper vom Exponenten $q+1$. Dann gibt es zwei Variablen $u, v \in F$ mit

$$F = K(u,v) \qquad \textit{und} \qquad v^q + v = u^{q+1}.$$

Dabei gelten:

(a) *Die Polstellendivisoren der Funktionen u und v sind Potenzen einer rationalen Stelle $\mathfrak{P}_\infty$, genauer gelten*

$$(u)_\infty = \mathfrak{P}_\infty^q \qquad \textit{sowie} \qquad (v)_\infty = \mathfrak{P}_\infty^{q+1}.$$

(b) *Die Differente $\mathfrak{D}(F{:}K(u))$ hat die Gestalt $\mathfrak{P}_\infty^{q^2+q-2}$.*

(c) *Das Differential du hat den Divisor $(du) = \mathfrak{P}_\infty^{q^2-q-2}$.*

Beweis. Es gibt Konstanten $a, b \in K = \mathbb{F}_{q^2}$ mit $a^q + a = -1 = b^{q+1}$. Die Funktionen u und v werden definiert durch

$$u := \frac{b}{y - bx} \qquad \text{und} \qquad v := a - ux.$$

Dann gilt $y = bu^{-1}(1+ux)$ und die Relation $1 = x^{q+1}+y^{q+1}$ wird nach Multiplikation mit u^{q+1} zu

$$\begin{aligned} u^{q+1} &= (ux)^{q+1} + (uy)^{q+1} = (a-v)^{q+1} + b^{q+1}(1+ux)^{q+1} \\ &= (a-v)^{q+1} - (a-v+1)^{q+1} = -(a-v) - (a^q - v^q + 1) = v^q + v. \end{aligned}$$

(a) Jede Polstelle von u ist auch eine Polstelle von v. Dies ergibt sich aus der definierenden Relation. Für eine Polstelle $\mathfrak{P}$ von u gilt nach der strikten Dreiecksungleichung wegen $\operatorname{ord}_\mathfrak{P}(u), \operatorname{ord}_\mathfrak{P}(v) < 0$

$$-(q+1) \cdot e_\mathfrak{P}(F{:}K(u)) = (q+1)\operatorname{ord}_\mathfrak{P}(u) = \operatorname{ord}_\mathfrak{P}(u^{q+1}) = \operatorname{ord}_\mathfrak{P}(v^q + v) = q \cdot \operatorname{ord}_\mathfrak{P}(v)$$

und somit $q = e_\mathfrak{P}(F{:}K(u)) = -\operatorname{ord}_\mathfrak{P}(u)$ sowie $\operatorname{ord}_\mathfrak{P}(v) = -(q+1)$. Insbesondere besitzen u und v nur eine Polstelle, die wir mit $\mathfrak{P}_\infty$ kennzeichnen.
(b) Die Verzweigungsstellen in $F{:}K(u)$ sind entweder Pol- oder Nullstellen von u. Nach Teil (a) ist die Polstelle von u total verzweigt. Der Nullstellendivisor von u ist hingegen nach dem *Dedekind-Kriterium* vollständig zerlegt. Die Differente $\mathfrak{D}(F{:}K(u))$ besitzt ledglich den Primteiler $\mathfrak{P}_\infty$. Seinen Differentenexponenten $d_{\mathfrak{P}_\infty}(F{:}K(u))$ erhält man aus der *Hurwitzschen Relativgeschlechtformel* vermöge

$$d_{\mathfrak{P}_\infty}(F{:}K(u)) = \deg(\mathfrak{D}(F{:}K(u))) = 2(g-1) + 2[F{:}K(u)] = q^2 + q - 2.$$

(c) Diese Aussage ergibt sich aus der *Differentialdivisorformel* vermöge

$$(du) = (u)_\infty^{-2} \cdot \mathfrak{D}(F{:}K(u)) = \mathfrak{P}_\infty^{q^2-q-2}. \qquad \square$$

Definition 17.5. (Hermitesche Codes und Standardcodes)
Ein arithmetischer Code über einen Hermiteschen Funktionenkörper $F{:}K$ heißt **Hermitescher Code**. Wählt man speziell $\mathfrak{G} = \mathfrak{P}_\infty^r$ mit der Polstelle $\mathfrak{P}_\infty$ von u aus Bemerkung 17.4 und $\mathfrak{A}$ als Produkt aller aller rationalen Stellen in $F{:}K$ außer $\mathfrak{P}_\infty$, so heißen die Codes

$$C_r := C(\mathfrak{A}, \mathfrak{P}_\infty^r)$$

für $r \in \mathbb{Z}$ **Hermitesche Standardcodes**.

Notiz 17.6. (a) Die Hermiteschen Standardcodes haben nach Satz 17.2 Länge q^3. (b) Für negative r gilt $C_r = 0$. Nach Korrolar 11.4 ist bei $r \geq q^3 + 2g - 1 = q^3 + q^2 - q - 1$ der Code C_r der volle Vektorraum $K^{\,q^3}$. Also können wir uns im folgenden auf natürliche Zahlen r mit $0 \leq r \leq q^3 + q^2 - q - 2$ beschränken.

Bemerkung 17.7. *Die Symmetriegruppe eines Hermiteschen Standardcodes umfaßt die Fixgruppe von $\mathfrak{P}_\infty$ in $\mathrm{Aut}(F{:}K)$ mit Kardinalität $\#\mathrm{Stab}(\mathfrak{P}_\infty) \geq q^3(q^2-1)$.*

Beweis. Die Länge eines Hermiteschen Standardcode ist größer als $2g + 2$. Somit ist die Automorphismengruppe $\mathrm{Aut}(\mathfrak{A}, \mathfrak{P}_\infty^{\mathfrak{r}}) = \mathrm{Stab}(\mathfrak{P}_\infty)$ nach Satz 12.13 in die Symmetriegruppe des Codes eingebettet. Aufgrund der Transitivität von $\mathrm{Aut}(F{:}K)$ auf $\mathbb{P}_{F:K}^{(1)}$ folgt $\#\mathrm{Stab}(\mathfrak{P}_\infty) = \#\,\mathrm{Aut}(F{:}K)/(q^3+1) \geq q^3(q^2-1)$. □

Satz 17.8. *Die Klasse der Hermiteschen Standardcodes über einen Hermiteschen Funktionenkörper $F{:}K$ ist abgeschlossen bezüglich Dualisierung. Genauer gilt für den Code C_r*

$$C_r^\perp = C_{q^3+q^2-q-2-r}.$$

Beweis. Die q^3 rationalen Stellen $\mathfrak{P} \in \mathbb{P}_{F:K}^{(1)} \backslash \{\mathfrak{P}_\infty\}$ werden parametrisiert durch die Paare $(a,b) \in \mathbb{F}_{q^2}^2$ mit $a^{q+1} = b^q + b$. Dabei gibt es für alle $a \in \mathbb{F}_q$ jeweils genau q verschiedene $b \in \mathbb{F}_{q^2}$ mit $a^{q+1} = b^q + b$. Bezeichnet man die entsprechenden Primdivisoren, d.h. die Kerne der Stellen $u \mapsto a, v \mapsto b$ mit $\mathfrak{P}_{a,b}$, so gelten

$$\mathfrak{A} = \prod_{\substack{a,b \in K \\ a^{q+1} = b^q + b}} \mathfrak{P}_{a,b} \qquad \text{sowie} \qquad (u-a) = \left(\prod_{a^{q+1} = b^q + b} \mathfrak{P}_{a,b} \right) \cdot \mathfrak{P}_\infty^{-q}.$$

Die Funktion $z := u^{q^2} - u = \prod_{a \in K} (u-a)$ hat den Divisor

$$(z) = (u^{q^2} - u) = \prod_{a \in K} (u-a) = \mathfrak{A}\mathfrak{P}_\infty^{-q^3}$$

und ist damit Primelement für alle $\mathfrak{P}_{a,b}$. Das Differential $\delta = z^{-1}du$ besitzt den kanonischen Divisor

$$(\delta) = (z^{-1})(du) = \mathfrak{P}_\infty^{q^3}\mathfrak{A}^{-1}\,\mathfrak{P}_\infty^{q^2-q-2} = \mathfrak{A}^{-1}\mathfrak{P}_\infty^{q^3+q^2-q-2}$$

und hat somit an allen Stellen $\mathfrak{P}_{a,b}$ Ordnung -1 und Residuum 1. Nach Satz 11.14 ist dann C_r dual zum Code $C(\mathfrak{A}, \mathfrak{G}^*)$ mit Goppadivisor

$$\mathfrak{G}^* = (\delta)\mathfrak{A}\mathfrak{P}_\infty^{-r} = \mathfrak{P}_\infty^{q^3+q^2-q-2-r}.$$

□

Korollar 17.9. (Kriterien für Selbstdualität und -orthogonalität)

(a) *Im Falle* $r \leq \frac{1}{2}(q^3+q^2-q-2)$ *ist* C_r *selbstorthogonal, d.h. es gilt*

$$C_r \leq C_r^*.$$

(b) C_r *ist genau dann selbstdual, wenn* $r = \frac{1}{2}(q^3+q^2-q-2)$ *gilt. Insbesondere gibt es nur in Charakteristik* 2 *selbstduale Hermitesche Standardcodes.* □

17.3 Dimension und Distanz Hermitescher Codes

Bemerkung 17.10. (Pol- und Fehlzahlen vom $\mathfrak{P}_\infty$)
Es sei $F = K(u,v)$ *mit* $v^q + v = u^{q+1}$ *ein Hermitescher Funktionenkörper und* $\mathfrak{P}_\infty$ *die Polstelle von* u *in* F. *Dann gelten:*

(a) $\mathfrak{P}_\infty$ *hat die Polzahlhalbgruppe* $\mathbb{H} := \mathbb{N}q + \mathbb{N}(q+1)$ *und ist für* $q > 3$ *ein Weierstraßpunkt.*

(b) *Der lineare Raum* $\mathcal{L}(\mathfrak{P}_\infty^r)$ *hat die Basis*

$$\{u^i v^j : i,j \in \mathbb{N}, j \leq q-1, iq + j(q+1) \leq r\}.$$

Beweis. Nach Bemerkung 17.4 sind q und $q+1$ Polzahlen von $\mathfrak{P}_\infty$, d.h. $\mathbb{H}$ ist enthalten in der Polzahlhalbgruppe von $\mathfrak{P}_\infty$. Die Menge $\mathbb{N}\backslash\mathbb{H}$ enthält genau $(q-1) + (q-2) + \ldots + 1 = \frac{q(q-1)}{2} = g$ Elemente. Da jede rationale Stelle genau g Fehlzahlen besitzt, ist $\mathbb{N}\backslash\mathbb{H}$ die Menge aller Fehlzahlen und $\mathbb{H}$ die volle Menge der Polzahlen von $\mathfrak{P}_\infty$. Die Aussage (b) folgt aus Bemerkung 17.4 und Teil (a). □

Aufgabe 17.11. Beweisen Sie, daß $\mathfrak{P}_\infty$ für $q > 3$ ein Weierstraßpunkt ist. Zeigen Sie weiter, daß $\mathbb{P}_{F:K}^{(1)}$ die Menge aller Weierstraßpunkte von $F{:}\overline{\mathbb{F}}_q$ ist, wobei $\overline{\mathbb{F}}_q$ den algebraischen Abschluß von $\mathbb{F}_q$ bezeichne.
Hinweis: Berechnen Sie hierzu den zusammengesetzten Verzweigungsdivisor von F: K bzgl. iterativer Differentation.

Satz 17.12. (Hermitescher Standardcodes mit normalen Goppadivisor)
Es sei C_r *ein Hermitescher Standardcode mit* $0 \leq r < q^3$, *d.h. mit normalem Goppadivisor. Dann gelten:*

(a) C_r *besitzt die Dimension*

$$\dim(C_r) = \dim(\mathfrak{P}_\infty^r) = \#\{(i,j) : i,j \in \mathbb{N}, j \leq q-1, iq + j(q+1) \leq r\}.$$

(b) *Die Minimaldistanz* $d(C_r)$ *des Codes* C_r *ist*

$$d(C_r) = \begin{cases} q^3 - r & \text{falls } r, q^3 - r \in \mathbb{H} \\ d(C_{r-1}) & \text{sonst.} \end{cases}$$

Beweis. (a) Die Behauptung folgt unmittelbar aus Korollar 11.4 und Bemerkung 17.10, da der Goppadivisor kleineren Grad als die Länge des Codes besitzt.
(b) Ist r eine Fehlzahl von $\mathfrak{P}_\infty$, so gilt $\dim(C_r) = \dim(\mathfrak{P}_\infty^r) = \dim(\mathfrak{P}_\infty^{r-1}) = \dim(C_{r-1})$. Wegen $C_{r-1} \leq C_r$ folgen hieraus $C_r = C_{r-1}$ und $d(C_r) = d(C_{r-1})$.
Im folgenden sei r eine Polzahl und es gelte $r = kq + l(q+1)$. Dabei kann man o.E. $l \leq q-1$ wählen (vergleiche auch Bemerkung 17.10). Nach Satz 11.2 gilt $d(C_r) \geq q^3 - r$, also ist lediglich $d(C_r) \leq q^3 - r$ bzw. die Existenz eines Codeswortes vom Gewicht $q^3 - r$ zu zeigen.
1.Fall: Es ist $r = q^3 - q^2 = (q^2 - q)q$. Wir wählen $q^2 - q$ paarweise verschiedene Konstanten $a_1, \ldots, a_{q^2-q} \in K$. Die Funktion $z := \prod_{i=1}^{q^2-q}(u - a_i)$ hat den Divisor

$$(z) = \mathfrak{P}_\infty^{-q(q^2-q)} \prod_{i=1}^{q^2-q} (u - a_i)_0 = \mathfrak{P}_\infty^{-r} \prod_{i=1}^{q^2-q} \prod_{b^q+b=a_i^{q+1}} \mathfrak{P}_{a_i,b}.$$

Also ist $\boldsymbol{z} = (z(\mathfrak{P}_{a,b}))_{b^q+b=a^{q+1}}$ ein Codewort von C_r vom Gewicht $q^3 - r$.
2.Fall: Es gilt $r < q^3 - q^2$ und damit $k \leq q^2 - q - 1$. Wir wählen eine nichtverschwindende Konstante $c \in \mathbb{F}_q^\times$. Nach dem Beweis zu Satz 17.8 hat die Menge $A := \{a \in K : a^{q+1} \neq c\}$ Kardinalität $q^2 - (q+1)$. A enthält also mindestens k paarweise verschiedene Konstanten $a_1, \ldots, a_k$. Die Funktion $z_1 := \prod_{i=1}^{k}(u - a_i)$ hat somit genau kq Nullstellen. Desweiteren gibt es mindestens l verschiedenen Konstanten $b_1, \ldots, b_l$ mit $b_j^q + b_j = c$, da die Spurabbildung der Erweiterung $K{:}\mathbb{F}_q$ surjektiv ist. Also hat $z_2 := \prod_{j=1}^{l}(v - b_j)$ genau $l(q+1)$ Nullstellen der Form $\mathfrak{P}_{a,b_j}$. Wegen

$$c = b_j^q + b_j = a^{q+1} = (u(\mathfrak{P}_{a,b_j}))^{q+1}$$

sind diese Stellen verschieden von den Nullstellen von z_1. Die Funktion $z_1 z_2$ hat also $kq + l(q+1) = r$ Nullstellen und besitzt den Polstellendivisor $(z_1 z_2)_\infty = \mathfrak{P}_\infty^r$. Somit ist $(\boldsymbol{z_1 z_2})$ ein Codewort mit Gewicht $q^3 - r$.
3.Fall: Es ist $r > q^3 - q^2$. Im Gegensatz zu den obigen Fällen ist hier $q^3 - r$ in der Regel keine Polzahl mehr. Nun bezeichne s die kleinste Polzahl mit $s \geq q^3 - r$. Für diese gilt nach Bemerkung 17.10 (b) jedenfalls $s \leq q^2 \leq q^3 - q^2$. Gemäß der Fälle 1 und 2 gibt es daher eine Funktion z aus $\mathcal{L}(\mathfrak{P}_\infty^s)$ mit $(z) = \mathfrak{B}\mathfrak{P}_\infty^{-s}$ und $\mathfrak{B}|\mathfrak{A}$. Damit ergibt sich

$$\mathfrak{P}_\infty^r \sim \mathfrak{P}_\infty^r (u^{q^2} - u)(z^{-1}) = \mathfrak{P}_\infty^{r+s-q^3} \mathfrak{B}^{-1}\mathfrak{A}.$$

Es sei zunächst $s = q^3 - r$. Dann ist der Goppadivisor von C_r äquivalent zu einem Teiler des Auswertungsdivisor $\mathfrak{A}$ und es gilt nach Zusatz 11.3 $d(C_r) = q^3 - r$.
Ist hingegen $s > q^3 - r$ und damit $c_r := r + s - q^3 > 0$, so ist $\mathfrak{P}_\infty^r$ äquivalent zu einen Divisor der Gestalt $\mathfrak{P}_\infty^{c_r}\mathfrak{B}$, wobei $\mathfrak{B}$ ein ganzer Teiler von $\mathfrak{A}$ ist. Nach Zusatz 11.3 folgt dann

$$d(C_r) = q^3 - r + c_r.$$

Ersetzen wir hierin r durch $r-1$, so wird $c_{r-1} = c_r - 1$, und es folgt

$$d(C_r) = q^3 - r + c_r = q^3 - (r-1) + c_{r-1} = d(C_{r-1}).$$ □

Korollar 17.13. *Im Falle $q^2 - q \leq r \leq q^3 - q^2 + q$ gelten für die Dimension und die Minimaldistanz des Hermiteschen Standardcodes C_r*

$$\dim(C_r) = r - g + 1 = r + 1 - \frac{q(q-1)}{2} \qquad \textit{und} \qquad d(C_r) = q^3 - r.$$

Beweis. Jede Fehlzahl ist kleiner als $2g = q(q-1)$. Somit ist r eine Polzahl und die Aussagen folgen aus dem bisher gezeigten sowie dem Satz von *Riemann-Roch*. □

Zusatz 17.14. *Es sei C_r ein Hermitescher Standardcode mit $q^3 \leq r \leq q^3+q^2-q-2$, d.h. mit nicht-normalem Goppadivisor. Dann gelten:*

(a) $\dim(C_r) = q^3 - \dim(\mathfrak{P}_\infty^{q^3+q^2-q-2-r})$

(b) $d(C_r) = q - \left\lfloor \frac{r-q^3+q}{q+1} \right\rfloor$.

Aufgabe 17.15. Beweisen Sie Zusatz 17.14.

Aufgabe 17.16. Bestimmen Sie die Parameter der Teilkörpercodes $C_r|_{\mathbb{F}_q}$ und der Spurcodes $\mathrm{Tr}_{K:\mathbb{F}_q}(C_r)$.

Kapitel 18

Artin-Schreier-Türme

In den nächsten beiden Kapiteln werden Codes nachgewiesen, welche die *Gilbert-Varshamov-Schranke* übertreffen. In diesem Kapitel werden die dazu verwendeten Funktionenkörper studiert, die sich aus Türmen von Artin-Schreier-Erweiterungen konstruieren lassen.

18.1 Artin-Schreier-Erweiterungen

Definition 18.1. (Artin-Schreier-Erweiterung)
Eine Körpererweiterung E:F vom Grad q mit $F \geq \mathbb{F}_q$ heißt **Artin-Schreier-Erweiterung**, falls $E = F(y)$ Stammkörper eines y über F mit $y^q - y \in F$ ist.

Satz 18.2. (Hauptsatz der Artin-Schreier-Theorie)
Es seien F:K ein algebraischer Funktionenkörper mit Konstantenkörper K der Charakteristik $p > 0$ und

$$h(T) = T^q + a_1 T^{q/p} + a_2 T^{q/p^2} + \cdots + a_{r-1} T^p + a_r T$$

ein separables, additives Polynom, welches über K vollständig in Linearfaktoren zerfällt. Desweiteren sei $E = F(y)$ eine Erweiterung von F gegeben durch

$$h(y) = z \in F.$$

Für jeden Primdivisor $\mathfrak{P} \in \mathbb{P}_{F:K}$ mit $\operatorname{ord}_{\mathfrak{P}}(z - h(u)) \not\equiv 0 \pmod{p}$ für eine Funktion $u \in F$ definieren wir die Zahl $m_{\mathfrak{P}}$ via

$$m_{\mathfrak{P}} := \begin{cases} m & : \text{ es gibt ein } u \in F \text{ mit } \operatorname{ord}_{\mathfrak{P}}(z - h(u)) = -m < 0 \text{ und } m \not\equiv 0 \pmod{p} \\ -1 & : \text{ es gibt ein } u \in F \text{ mit } \operatorname{ord}_{\mathfrak{P}}(z - h(u)) \geq 0. \end{cases}$$

Dann ist $m_{\mathfrak{P}}$ für diese Stellen wohldefiniert. (Man beachte, daß Primdivisoren $\mathfrak{P}$ mit $\operatorname{ord}_{\mathfrak{P}}(z - h(u)) \equiv 0 \pmod{p}$ für alle $u \in F$ kein Wert $m_{\mathfrak{P}}$ zugewiesen wird.) Besitzt F:K mindestens eine Stelle $\mathfrak{Q}$ mit $m_{\mathfrak{Q}} > 0$, so ist E:F eine geometrische elementarabelsche Erweiterung vom Grad q und es gelten:

(a) *Die Primdivisoren* $\mathfrak{P} \in \mathbb{P}_{F:K}$ *mit* $m_{\mathfrak{P}} > 0$ *sind total verzweigt in* $E{:}F$ *mit Differentenexponenten* $d_{\mathfrak{P}}(E{:}F) = (q-1)(m_{\mathfrak{P}}+1)$.

(b) *Die Primdivisoren* $\mathfrak{P} \in \mathbb{P}_{F:K}$ *mit* $m_{\mathfrak{P}} = -1$ *sind unverzweigt in* $E{:}F$.

(c) *Ist der Index* $m_{\mathfrak{P}}$ *für alle Primdivisoren* $\mathfrak{P} \in \mathbb{P}_{F:K}$ *definiert, so ist jede in* $E{:}F$ *verzweigte Stelle total verzweigt und* $E{:}K$ *besitzt das Geschlecht*

$$g_{E:K} = 1 + q \cdot (g_{F:K} - 1) + \frac{q-1}{2} \sum_{\mathfrak{P} \in \mathbb{P}_{F:K}} (m_{\mathfrak{P}} + 1) \cdot \deg(\mathfrak{P}).$$

Beweis. Zunächst weisen wir die Wohldefiniertheit von $m_{\mathfrak{P}}$ nach. Dazu ist zu zeigen, daß die beiden aufgeführten Fälle nicht gleichzeitig eintreten können und $m_{\mathfrak{P}}$ im Fall $m_{\mathfrak{P}} > 0$ eindeutig bestimmt ist. Wir nehmen an, zur Primstelle $\mathfrak{P} \in \mathbb{P}_{F:K}$ gebe es zwei Funktionen $u_1, u_2 \in F$ mit $\operatorname{ord}_{\mathfrak{P}}(z - h(u_1)) = m_1$, $\operatorname{ord}_{\mathfrak{P}}(z - h(u_2)) = m_2 < 0$ sowie $m_1 \neq m_2 \not\equiv 0 \pmod{p}$. Dann folgt nach der ultrametrischen Dreiecksungleichung

$$\min\{m_1, m_2\} = \operatorname{ord}_{\mathfrak{P}}(z - h(u_1) - (z - h(u_2))) = \operatorname{ord}_{\mathfrak{P}}(h(u_2 - u_1)) = q \operatorname{ord}_{\mathfrak{P}}(u_2 - u_1).$$

Der Fall $m_1 > m_2$ führte zum Widerspruch zur Teilerfremdheit von m_2 und q. Es ist also nur der Fall $m_1 < m_2$ möglich und $m_{\mathfrak{P}}$ ist bei $m_{\mathfrak{P}} > 0$ eindeutig durch

$$-m_{\mathfrak{P}} = \max\{\operatorname{ord}_{\mathfrak{P}}(z - h(u)) : u \in F\}$$

gegeben. Das zeigt die Wohldefiniertheit der Indices $m_{\mathfrak{P}}$ für die fraglichen Stellen $\mathfrak{P}$ mit $\operatorname{ord}_{\mathfrak{P}}(z - h(u)) \not\equiv 0 \pmod{p}$ für ein $u \in F$. Wir nehmen nun an, es gäbe eine Primstelle $\mathfrak{Q} \in \mathbb{P}_{F:K}$ mit Index $m_{\mathfrak{Q}} > 0$. Dann gibt es eine Funktion $u \in F$ mit

$$\operatorname{ord}_{\mathfrak{Q}}(z - h(u)) = -m_{\mathfrak{Q}} \not\equiv 0 \pmod{p}.$$

Für den Verzweigungsindex $e_{\tilde{\mathfrak{Q}}}(E{:}F)$ einer Fortsetzung $\tilde{\mathfrak{Q}}$ von $\mathfrak{Q}$ in E ergibt sich

$$-m_{\mathfrak{Q}} \cdot e_{\tilde{\mathfrak{Q}}}(E{:}F) = \operatorname{ord}_{\tilde{\mathfrak{Q}}}(z - h(u)) = \operatorname{ord}_{\tilde{\mathfrak{Q}}}(h(y) - h(u)) = q \cdot \operatorname{ord}_{\tilde{\mathfrak{Q}}}(y - u).$$

Aus der Teilerfremdheit zwischen m und q folgen hieraus

$$\operatorname{ord}_{\tilde{\mathfrak{Q}}}(y - u) = -m_{\mathfrak{Q}} \qquad \text{sowie} \qquad q \geq [E{:}F] \geq e_{\tilde{\mathfrak{Q}}}(E{:}F) \geq q.$$

Insbesondere ist $\mathfrak{Q}$ total verzweigt in $E{:}F$ und $h(T) - z \in F[T]$ irreduzibel über F. Die Nullstellenmenge $A := \{a \in \overline{K} : h(a) = 0\}$ von $h(T)$ bildet eine additive Gruppe mit Exponent p. Nach Voraussetzung ist A in K enthalten und es gilt $\#A = q$. Also ist E als Zerfällungskörper des separablen Polynoms $h(T) - z$ eine galoissche Erweiterung von F. Die Galoisoperation ist durch $\sigma(y) = y + a$ mit $a \in A$ gegeben und wir erhalten die Gruppenisomorphie

$$G := \operatorname{Gal}(E{:}F) \cong A \cong \mathbf{Z}_p \times \cdots \times \mathbf{Z}_p.$$

Somit ist E:F eine elementarabelsche Erweiterung vom Grad q. Es sei L der algebraische Abschluß von K in E und $LF \leq E$ die maximale Konstantenerweiterung von F in E. Da Konstantenerweiterungen unverzweigt sind (siehe Anhang), folgt

$$q = e_{\mathfrak{Q}}(E{:}F) = e_{\mathfrak{Q}}(E{:}LF) \cdot e_{\mathfrak{Q}}(LF{:}F) = e_{\mathfrak{Q}}(E{:}LF)$$

und somit $[L{:}K] = [LF{:}F] = 1$. Also ist $L = K$ der vollständige Konstantenkörper von E und E:F bildet eine geometrische Erweiterung.

(a) Wir haben bereits gezeigt, daß jede Primstelle $\mathfrak{P} \in \mathbb{P}_{F:K}$ mit $m_{\mathfrak{P}} > 0$ total verzweigt in E:F. Es bleibt somit nur noch der Differentenexponent $d_{\tilde{\mathfrak{P}}}(E{:}F) = d_{\mathfrak{P}}(E{:}F)$ der einzigen Fortsetzung $\tilde{\mathfrak{P}} \in \mathbb{P}_{E:K}$ von $\mathfrak{P}$ in E zu bestimmen. Für eine Funktion $u \in F$ mit $\mathrm{ord}_{\mathfrak{P}}(z - h(u)) = -m_{\mathfrak{P}}$ setzen wir $\tilde{y} := y - u$. Auf Grund der Teilerfremdheit von $m_{\mathfrak{P}}$ und q gilt wie oben $\mathrm{ord}_{\tilde{\mathfrak{P}}}(\tilde{y}) = -m_{\mathfrak{P}}$ und es gibt natürliche Zahlen $i, j > 0$ mit

$$i \cdot q - j \cdot m_{\mathfrak{P}} = 1.$$

Für ein Primelement $x \in F$ zu $\mathfrak{P}$ ist dann $t := x^i \tilde{y}^j \in E$ ein Primelement zu $\tilde{\mathfrak{P}}$. Die Galoisoperation von G auf t ist durch $\sigma(t) = x^i(\tilde{y} + a)^j$ mit $a \in A$ gegeben und es gilt

$$\sigma(t) - t = x^i \cdot \left(\sum_{l=0}^{j} \binom{l}{j} \tilde{y}^{j-l} a^l - \tilde{y}^j \right) = x^i \cdot \sum_{l=1}^{j} \binom{l}{j} \tilde{y}^{j-l} a^l$$

für $\sigma \neq \mathrm{id}$. Wegen $\mathrm{ord}_{\tilde{\mathfrak{P}}}(a) = 0$ und $\mathrm{ord}_{\tilde{\mathfrak{P}}}(\tilde{y}^{j-1}) < \mathrm{ord}_{\tilde{\mathfrak{P}}}(\tilde{y}^{j-l})$ für $l > 1$ hat die Differenz $\sigma(t) - t$ die Ordnung

$$\mathrm{ord}_{\tilde{\mathfrak{P}}}(\sigma(t) - t) = \mathrm{ord}_{\tilde{\mathfrak{P}}}(x^i) + \mathrm{ord}_{\tilde{\mathfrak{P}}}(ja\tilde{y}^{j-1}) = i \cdot q - (j-1) \cdot m_{\mathfrak{P}} = 1 + m_{\mathfrak{P}}$$

bei $\tilde{\mathfrak{P}}$. Also ist jeder Galoisautomorphismus $\sigma \neq \mathrm{id}$ in der $m_{\mathfrak{P}}$-ten Verzweigungsgruppe, nicht aber in den höheren Verzweigungsgruppen G_i von $\mathfrak{P}$ mit $i \geq m_{\mathfrak{P}} + 1$ enthalten. Mit der *Hilbertschen Differentenformel* folgt schließlich

$$d_{\mathfrak{P}}(E{:}F) = \sum_{i=0}^{\infty} (\#G_i - 1) = (m_{\mathfrak{P}} + 1)(\#G - 1) = (m_{\mathfrak{P}} + 1)(q - 1).$$

(b) Es sei nun $\mathfrak{P} \in \mathbb{P}_{F:K}$ eine Stelle mit $m_{\mathfrak{P}} = -1$ und $\tilde{\mathfrak{P}}$ eine Erweiterung von $\mathfrak{P}$ in E. Dann gibt es eine Funktion $u \in F$ mit $\tilde{z} := z - h(u) \in \mathcal{O}_{\mathfrak{P}}$. Das Element $\tilde{y} := y - u$ ist ebenfalls ein primitives Element von E:F und $g(T) := h(T) - \tilde{z} \in \mathcal{O}_{\mathfrak{P}}[T]$ das zugehörige Minimalpolynom von $\tilde{y}$ über F. Dann ist der Differentenexponent durch die Ordnung von $g'(\tilde{y})$ bei $\tilde{\mathfrak{P}}$ beschränkt [Sti93, Thm.III.5.10.]. Somit folgt die Aussage (b) aus $g'(\tilde{y}) = a_r \neq 0$.

(c) Mit den gemachten Voraussetzungen ist E:F eine geometrische Erweiterung vom Grad q und jede Primstelle $\mathfrak{P} \in \mathbb{P}_{F:K}$ liefert den Gradbeitrag $\deg(\mathfrak{P})(m_{\mathfrak{P}}+1)(q-1)$ zur Differente $\mathfrak{D}(E{:}F)$ von E:F. Es folgt mit der *Hurwitzschen Relativgeschlechtsformel*

$$g_{E:K} - (1 + q \cdot (g_{F:K} - 1)) = \frac{\deg(\mathfrak{D}(E{:}F))}{2} = \frac{q-1}{2} \sum_{\mathfrak{P} \in \mathbb{P}_{F:K}} (m_{\mathfrak{P}} + 1) \cdot \deg(\mathfrak{P}). \quad \square$$

Für Artin-Schreier-Erweiterungen $E{:}F$ algebraischer Funktionenkörper mit Konstantenkörper $K \geq \mathbb{F}_{q^2}$ kann die erzeugende Relation auch in der Normalform

$$y^q + y + z \in F$$

angegeben werden. (Bei ungerader Charakteristik ersetzt man dabei einfach das primitive Element y durch $-ay$ mit einer $2(q-1)$-ten Einheitswurzel $a \in \mathbb{F}_{q^2}$.) Für den Rest dieses Kapitels sei stets, sofern nicht anders angegeben, $K = \mathbb{F}_{q^2}$. Für eine Konstante $c \in \mathbb{F}_q$ bezeichnen wir die Spurfaser von c unter der Spurabbildung von K nach $\mathbb{F}_q$ mit

$$A_c = \{a \in K : a^q + a = c\}.$$

Für $c = 0$ setzen wir $A := A_0$ und

$$A^\times := A \backslash \{0\} = \{a \in K : a^{q-1} + 1 = 0\}.$$

Man beachte, daß A eine additive Untergruppe von K bildet und bei gerader Charakteristik mit $\mathbb{F}_q$ übereinstimmt.

Bemerkung 18.3. *Es sei $E{:}F$ eine Artin-Schreier-Erweiterung mit $K \geq \mathbb{F}_{q^2}$ erzeugt durch die Relation $y^q + y = z \in F$. Dann sind die Zählerstellen $\mathfrak{P}_c$ von $z - c$ für $c \in \mathbb{F}_q$ vollständig zerlegt in $E{:}F$ und die q Fortsetzungen $\mathfrak{P}_{a,c} | \mathfrak{P}_c$ sind eindeutig bestimmt durch $y - a \in \mathfrak{P}_{a,c}$ mit $a \in A_c$.*

Beweis. Das modulo $\mathfrak{P}_c$ reduzierte Minimalpolynom von y hat die Gestalt

$$\overline{g}(T) = T^q + T - c = \prod_{a \in A_c} (T - a)$$

und zerfällt somit über $\mathcal{O}_{\mathfrak{P}_c}/\mathfrak{P}_c \geq K$ vollständig in Linearfaktoren. Somit folgt unsere Behauptung aus dem *Dedekind-Kriterium.* $\square$

Bemerkung 18.4. (Geschlecht und Verzweigung der Norm-Spur-Gleichung)
Der algebraische Funktionenkörper $E = K(x, y)$ mit $K \geq \mathbb{F}_{q^2}$ sei erzeugt durch die Relation

$$y^q + y = \frac{x^q}{x^{q-1} + 1} \ . \tag{18.5}$$

Dann sind $F{:}K(x)$ und $F{:}K(y)$ Artin-Schreier-Erweiterungen vom Grad q und es gelten die folgende Aussagen:

(a) *Die Nenner- und Zählerdivisoren zu $x^{q-1} + 1$ sind total verzweigt in $E{:}K(x)$ und die Zählerdivisoren zu $y^q + y$ sind total verzweigt in $E{:}K(y)$. Diese Stellen sind die einzigen Verzweigungsstellen von $E{:}K(x)$ bzw. $E{:}K(y)$. Ihr Differentenexponent ist jeweils $2(q-1)$ und die Differenten von $E{:}K(x)$ und $E{:}K(y)$ haben die Gestalt*

$$\mathfrak{D}(E{:}K(x)) = (\mathfrak{P}_\infty \prod_{a\in A^\times} \mathfrak{P}_a)^{2(q-1)} \quad \textit{und} \quad \mathfrak{D}(E{:}K(y)) = (\prod_{b\in A} \mathfrak{Q}_b)^{2(q-1)}.$$

Dabei bezeichne $\mathfrak{P}_a$ den primen Zählerdivisor von $x-a$ für $a \in A^\times$, $\mathfrak{P}_\infty$ den primen Nennerdivisor von x sowie $\mathfrak{Q}_b$ den primen Zählerdivisor von $y-b$ für $b \in A$.

(b) *Das Geschlecht von $E{:}K$ beträgt $g_{E:K} = (q-1)^2$.*

(c) *Die Hauptdivisoren von $x-b$ und $y-b$ für $b \in A$ haben die Gestalt*

$$(x) = \mathfrak{P}_\infty^{-q} \prod_{b\in A} \mathfrak{Q}_b, \qquad (x-a) = \mathfrak{P}_\infty^{-q}\mathfrak{P}_a^q \qquad \textit{für} \quad a \in A^\times,$$
$$(y-b) = (\mathfrak{P}_\infty^{-1} \prod_{a\in A^\times} \mathfrak{P}_a^{-1})\mathfrak{Q}_b^q.$$

Beweis. Die Körpererweiterung $F{:}K(y)$ besitzt das primitive Element $\frac{1}{x}$ mit der definierenden Relation

$$\left(\frac{1}{x}\right)^q + \frac{1}{x} = \frac{1}{y^q+y},$$

die man aus (18.5) gewinnt. Somit sind $E{:}K(y)$ wie auch $E{:}K(x)$ Artin-Schreier-Erweiterungen vom Grad q. Die Gestalt der Differenten und das Geschlecht von $E{:}K$ erhält man unmittelbar aus Satz 18.2. Insbesondere sind die Stellen $\mathfrak{P}_\infty$ und $\mathfrak{P}_a$ für $a \in A^\times$ total verzweigt in $E{:}K(x)$ und es gelten $(x)_\infty = \mathfrak{P}_\infty^q$ sowie $(x-a)_0 = \mathfrak{P}_a^q$. Analog gilt $(y-b)_0 = \mathfrak{Q}_b^q$ für $b \in A$. Für den Hauptdivisor von y^q+y ergibt sich

$$\frac{\prod_{b\in A} \mathfrak{Q}_b^q}{(y)_\infty^q} = (y^q+y) = \left(\frac{x^q}{x^{q-1}+1}\right) = \frac{(x)_0^q (x)_\infty^{q-1}}{(x)_\infty^q \prod_{a\in A^\times}(x-a)_0} = \frac{(x)_0^q}{\mathfrak{P}_\infty^q \prod_{a\in A^\times} \mathfrak{P}_a^q}.$$

Hieraus folgen $(x)_0 = \prod_{b\in A} \mathfrak{Q}_b$ sowie $(y)_\infty = \mathfrak{P}_\infty \prod_{a\in A^\times} \mathfrak{P}_a$. □

18.2 Verzweigung im Norm-Spur-Turm

Definition 18.6. (Norm-Spur-Turm)
Der Kongruenzfunktionenkörper $T_m := K(x_0, x_1, \ldots, x_m)$ mit den definierenden Relationen

$$x_i^q + x_i = \frac{x_{i-1}^q}{x_{i-1}^{q-1}+1} \qquad \text{für } i = 1, \ldots, m$$

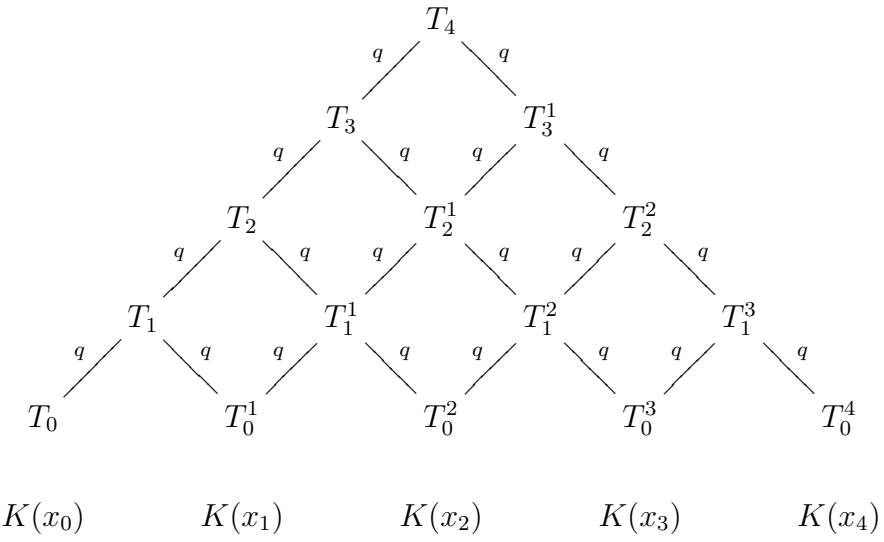
heißt **Norm-Spur-Turm**. Der Index m wird Höhe oder Stufe des Turms genannt. Die Namensgebung des Norm-Spur-Turms ist motiviert duch die Gleichungen

$$\mathrm{Norm}_{\mathbb{F}_{q^2}:\mathbb{F}_q}(a) = a^{q+1} \qquad \text{und} \qquad \mathrm{Spur}_{\mathbb{F}_{q^2}:\mathbb{F}_q}(a) = a^q + a.$$

Desweiteren setzen wir

$$T_k^i := K(x_i, \ldots, x_{i+k}).$$

Offensichtlich ist T_k^i isomorph zu T_k. Die Erweiterungen $T_k^i{:}T_{k-1}^{i-1}$ sind ebenfalls Artin-Schreier-Erweiterungen. Somit liefert der Norm-Spur-Turm eine Pyramide mit Artin-Schreier-Erweiterungen vom Grad q.



Bemerkung 18.7. *Für den Norm-Spur-Turm $T_m{:}K$ der Höhe m gelten:*

(a) *Die Erweiterungen $T_m{:}K(x_i)$ mit $i = 0, \ldots, m$ sind geometrisch vom Grad q^m.*

(b) *Alle Primdivisoren außerhalb der Trägerstellen von $x_0^q + x_0$ sind unverzweigt in der Norm-Spur-Pyramide, d.h. diese Stellen sind unverzweigt in $T_m{:}K(x_i)$ für $i = 0, \ldots, m$.*

(c) *Die Polstelle $\mathfrak{P}_\infty$ von x_0 sowie die Nullstellen $\mathfrak{P}_a$ von $x_0 - a$ für $a \in A^\times$ sind total verzweigt in $T_m{:}T_0$ mit dem Differentenexponenten $2(q^m - 1)$.*

Beweis. (b) Es sei $\mathfrak{P} \in \mathbb{P}_{T_m:K}$ weder Pol- noch Nullstelle von $x_0^q + x_0$. Dann besitzt $\mathfrak{P}$ Ordnung 0 bei $x_0^q/(x_0^{q-1} + 1)$ und ist somit weder Pol- noch Nullstelle von $x_1^q + x_1$. Induktiv folgt nun, daß $\mathfrak{P}$ weder Pol- noch Nullstelle von $x_i^q + x_i$ für $i = 0, \ldots, m$ ist. Daher besitzt $\mathfrak{P}$ in jeder Körpererweiterung $E{:}F$ der Norm-Spur-Pyramide den Index $m_\mathfrak{P} = -1$ und ist somit nach Satz 11.12 in der gesamten Norm-Spur-Pyramide unverzweigt.

(c) Es sei $\mathfrak{P} \in \{\mathfrak{P}_\infty, \mathfrak{P}_a : a \in A^\times\}$ entweder eine Pol- oder eine Nullstelle von $x_0^{q-1} + 1 = \prod_{a \in A^\times}(x_0 - a)$. Es ist $e_\mathfrak{P}(T_m{:}T_0) = q^m$ bzw. $e_\mathfrak{P}(T_k{:}T_{k-1}) = q$ für $k = 1, \ldots, m$ zu zeigen. Dazu zeigen wir via Induktion nach k, daß $\mathfrak{P}$ die Verzweigungsindices

$$e_\mathfrak{P}(T_k^i{:}T_{k-1}^i) = q \quad \text{und} \quad e_\mathfrak{P}(T_k^i{:}T_{k-1}^{i+1}) = 1 \quad \text{für } i = 0, \ldots, m-k$$

besitzt. Die Aussage für $k = 1$ erhalten wir komplett aus Bemerkung 12.10. Denn nach Bemerkung 12.10 ist $\mathfrak{P}$ total verzweigt in $K(x_1, x_0){:}K(x_0) = T_1^0{:}T_0^0$ sowie vollständig zerlegt in $T_1^0{:}T_0^1 = K(x_1, x_0){:}K(x_1)$ und bildet einen Pol zu x_1. Als solcher

ist $\mathfrak{P}$ wiederum nach Bemerkung 12.10 total verzweigt in $T_1^1{:}T_0^1$ und vollständig zerlegt in $T_1^1{:}T_0^2$. Mit einer seperaten Induktion folgt dann

$$e_{\mathfrak{P}}(T_1^i{:}T_0^i) = q \quad \text{und} \quad e_{\mathfrak{P}}(T_1^i{:}T_0^{i+1}) = 1 \quad \text{für } i = 0, \ldots, m-1.$$

Unsere Behauptung sei nun gültig für $k \geq 1$. Dann gilt für den Verzweigungsindex von $\mathfrak{P}$ in $T_{k+2}^i{:}T_k^{i+1}$

$$\begin{aligned} e_{\mathfrak{P}}(T_{k+2}^i{:}T_k^{i+1}) = e_{\mathfrak{P}}(T_{k+2}^i{:}T_{k+1}^i) \cdot e_{\mathfrak{P}}(T_{k+1}^i{:}T_k^{i+1}) &= e_{\mathfrak{P}}(T_{k+2}^i{:}T_{k+1}^i) \cdot 1 \\ = e_{\mathfrak{P}}(T_{k+2}^i{:}T_{k+1}^{i+1}) \cdot e_{\mathfrak{P}}(T_{k+1}^{i+1}{:}T_k^{i+1}) &= e_{\mathfrak{P}}(T_{k+2}^i{:}T_{k+1}^{i+1}) \cdot q, \end{aligned}$$

was $e_{\mathfrak{P}}(T_{k+2}^i{:}T_k^{i+1}) = q$ sowie $e_{\mathfrak{P}}(T_{k+2}^i{:}T_{k+1}^i) = q$ und $e_{\mathfrak{P}}(T_{k+2}^i{:}T_{k+1}^{i+1}) = 1$ zur Folge hat. Dies schließt den Induktionsbeweis und wir erhalten insbesondere

$$e_{\mathfrak{P}}(T_m{:}T_0) = q^m \qquad \text{und} \qquad e_{\mathfrak{P}}(T_i{:}K(x_i)) = \prod_{k=1}^{i} e_{\mathfrak{P}}(T_k^{i-k}{:}T_{k-1}^{i-k+1}) = 1 \quad \text{für } i = 0, \ldots, m.$$

Als eine in $T_i{:}K(x_i)$ unverzweigte Polstelle von $x_i^q/(x_i^{q-1}+1)$ erfüllt $\mathfrak{P}$

$$\operatorname{ord}_{\mathfrak{P}\cap T_i}\left(\tfrac{x_i^q}{x_i^{q-1}+1}\right) = -1 \quad \text{für } i = 0, \ldots, m-1.$$

Somit besitzt $\mathfrak{P}$ in $T_{i+1}{:}T_i$ nach Satz 11.12 den Index $m_{\mathfrak{P}\cap T_i} = 1$ und Differentenexponenten

$$d_{\mathfrak{P}}(T_{i+1}{:}T_i) = 2(q-1) \quad \text{für } i = 0, \ldots, m-1.$$

Mit der Formel für zusammengesetzte Differentenexponenten

$$d_{\mathfrak{P}}(E{:}H) = d_{\mathfrak{P}}(E{:}F) + e_{\mathfrak{P}}(E{:}F) d_{\mathfrak{P}}(F{:}H)$$

für Körpererweiterungen $E \geq F \geq H$ folgt schließlich

$$d_{\mathfrak{P}}(T_m{:}T_0) = \sum_{i=1}^{m} d_{\mathfrak{P}}(T_i{:}T_{i-1}) \cdot q^{m-i} = 2(q^m - 1).$$

(a) Sämtliche Erweiterungen in der Norm-Spur-Pyramide sind separabel. Da $T_m{:}T_0$ nach (b) total verzweigt ist, ist K der vollständige Konstantenkörper von T_m und somit von sämtlichen Unterkörpern in der Pyramide. □

Die möglichen Verzweigungstellen in $T_m{:}T_0$ sind die Pol- oder Nullstellen von $x_0^q + x_0$. Mit obiger Bemerkung haben wir bereits gezeigt, daß die Pol- und Nullstellen von $x_0^{q-1}+1$ total verzweigen. Um die Differente von $T_m{:}T_0$ zu bestimmen, bleibt somit das Fortsetzungsverhalten der Nullstellen zu x_0 zu untersuchen. Aus Bemerkung 18.3 folgt, daß die Nullstellen zu x_k in $T_{k+1}{:}T_k$ vollständig zerlegt in Nullstellen zu $x_{k+1} - a$ mit $a \in A$ sind. Somit erfüllt jede Nullstelle $\mathfrak{Q}$ zu x_0 eine der beiden folgenden Eigenschaften

(1) $\mathfrak{Q}$ ist eine gemeinsame Nullstelle von $x_0, x_1, \ldots, x_{m-1}$ und $x_m - b$ für ein $b \in A$.

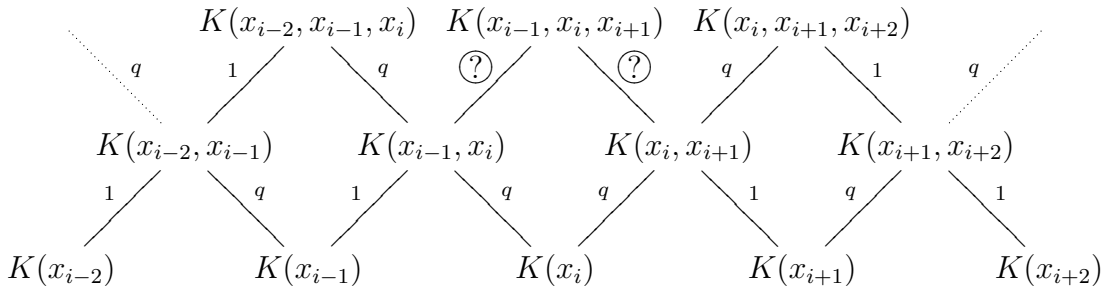
(2) Es gibt einen Index $i \in \{0, \ldots, m-1\}$ mit

(2a) $\mathfrak{Q}$ ist gemeinsame Nullstelle von $x_0, \ldots, x_{i-1}$.

(2b) $\mathfrak{Q}$ ist Nullstelle von $x_i - a$ für ein $a \in A^\times$.

(2c) $\mathfrak{Q}$ ist gemeinsame Polstelle zu $x_{i+1}, \ldots, x_m$.

Im ersten Fall ist $\mathfrak{Q}$ unverzweigt in $T_m{:}T_0$ und liefert somit keinen Beitrag zur Differente $\mathfrak{D}(T_m{:}T_0)$. Im zweiten Fall erhalten wir aus Bemerkung 12.10 das folgende Verzweigungsdiagramm zu $\mathfrak{Q}$:



$x_{i-2} \equiv 0$ $\quad$ $x_{i-1} \equiv 0$ $\quad$ $x_i \equiv a$ $\quad$ $x_{i+1} \equiv \infty$ $\quad$ $x_{i+2} \equiv \infty$

Man sieht, daß der Verzweigungsgrad $e_{\mathfrak{Q}}(K(x_{i-1}, x_i, x_{i+1}){:}K(x_{i-1}, x_i))$ nicht wie in Bemerkung 18.7 durch Diagrammabgleich erhalten werden kann. Stattdessen bekommen wir diesen mit Hilfe einer $\mathfrak{Q}$-ganzen erzeugenden Gleichung, die das Kernstück bei der Berechnung der Differente $\mathfrak{D}(T_m{:}T_0)$ bilden.

Bemerkung 18.8. *Für die Nullstellen $\mathfrak{Q}$ von $x_i - a$ mit $i \geq 1$ und $a \in A^\times$ gelten:*

(a) *In $T_i{:}T_0$ ist $\mathfrak{Q}$ vollständig zerlegt.*

(b) *In $T_{2i}{:}T_i$ ist $\mathfrak{Q}$ unverzweigt.*

(c) *Im Fall $m > 2i$ ist $\mathfrak{Q}$ total verzweigt in $T_m{:}T_{2i}$ mit dem Differentenexponenten $2(q^{m-2i} - 1)$.*

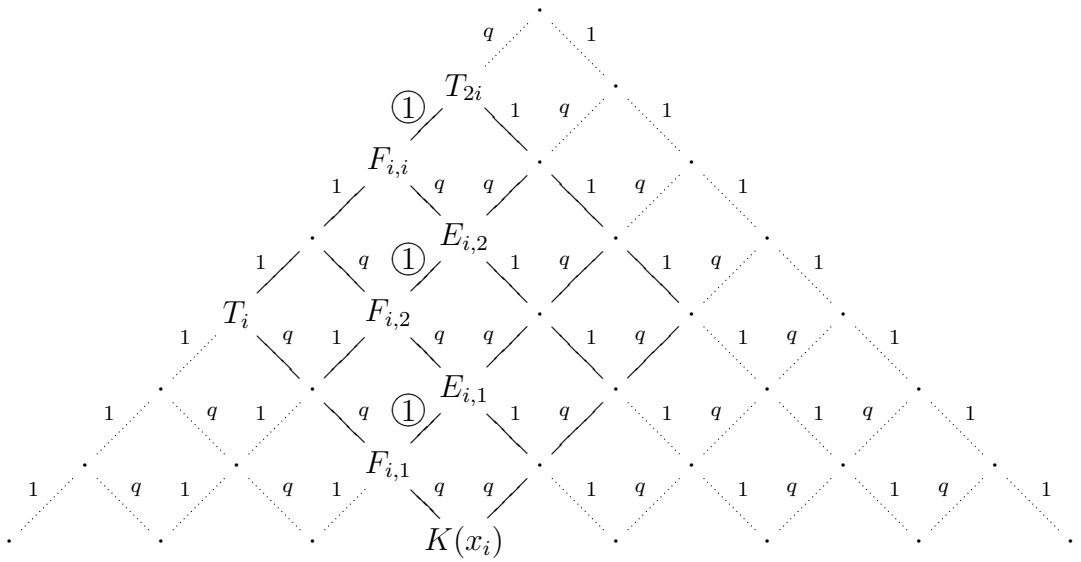
Beweis. Die Aussage (a) folgt wie oben für den Fall (1) aus der Bemerkung 12.2. Wir definieren

$$E_{i,j} := K(x_{i-j}, \ldots, x_{i+j}) \qquad \text{und} \qquad F_{i,j} := K(x_{i-j}, \ldots, x_{i+j-1})$$

für $j = 1, \ldots, i$. Hauptbestandteil des Beweises von Aussage (b) ist der Nachweis von

$$e_{\mathfrak{Q}}(E_{i,j}{:}F_{i,j}) = 1 \qquad \text{für } j = 1, \ldots, i.$$

Daraus ergeben sich alle restlichen Verzweigungsgrade $e_{\mathfrak{Q}}(E{:}F)$ in der Norm-Spur-Pyramide, indem man die einzelnen Diagramme vergleicht.



$x_0 \equiv 0 \qquad \cdots \qquad x_{i-1} \equiv 0 \qquad x_i \equiv a \qquad x_{i+1} \equiv \infty \qquad \cdots \qquad x_{2i} \equiv \infty$

Es sei $\mathfrak{Q}_j := \mathfrak{Q} \cap F_{i,j}$. Wir wollen zeigen, daß $\mathfrak{Q}_j$ unverzweigt ist in $E_{i,j}$:$F_{i,j}$. Die Artin-Schreier-Erweiterung $E_{i,j}$:$F_{i,j}$ wird erzeugt durch die Relation

$$x_{i+j}^q + x_{i+j} = \frac{x_{i+j-1}^q}{x_{i+j-1}^{q-1} + 1} =: w_j.$$

Nach Satz 11.12 reicht es also zu zeigen, daß es ein Element $u_j \in F_{i,j}$ gibt mit

$$\mathrm{ord}_{\mathfrak{Q}_j}(w_j + (u_j^q + u_j)) \geq 0.$$

Wir zeigen diese Aussage induktiv für $u_j := a^2 x_{i-j}^{-1}$ mit $1 \leq j \leq i$. Die Artin-Schreier-Funktion $u_j^q + u_j$ hat die Gestalt

$$u_j^q + u_j = a^{2q} x_{i-j}^{-q} + a^2 x_{i-j}^{-1} = (-a)^2 x_{i-j}^{-q} + a^2 x_{i-j}^{-1} \quad = \quad a^2(x_{i-j}^{-q} + x_{i-j}^{-1})$$

$$= a^2 \cdot \frac{1 + x_{i-j}^{q-1}}{x_{i-j}^q} \quad = \quad \frac{a^2}{x_{i-j+1}^q + x_{i-j+1}}.$$

Induktionsbeginn: Für $j = 1$ erhalten wir

$$w_1 + (u_1^q + u_1) = \frac{x_i^q}{x_i^{q-1} + 1} + \frac{a^2}{x_i^q + x_i} = \frac{x_i^{q+1} + a^2}{x_i^q + x_i} = \frac{x_i^{q+1} - a^{q+1}}{x_i^q + x_i}$$

$$= \sum_{k=0}^{q} x_i^k a^{q-k} \cdot \prod_{b \in A \setminus \{a\}} (x_i - b)^{-1}.$$

Folglich hat $w_1 + (u_1^q + u_1)$ nicht-negative Ordnung bei $\mathfrak{Q}_1$ vermöge der Kongruenz

$$w_1 + (u_1^q + u_1) \equiv \prod_{b \in A \setminus \{a\}} (a - b)^{-1} \cdot \sum_{k=0}^{q} (a^k a^{q-k}) = 1 \cdot (q+1) a^q = -a \pmod{\mathfrak{Q}_1}.$$

Induktionsschritt: Wir nehmen nun an, die Induktionsbehauptung gelte für ein j mit $1 \leq j \leq i-1$. Im folgenden verwenden wir - falls möglich - die Schreibweise $u = \mathcal{O}(\mathfrak{Q}_{j+1})$ für $u \in \mathfrak{Q}_{j+1}$. Da $\mathfrak{Q}_{j+1}$ eine Polstelle zu x_{i+j} ist, gelten $x_{i+j}^{-1} \in \mathfrak{Q}_{j+1}$ und

$$\begin{aligned} w_{j+1} = \frac{x_{i+j}^q}{x_{i+j}^{q-1}+1} = \frac{x_{i+j}}{1+(x_{i+j}^{-1})^{q-1}} &= x_{i+j}\left(1 - x_{i+j}^{-(q-1)} + x_{i+j}^{-2(q-1)} \mp \cdots\right) \\ &= x_{i+j} - x_{i+j}^{-(q-2)} + \mathcal{O}(\mathfrak{Q}_{j+1}) \end{aligned}$$

vermöge der Formel für geometrische Reihen. Genauer erhalten wir sogar

$$w_{j+1} = \frac{x_{i+j}^q}{x_{i+j}^{q-1}+1} = \begin{cases} x_{i+j} + 1 + \mathcal{O}(\mathfrak{Q}_{j+1}) & \text{falls } q = 2 \\ x_{i+j} + \mathcal{O}(\mathfrak{Q}_{j+1}) & \text{sonst.} \end{cases} \tag{18.9}$$

Desweiteren gilt

$$u_{j+1}^q + u_{j+1} = \frac{a^2}{x_{i-j}^q + x_{i-j}} = \frac{a^2(1+x_{i-j}^{q-1})}{x_{i-j}^q + x_{i-j}} - \frac{a^2 x_{i-j}^{q-2}}{x_{i-j}^{q-1}+1} = u_j - \frac{a^2 x_{i-j}^{q-2}}{x_{i-j}^{q-1}+1}.$$

Wegen $x_{i-j} \in \mathfrak{Q}_{j+1}$ ist $a^2 x_{i-j}^{q-2}/(x_{i-j}^{q-1}+1)$ eine über $\mathfrak{Q}_{j+1}$ ganze Funktion mit der Kongruenz $a^2 x_{i-j}^{q-2}/(x_{i-j}^{q-1}+1) \equiv a^2 x_{i-j}^{q-2} \pmod{\mathfrak{Q}_{j+1}}$ und ist genau dann nicht schon in $\mathfrak{Q}_{j+1}$ enthalten, wenn $q = 2$ gilt. In diesem Fall ist $a = 1$ vermöge $a \in A^\times = \mathbb{F}_2^\times$ und wir erhalten

$$u_{j+1}^q + u_{j+1} = \begin{cases} u_j + 1 + \mathcal{O}(\mathfrak{Q}_{j+1}) & \text{falls } q = 2 \\ u_j + \mathcal{O}(\mathfrak{Q}_{j+1}) & \text{sonst.} \end{cases} \tag{18.10}$$

Mit den Kongruenzen (18.9) und (18.10) folgt schließlich unabhängig von q

$$w_{j+1} + (u_{j+1}^q + u_{j+1}) = x_{i+j} + u_j + \mathcal{O}(\mathfrak{Q}_{j+1}).$$

Nach Induktionsvorausetzung gilt

$$\operatorname{ord}_{\mathfrak{Q}_j}((x_{i+j}+u_j)^q + (x_{i+j}+u_j)) = \operatorname{ord}_{\mathfrak{Q}_j}(w_j + (u_j^q + u_j)) \geq 0.$$

Daher folgt mit der Dreiecksungleichung für diskrete Bewertungen

$$\operatorname{ord}_{\mathfrak{Q}_{j+1}}(w_{j+1} + (u_{j+1}^q + u_{j+1})) \geq \min\{\operatorname{ord}_{\mathfrak{Q}_{j+1}}(x_{i+j}+u_j), \operatorname{ord}_{\mathfrak{Q}_{j+1}}(\mathcal{O}(\mathfrak{Q}_{j+1}))\} \geq 0.$$

Das schließt den Induktionsbeweis.

(c) Mittels Diagrammabgleich folgt aus dem Beweis zu (b), daß $\mathfrak{Q}$ in den Erweiterungen $T_m{:}T_{2i}$ für $m > 2i$ total verzweigt ist. Es bleibt also lediglich der Differentenexponent $d_{\mathfrak{Q}}(T_m{:}T_{2i})$ zu bestimmen. Als eine in $T_{2i+j}{:}K(x_{2i+j})$ unverzweigte Polstelle zu x_{2i+j} für $j = 0, \ldots, m-2i-1$ ist $\mathfrak{Q}$ eine einfache Polstelle zu $x_{2i+j}^q/(x_{2i+j}^{q-1}+1)$ und besitzt daher in $T_{2i+j+1}{:}T_{2i+j}$ den Index $m_{\mathfrak{Q}\cap T_{2i+j}} = 1$. Aus Satz 11.12 folgt hieraus $d_{\mathfrak{Q}}(T_{2i+j+1}{:}T_{2i+j}) = 2(q-1)$ und man erhält unsere Behauptung vermöge

$$d_{\mathfrak{Q}}(T_m{:}T_{2i}) = \sum_{j=1}^{m-2i} d_{\mathfrak{Q}}(T_{2i+j}{:}T_{2i+j-1}) \cdot q^{m-2i-j} = 2(q^{m-2i}-1). \qquad \square$$

18.3 Rationale Punkte im Norm-Spur-Turm

Bemerkung 18.11. *Alle rationalen Stellen außerhalb der Trägerstellen von $x_0^q + x_0$ sind vollständig zerlegt in der Norm-Spur-Pyramide, d.h. eine Nullstelle von $x_i - c$ mit $c \in K\backslash A$ ist rational und vollständig zerlegt in $T_m{:}K(x_i)$ für $i = 0, \ldots, m$.*

Beweis. Es seien $\mathfrak{R} \in \mathbb{P}_{T_m:K}$ ein primer Zählerdivisor von $x_i - c$ mit $c \in K\backslash A$ und

$$E_{i,j} := K(x_{i-j}, \ldots, x_i) \qquad \text{und} \qquad e := \frac{c^q}{c^{q-1} + 1}$$

für $0 \leq j \leq i$ sowie

$$F_{i,k} := K(x_i, \ldots, x_{i+k}) \qquad \text{und} \qquad f := \frac{1}{c^q + c}$$

für $0 \leq k \leq m - i$. Als Bilder von c unter der Norm- bzw. Spurabbildung sind c^{q+1}und $c^q + c$ in $\mathbb{F}_q^\times$ enthalten und somit auch e und f. Somit ist $\mathfrak{R} \cap E_{i,j}$ nach Bemerkung 18.3 als Nullstelle zu $x_{i+1}^q + x_{i+1} - e = x_i^q/(x_i^{q-1} + 1) - e$ vollständig zerlegt in $E_{i,j}(x_{i+1}){:}E_{i,j}$ und es gilt

$$x_{i+1} \equiv c_{i+1} \pmod{\mathfrak{R}} \qquad \text{mit} \qquad c_{i+1}^q + c_{i+1} = e \neq 0.$$

Ebenso ist $\mathfrak{R} \cap F_{i,j}$ als Nullstelle von $x_{i-1}^{-q} + x_{i-1}^{-1} - f = (x_i^q + x_i)^{-1} - f$ vollständig zerlegt in $F_{i,k}(x_{i-1}){:}F_{i,k}$ mit

$$x_{i-1} \equiv c_{i-1} \pmod{\mathfrak{R}} \qquad \text{mit} \qquad c_{i-1}^{-q} + c_{i-1} = f \neq 0,$$

wobei wir den Fall $i = 0$ weglasssen. Insbesondere ist $\mathfrak{R}$ eine Nullstelle von $x_{i-1} - c_{i-1}$ und $x_{i+1} - c_{i+1}$ mit $c_{i-1}, c_{i+1} \in K\backslash A$. Mit induktiver Wiederholung dieser Argumentation für $i \mapsto i - 1$ bzw. $i \mapsto i + 1$ erhält man schließlich, daß $\mathfrak{R}$ eine Nullstelle von $x_j - c_j$ mit $c_j \in K\backslash A$ für $j = 0, \ldots, m$ ist und daß $\mathfrak{R} \cap F$ in jeder Erweiterung $E{:}F$ der Norm-Spur-Pyramide vollständig zerlegt ist. Insbesondere ist $\mathfrak{R}$ rational in $T_m{:}K$. □

Folgende Bemerkung präzisiert die Aussage 18.8 (b).

Bemerkung 18.12. *Für die Nullstellen $\mathfrak{Q}$ von $x_i - a$ mit $i \geq 1$ und $a \in A^\times$ gelten:*

(a) *Bei ungerader Charakteristik ist $\mathfrak{Q}$ in $T_{i+1}{:}T_i$ unverzweigt mit nichttrivialem Trägheitsindex $f_{\mathfrak{Q}}(T_{i+1}{:}T_i) > 1$.*

(b) *Bei gerader Charakteristik ist $\mathfrak{Q}$ vollständig zerlegt in $T_{i+1}{:}T_i$. Für $i \geq 2$ besitzt $\mathfrak{Q}$ einen von 1 verschiedenen Trägheitsindex in $T_{i+2}{:}T_{i+1}$.*

Beweis. Es seien $\mathfrak{Q}^* := \mathfrak{Q} \cap T_i$ und $\mathfrak{Q}^{**} := \mathfrak{Q} \cap T_{i+1}$. Nach dem Beweis zu Bemerkung 18.8 ist

$$(x_{i+1} + a^2 x_{i-1}^{-1})^q + (x_{i+1} + a^2 x_{i-1}^{-1}) - \left(\frac{x_i^q}{x_i^{q-1}+1} + a^2(x_{i-1}^{-q} + x_{i-1}^{-1}) \right) = 0$$

eine $\mathfrak{Q}^*$-ganze Gleichung für $x_{i+1}+a^2x_{i-1}^{-1}$. Folglich besitzt $x_{i+1}+a^2x_{i-1}^{-1}$ als primitives Element der Körpererweiterung T_{i+1}:T_i das Minimalpolynom

$$g(T) := T^q + T - \left(\frac{x_i^q}{x_i^{q-1}+1} + a^2(x_{i-1}^{-q} + x_{i-1}^{-1}) \right) \in \mathcal{O}_{\mathfrak{Q}^*}[T].$$

Aus dem Induktionsanfang im Beweis zu Bemerkung 18.8 erhalten wir ebenfalls

$$g(T) \equiv T^q + T + a \pmod{\mathfrak{Q}^*}.$$

(a) Unter der Spurabbildung $c \mapsto c^q + c$ wird K auf $\mathbb{F}_q$ abgebildet. Im Fall $\mathrm{char}(K) \neq 2$ ist a nicht in $\mathbb{F}_q$ enthalten und somit besitzt $\overline{g}(T) := g(T) \pmod{\mathfrak{Q}^*}$ keine Nullstelle in K, d.h. alle irreduziblen Faktoren $p(T)$ von $\overline{g}(T)$ sind vom Grad $\deg(p) > 1$. Da $\overline{g}(T)$ separabel ist, stimmt der Trägheitsgrad der Fortsetzungen $\tilde{\mathfrak{Q}}|\mathfrak{Q}^*$ in T_{i+1}:T_i nach dem *Dedekind-Kriterium* mit dem Grad der irreduziblen Faktoren π überein. Somit besitzt $\mathfrak{Q}$ einen nichttrivialen Trägheitsindex in T_{i+1}:T_i.
(b) Im Fall gerader Charakteristik fällt A jedoch mit $\mathbb{F}_q$ zusammen. Somit ist $\mathfrak{Q}^*$ bzw. $\mathfrak{Q}$ nach Bemerkung 18.3 vollständig zerlegt in T_{i+1}:T_i und es gilt

$$x_{i+1} + a^2 x_{i-1}^{-1} \equiv b \pmod{\mathfrak{Q}^{**}} \qquad \text{für ein} \quad b \in A_a.$$

Das primitive Element $x_{i+2} + a^2 x_{i-2}^{-1}$ der Körpererweiterung T_{i+2}:T_{i+1} hat das Minimalpolynom

$$g(T) := T^q + T - \left(\frac{x_{i+1}^q}{x_{i+1}^{q-1}+1} + a^2(x_{i-2}^{-q} + x_{i-2}^{-1}) \right).$$

Aus dem Induktionsschritt zum Beweis zu Bemerkung 18.8 erhält man $g(T) \in \mathcal{O}_{\mathfrak{Q}^{**}}[T]$ und mit $j = 1$ die Kongruenz

$$g(T) \equiv T^q + T + x_{i+1} + a^2 x_{i-1}^{-1} \equiv T^q + T + b \pmod{\mathfrak{Q}^{**}}.$$

Wegen $b^q + b = a \neq 0$ ist b kein Körperelement von $\mathbb{F}_q$ und somit ist $g(T) \pmod{\mathfrak{Q}^{**}}$ wie im Beweis zu (a) nicht zerlegbar in Linearfaktoren. Das zeigt $f_{\mathfrak{Q}}(T_{i+2}|T_{i+1}) > 1$. □

Satz 18.13. (Garcia-Stichtenoth)

(a) *Der Norm-Spur-Turm T_m:K der Höhe $m \geq 1$ besitzt das Geschlecht*

$$g_m = \begin{cases} (q^{\frac{m+1}{2}} - 1)^2 & \text{für } m \equiv 1 \pmod 2 \\ (q^{\frac{m}{2}} - 1)(q^{\frac{m+2}{2}} - 1) & \text{für } m \equiv 0 \pmod 2. \end{cases}$$

(b) *Die Anzahl rationaler Stellen im Norm-Spur-Turm der Höhe $m \geq 1$ beträgt*

$$\#\mathbb{P}^{(1)}_{T_m:K} = q^m(q^2-q) + 2q + \varepsilon_m$$

mit $\varepsilon_m = 0$ bei ungerader Charakteristik oder $m = 1$ sowie $\varepsilon_2 = q(q-1)$ und $\varepsilon_m = 2q(q-1)$ für $m \geq 3$ bei gerader Charakteristik.

Beweis. (a) Nach den Bemerkungen 18.7 und 18.8 sind in $T_m{:}T_0$ nur die Stellen $\mathfrak{P}_\infty$, $\mathfrak{P}_a$ sowie die Nullstellen $\mathfrak{Q}$ von $x_i - a$ mit $a \in A^\times$ und $1 \leq i \leq \left\lfloor \frac{m-1}{2} \right\rfloor$ verzweigt. Der Gradanteil der Stellen $\mathfrak{P}_\infty$ und $\mathfrak{P}_a$ zu der Differente $\mathfrak{D}(T_m{:}T_0)$ von $T_m{:}T_0$ beträgt jeweils $2(q^m-1)$. Nach der *arithmetischen Gradformel* $\sum e_j f_j = n$ und Bemerkung 18.8 gilt

$$\deg(\mathfrak{A}_{a,i}) = q^i \qquad \text{für} \quad \mathfrak{A}_{a,i} := \textstyle\prod_{x_i \equiv a(\mathfrak{Q})} \mathfrak{Q}$$

und der Divisor $\mathfrak{A}_{a,i}$ hat den Gradanteil $2(q^{m-2i}-1)q^i = 2(q^{m-i}-q^i)$ zu $\mathfrak{D}(T_m{:}T_0)$. Somit ergibt sich insgesamt für den Grad der Differente $\mathfrak{D}(T_m{:}T_0)$ der Erweiterung $T_m{:}T_0$

$$\begin{aligned}
\deg(\mathfrak{D}(T_m{:}T_0)) &= q \cdot 2(q^m-1) + (q-1) \sum_{i=1}^{\lfloor (m-1)/2 \rfloor} 2(q^{m-i} - q^i) \\
&= 2\left(q^{m+1} - q + q^m - q^{m-\lfloor (m-1)/2 \rfloor} - q^{1+\lfloor (m-1)/2 \rfloor} + q\right) \\
&= \begin{cases} 2(q^{m+1} + q^m - 2q^{(m-1)/2}) & \text{für } m \equiv 1 \pmod 2 \\ 2(q^{m+1} + q^m - q^{(m+2)/2} - q^{m/2}) & \text{für } m \equiv 0 \pmod 2. \end{cases}
\end{aligned}$$

Die Behauptung folgt nun aus $g_0 = g(K(x_0)) = 0$ und der *Hurwitzschen Relativgeschlechtsformel* vermöge

$$g_m = 1 + (g_0 - 1)[T_m{:}T_0] + \frac{1}{2}\deg(\mathfrak{D}(T_m{:}T_0)) = 1 - q^m + \frac{1}{2}\deg(\mathfrak{D}(T_m{:}T_0)).$$

(b) Nach den Bemerkungen 18.7 und 18.11 sind die Nullstellen von $x_0 - a$ für $a \in A^\times$ total verzweigt und die Zählerdivisoren von $x_0 - c$ mit $c \in K \backslash A$ vollständig zerlegt in $T_m{:}K(x_0)$. Zudem ist der Poldivisor $\mathfrak{P}_\infty$ ebenfalls total verzweigt in $T_m{:}K(x_0)$. Das zeigt

$$\#\mathbb{P}^{(1)}_{T_m:K} \geq q^m(q^2-q) + (q-1) + 1 = q^{m+2} - q^{m+1} + q.$$

In der Auflistung der rationalen Stellen in $T_m{:}K$ fehlen also nur noch die Fortsetzungen des Zählerdivisors $\mathfrak{P}_0$ zu x_0. Eine solche ist nach unseren obigen Überlegungen entweder ein gemeinsamer Zählerdivisor von $x_0, \ldots, x_{m-1}$ oder eine Nullstelle von $x_i - a$ für ein $a \in A^\times$ und $1 \leq i \leq m-1$. Die gemeinsamen Nullstellen von $x_0, \ldots, x_{m-1}$ sind rational in $T_m{:}K$ und folglich zählt man zu der obigen Abschätzung noch q weitere Stellen hinzu, d.h. es gilt

$$\#\mathbb{P}^{(1)}_{T_m:K} \geq q^{m+2} - q^{m+1} + 2q = r_m.$$

Diese Schranke ist scharf für $m = 1$. Für $m \geq 2$ und $\mathrm{char}(K) \neq 2$ sind sämtliche Nullstellen zu $x_i - a$ mit $1 \leq i \leq m-1$ nach Bemerkung 18.12 nicht-rational. Somit ist die vorgestellte Schranke auch scharf für jede Stufe m bei ungerader Charakteristik.

Im Fall gerader Charakteristik sind die Nullstellen zu $x_1 - a$ nach Bemerkung 18.12 vollständig zerlegt in $T_2{:}T_1$ und nach Bemerkung 18.8 total verzweigt in $T_m{:}T_2$. Diese $q(q-1)$ Fortsetzungen von $\mathfrak{P}_0$ sind also rational in $T_m{:}K$. Im Fall $m = 2$ zeigt dies

$$\#\mathbb{P}^{(1)}_{T_2:K} = q^4 - q^3 + 2q + q(q-1) = r_2 + \varepsilon_2.$$

Für $m \geq 3$ und $2 \leq i \leq m-2$ gehen die Nullstellen von $x_i - a$ ähnlich wie im Fall $\mathrm{char}(K) \neq 2$ wegen ihren nicht-trivialen Trägheitsindex in $T_{i+2}{:}T_{i+1}$ als rationale Stellen verloren. Der Zählerdivisor zu $x_{m-1} - a$ besitzt hingegen q rationale Fortsetzungen in $T_m{:}K$. Das zeigt schließlich

$$\#\mathbb{P}^{(1)}_{T_m:K} = q^{m+2} - q^{m+1} + 2q + 2q(q-1) = r_m + \varepsilon_m. \qquad \square$$

In der Diplomarbeit [Lag06] findet man eine eingehende Untersuchung der Standardcodes im Norm-Spur-Turm, die aus den Riemann-Roch-Räumen $\mathcal{L}(\mathfrak{P}^r_\infty)$ gewonnen werden. Diese sind u.a. deswegen interessant, da sie eine Codeklasse oberhalb der *Gilbert-Varshamov-Schranke* bilden. Sie sind also Beispiele für die in Korollar 19.10 angesprochenen Codes. Zudem enthält [Lag06] Berechnungen zur Automorphismengruppe des Norm-Spur-Turms.[1]

[1] Ein Artikel mit den Ergebnissen ist in Vorbereitung.

Kapitel 19

Asymptotische Schranken für arithmetische Codes

Dieses Kapitel enthält als einen der Höhepunkte der Vorlesung einen Beweis des Satzes von *Tsfasman-Vladut-Zink* über die asymptotische obere Schranke der Anzahl rationaler Stellen in Kongruenzfunktionenkörpern relativ zu deren Geschlecht. Diese zieht die Existenz von arithmetischen Codes oberhalb der *Gilbert-Varshamov-Schranke* nach sich.

19.1 Serre-Schranke

Definition 19.1. Es seien q eine Primzahlpotenz und $g \in \mathbb{N}$. Bezeichnet $N_1(F)$ die Anzahl aller rationalen Stellen in $F{:}\mathbb{F}_q$, so definieren wir

(a) $N(g,q) := \max\{N_1(F) : F{:}\mathbb{F}_q \text{ ist ein Funktionenkörper vom Geschlecht } g\}$.

(b) $N(q) := \limsup\limits_{g\to\infty} \frac{N(g,q)}{g}$.

Mit der *Hasse-Weil-Schranke* folgt sofort

Bemerkung 19.2. *Für eine Primzahlpotenz q gilt die Abschätzung*

$$N(q) \leq 2\sqrt{q}.$$

Beweis. Für die Anzahl N_1 der rationalen Stellen eines Kongruenzfunktionenkörpers über $\mathbb{F}_q$ vom Geschlecht g gilt nach der *Hasse-Weil-Schranke*

$$|N_1 - (q+1)| \leq 2g\sqrt{q}.$$

Folglich ist $N(g,q)$ beschränkt durch $q+1+2g\sqrt{q}$ und es gilt

$$N(q) \leq \lim_{g\to\infty} \left(\frac{q+1}{g} + 2\sqrt{q}\right) = 2\sqrt{q}. \qquad \square$$

Beispiel 19.3. Mit den Parametern für den Norm-Spur-Turm T_m:$\mathbb{F}_{q^2}$ aus Kapiel 18 gilt

$$N(q^2) \geq \lim_{m\to\infty} \frac{q^{m+1}(q-1)}{(q^{\frac{m+1}{2}}-1)^2} = q-1.$$

Ist q eine quadratische Primzahlpotenz, so ist die *Hasse-Weil-Schranke* scharf. Die Hermiteschen Funktionenkörper (Kapitel 17) sind ein Beispiel dafür. Für nichtquadratische q kann die *Hasse-Weil-Schranke* verbessert werden.

Satz 19.4. (Schranke von Serre)
Es sei F:$\mathbb{F}_q$ ein Kongruenzfunktionkörper vom Geschlecht g. Dann unterliegt die Anzahl N_1 der rationalen Stellen in F der Schranke

$$|N_1 - (q+1)| \leq g\lfloor 2\sqrt{q}\rfloor.$$

Beweis. Da Kongruenzfunktionenkörper vom Geschlecht 0 stets rational sind (Satz von *F.K.Schmidt*) und damit genau $q+1$ rationale Stellen besitzen, können wir im folgenden $g > 0$ annehmen. Es sei $\mathbb{A}$ der Ring der ganzen algebraischen Zahlen in $\mathbb{C}$, d.h. der Ring aller komplexen Zahlen, die Nullstelle eines normierten Polynoms aus $\mathbb{Z}[T]$ sind. Wir betrachten das L-Polynom $L_{F:\mathbb{F}_q}(t) = \prod_{i=1}^{2g}(1-\omega_i t)$ von F:$\mathbb{F}_q$. Die Weilzahlen $\omega_i \in \mathbb{A}$ haben Betrag $|\omega_i| = \sqrt{q}$ nach dem Satz von *Hasse-Weil* und können so angeordnet werden, daß $\omega_i\omega_{g+i} = q$ und somit $\overline{\omega_i} = \omega_{g+i} = \frac{q}{\omega_i}$ gilt. Die reellen ganzen Zahlen

$$c_i := \omega_i + \overline{\omega_i} + \lfloor 2\sqrt{q}\rfloor + 1 \qquad \text{und} \qquad d_i := -\omega_i - \overline{\omega_i} + \lfloor 2\sqrt{q}\rfloor + 1$$

sind aufgrund $|\omega_i| = \sqrt{q}$ strikt positiv. Es seien N die galoissche Hülle von $\mathbb{Q}(w_1,\ldots,w_{2g})$:$\mathbb{Q}$ und $\sigma \in \mathrm{Gal}(N{:}\mathbb{Q})$. Da $L(t)$ ein Polynom mit Koeffizienten aus $\mathbb{Z}$ ist, permutiert σ die Weilzahlen $\omega_1,\ldots,\omega_{2g}$. Es gilt weiter

$$\sigma(\overline{\omega_i}) = \sigma(q/\omega_i) = q/\sigma(\omega_i) = \overline{\sigma(\omega_i)}.$$

Somit permutiert σ sowohl die Zahlen $c_1,\ldots,c_g$ als auch $d_1,\ldots,d_g$ und die Produkte

$$c := \prod_{i=1}^{g} c_i \qquad \text{und} \qquad d := \prod_{i=1}^{g} d_i$$

sind invariant unter $\mathrm{Gal}(N{:}\mathbb{Q})$. Also sind c und d echt positive ganze algebraische Zahlen aus $\mathbb{Q}$. Wegen $\mathbb{Q}\cap\mathbb{A} = \mathbb{Z}$ hat dies schließlich $c \geq 1$ und $d \geq 1$ zur Folge. Aus der Ungleichung zwischen dem arithmetischen und geometrischen Mittelwert erhalten wir

$$\frac{1}{g}\sum_{i=1}^{g} c_i \geq \left(\prod_{i=1}^{g} c_i\right)^{\frac{1}{g}} = c^{\frac{1}{g}} \geq 1.$$

Daraus folgt dann mit der Definition der c_i

$$g \leq \sum_{i=1}^{g} c_i = \left(\sum_{i=1}^{g} (\omega_i + \overline{\omega_i}) \right) + g\lfloor 2\sqrt{q} \rfloor + g = \sum_{i=1}^{2g} \omega_i + g\lfloor 2\sqrt{q} \rfloor + g.$$

Da die Summe aller Weilzahlen gleich $(q+1) - N_1$ ist folgt die Abschätzung

$$N_1 \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor.$$

Analog folgert man aus der Ungleichung

$$\frac{1}{g} \sum_{i=1}^{g} d_i \geq \left(\prod_{i=1}^{g} d_i \right)^{\frac{1}{g}} = d^{\frac{1}{g}} \geq 1$$

die Abschätzung

$$N_1 \geq q + 1 - g\lfloor 2\sqrt{q} \rfloor. \qquad \square$$

Mit dieser verbesserten Schranke erhält man analog zu Bemerkung 19.2 das folgende

Korollar 19.5. *Für eine Primzahlpotenz q gilt die Ungleichung*

$$N(q) \leq \lfloor 2\sqrt{q} \rfloor. \qquad \square$$

19.2 Der Satz von Drinfeld-Vladut

Die Abschätzung aus Korollar 19.5 kann weiter verbessert werden durch

Satz 19.6. (Drinfeld-Vladut)
Für eine Primzahlpotenz q gilt die Ungleichung

$$N(q) \leq \sqrt{q} - 1.$$

Beweis. Es seien $F{:}\mathbb{F}_q$ ein Kongruenzfunktionenkörper vom Geschlecht g sowie $\omega_1, \ldots, \omega_{2g}$ seine Weilzahlen mit $|\omega_i| = \sqrt{q}$. Dann sind

$$v_i := \frac{\omega_i}{\sqrt{q}}$$

Einheitswurzeln in $\mathbb{C}$. Für die Anzahl N_r der rationalen Stellen bei einer Konstantenerweiterung von F mit Grad r gilt

$$N_r - (q^r + 1) = -\sum_{i=1}^{2g} \omega_i^r = -\sqrt{q}^{\,r} \sum_{i=1}^{2g} v_i^r.$$

Da bei einer Konstantenerweiterung keine rationalen Stellen verloren gehen, folgen hieraus die Ungleichungen

$$N_1 \sqrt{q}^{\,-r} \leq N_r \sqrt{q}^{\,-r} = \sqrt{q}^{\,r} + \sqrt{q}^{\,-r} - \sum_{i=1}^{2g} v_i^r$$

und

$$\sum_{i=1}^{2g} v_i^r \leq \sqrt{q}^{\,r} + \sqrt{q}^{\,-r} - N_1\sqrt{q}^{\,-r}. \qquad (*)$$

Es sei m eine beliebige natürliche Zahl. Da $v_1, \ldots, v_{2g}$ Einheitswurzeln in $\mathbb{C}$ sind, gilt dann

$$\begin{aligned} 0 \leq \left| \sum_{r=0}^{m} v_i^{\,r} \right|^2 &= \left(\sum_{r=0}^{m} v_i^r \right) \cdot \left(\sum_{s=0}^{m} v_i^{-s} \right) = \sum_{r,s=0}^{m} v_i^{r-s} \\ &= m+1+\sum_{r=1}^{m} (m+1-r)(v_i^r + v_i^{-r}). \end{aligned}$$

Summieren wir diese Ungleichung über $i = 1, \ldots, 2g$, so erhalten wir mit der vorletzten Abschätzung $(*)$

$$\begin{aligned} 0 &\leq 2g(m+1) + \sum_{r=1}^{m} (m+1-r) \sum_{i=1}^{2g} (v_i^r + v_i^{-r}) \\ &= 2g(m+1) + 2\sum_{r=1}^{m} (m+1-r) \sum_{i=1}^{2g} v_i^r \\ &\leq 2g(m+1) + 2\sum_{r=1}^{m} (m+1-r)(\sqrt{q}^{\,r} + \sqrt{q}^{\,-r} - N_1\sqrt{q}^{\,-r}). \end{aligned}$$

Das zeigt

$$\frac{N_1}{g} \sum_{r=1}^{m} \frac{m+1-r}{m+1} \sqrt{q}^{\,-1} \leq 1 + \frac{1}{g} \sum_{r=1}^{m} \frac{m+1-r}{m+1} (\sqrt{q} + \sqrt{q}^{\,-1})$$

Wir definieren $h_m(t) := \sum_{r=1}^{m} \frac{m+1-r}{m+1}\, t^r$. Mit dieser Bezeichnung ist dann die obige Ungleichung äquivalent zu

$$\frac{N_1}{g} \leq \frac{1}{h_m(\sqrt{q}^{\,-r})} + \frac{1}{g}\left(1 + \frac{h_m(\sqrt{q}^{\,r})}{h_m(\sqrt{q}^{\,-r})}\right).$$

Es läßt sich leicht verifizieren, daß für $t \neq 1$

$$h_m(t) = \sum_{r=1}^{m} \frac{m+1-r}{m+1}\, t^r = \frac{t}{(1-t)^2}\left(\frac{t^{m+1}-1}{m+1} + 1 - t\right)$$

und für $t < 1$

$$\lim_{m\to\infty} (h_m(t)) = \frac{t}{(1-t)}$$

gelten. Also existiert für jedes $\varepsilon > 0$ eine natürliche Zahl m_0 mit

$$\frac{1}{h_{m_0}(\sqrt{q}^{\,-1})} < \frac{\left(1-\sqrt{q}^{\,-1}\right)}{\sqrt{q}^{\,-1}} + \frac{\varepsilon}{2} = \sqrt{q} - 1 + \frac{\varepsilon}{2}\,.$$

Desweiteren sei $g_0 \in \mathbb{N}$ hinreichend groß gewählt, sodaß

$$\frac{1}{g_0}\left(1+\frac{h_m(\sqrt{q})}{h_m(\sqrt{q}^{-1})}\right) \leq \frac{\varepsilon}{2}$$

gilt. Dann gilt folgt alle $g \geq g_0$ die Abschätzung

$$\frac{N_1}{g} \leq \sqrt{q} - 1 + \varepsilon.$$

Das zeigt schließlich $N(q) = \limsup_{g\to\infty} \frac{N_1}{g} \leq \sqrt{q} - 1$. □

Zusammen mit Beispiel 19.3 folgt

Korollar 19.7. (Tsfasman-Vladut-Zink)
Für eine Primzahlpotenz q gilt

$$N(q^2) = q - 1.$$

19.3 Vergleich mit der Gilbert-Varshomov Schranke

Im Anschluß von Abschnitt 9.3 zeigen wir nun, daß sich die *asymptotische Gilbert-Varshomov-Schranke* (9.13) mit der aus dem Satz von *Drinfeld-Vladut* ergebenden asymptotische Schranke für arithmetische Codes in einem gewissen Bereich verbessern läßt. Dabei müssen wir grundsätzlich voraussetzen, daß q ein Quadrat ist.

Bemerkung 19.8. (AG - Schranke)
Für die asymptotische Informationsrate der arithmetischen Codes über $\mathbb{F}_q$ bei quadratischer Primzahlpotenz q mit relativer Distanz δ gilt

$$R_q(\delta) \geq 1 - \delta - \frac{1}{\sqrt{q}-1}\ .$$

Beweis. Nach Korollar 11.4 ist die Dimension eines maximalen arithmetischen Codes der Länge n und Minimaldistanz d (falls er existiert) mindestens $n - (g-1) - d$. Daraus folgen

$$\log_q(A_q(n,d)) \geq n - (g-1) - d$$

und (mit $\delta = d/n$)

$$R_q(\delta) = \limsup_{n\to\infty} \frac{1}{n}\ \log_q(A_q(n,\delta n)) \geq 1 - \delta - \limsup_{n\to\infty} \frac{g}{n}.$$

Mit der Gleichheit aus Korollar 19.7 erhalten wir schließlich

$$R_q(\delta) \geq 1 - \delta - \frac{1}{\sqrt{q}-1}.$$ □

Satz 19.9. *Ab $q \geq 49$ verbessert die asymptotische Schranke für arithmetische Codes über $\mathbb{F}_q$ bei quadratischen q die asymptotische Gilbert-Varshomov Schranke im Intervall (δ_1, δ_2), wobei δ_1, δ_2 die Nullstellen der Gleichnung $H_{q^2}(\delta) - \delta = \frac{1}{\sqrt{q}-1}$ sind.*

Beweis. Die *AG-Schranke* ist linear mit Anstieg -1. Wir zeigen zunächst, daß die zur *AG-Schranke* parallele Tangente $\mathcal{T}$ an der *Gilbert-Varshomov-Schranke* $1-H_q(\delta)$ durch den Punkt $(\delta_0, 1 - H_q(\delta_0))$ mit

$$\delta_0 := \frac{q-1}{2q-1}$$

geht. Dazu bilden wir die Ableitung von $H_q(x)$ nach x.

$$\begin{aligned} H_q'(x) &= \left(x \log_q \left(\frac{1-x}{x}(q-1) \right) - \log_q(1-x) \right)' \\ &= \log_q \left(\frac{1-x}{x}(q-1) \right) + x \cdot \frac{1-q}{x^2} \cdot \frac{x}{(1-x)(q-1)} - (-1) \cdot \frac{1}{1-x} \\ &= \log_q \left(\frac{1-x}{x}(q-1) \right). \end{aligned}$$

Es ist also $H_q'(x) = 1$ genau dann, wenn $xq = (q-1)(1-x)$ gilt. Das ist für $x = \delta_0$ der Fall. Es gilt dann

$$H_q(\delta_0) = \delta_0 \log_q \left((2q-1) \cdot (1-\delta_0) \right) - \log_q (1-\delta_0) = \delta_0 - 1 + \log_q(2q-1).$$

Die Punkte (R, δ) auf der Tangente $\mathcal{T}$ erfüllen also die Gleichung

$$R - (1 - H_q(\delta_0)) = -1 \cdot (\delta - \delta_0)$$

beziehungsweise

$$R = (1 - H_q(\delta_0)) + \delta_0 - \delta = -\delta + 2 - \log_q(2q-1).$$

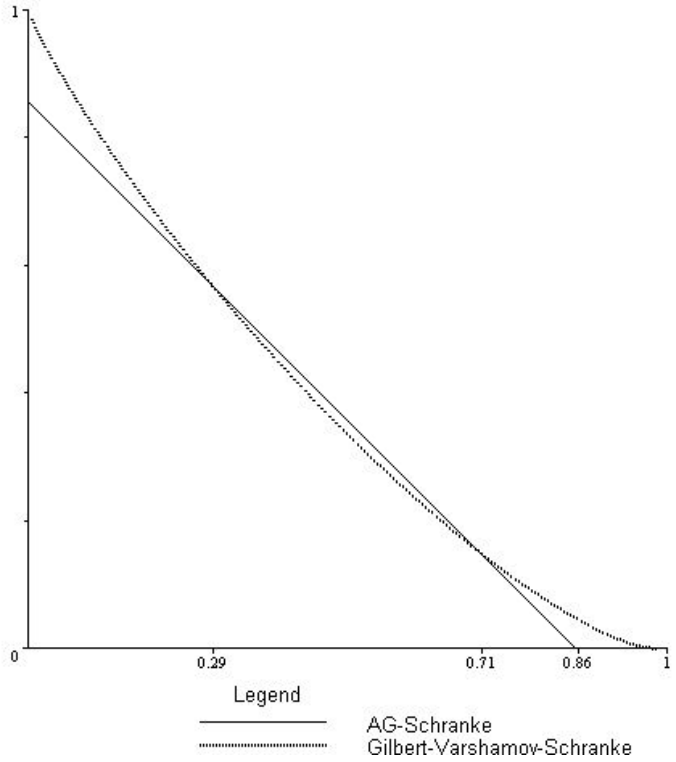
Die *AG-Schranke* schneidet die *Gilbert-Varshomov-Schranke* also genau dann, wenn $\log_q(2q-1) - 1 > (\sqrt{q}-1)^{-1}$ beziehungsweise

$$\log_q(2q-1) > \frac{\sqrt{q}}{\sqrt{q}-1}$$

gilt. Dies ist für $q \geq 49$ der Fall. □

Korollar 19.10. *Es gibt arithmetische Codes oberhalb der Gilbert-Varshomov-Schranke.*

Im folgenden Diagramm wird die Verbesserung der *Gilbert-Varshamov-Schranke* durch die *AG-Schranke* beispielhaft für $q = 64$ verdeutlich.



Asymptotische untere Schranken für $q = 64$

Kapitel 20

Lineare Codes als arithmetische Codes

Definitionsgemäß ist jeder arithmetische Code linear. In diesen Kapitel zeigen wir, daß jeder lineare Code über $\mathbb{F}_q$ zumindest ein auf $\mathbb{F}_q$ eingeschränkter Teilkörpercode eines arithmetischen Codes und damit ein verallgemeinerter arithmetischer Code ist.

20.1 Der gewöhnliche Spurturm

Definition 20.1. (Gewöhnlicher Spurturm)
Der Kongruenzfunktionenkörper $F_m := \mathbb{F}_q(x_0, x_1, \ldots, x_m)$ mit den definierenden Relationen

$$x_i^q - x_i = x_{i-1}(x_{i-1}^q - x_{i-1}) \qquad \text{für } i = 1, \ldots, m$$

heißt **gewöhnlicher** (oder auch **vektorieller**) **Spurturm** der Stufe m über $\mathbb{F}_q$.

Bemerkung 20.2. (Verzweigung im gewöhnlichen Spurturm)
Es sei F_m ein gewöhnlicher Spurturm über $\mathbb{F}_q$. Dann gelten:

(a) *Die Erweiterung F_m:F_0 ist geometrisch vom Grad q^m.*

(b) *Der Nennerdivisor von x_0 ist in F_m:F_0 total verzweigt; es gilt etwa*

$$(x_0)_\infty = \mathfrak{P}_\infty^{q^m}.$$

(c) *Die Differente von F_m:F_0 hat die Gestalt*

$$\mathfrak{D}(F_m{:}F_0) = \mathfrak{P}_\infty^{d_\infty} \qquad \textit{mit } \; d_\infty = (q^2-1)((q+1)^m - q^m) + q^m - 1.$$

Beweis. Sämtliche Körpererweiterungen F_l:F_{l-1} für $l = 1, \ldots, m$ besitzten Grad q und sind als Artin-Schreier-Erweiterungen geometrisch. Folglich ist F_m:F_0 geometrisch vom Grad q^m. Es bleiben somit noch (b) und (c) zu zeigen.

In jeder der Artin-Schreier Erweiterungen $F_l{:}F_{l-1}$ sind nach Satz 18.2 nur die Polstellen von x_{l-1} verzweigt. Aus den definierenden Gleichungen von F_m folgt

$$(x_l)_\infty^q = (x_{l-1})_\infty^{q+1} \qquad \text{für } l = 1, \ldots, m.$$

Also sind alle Polstellen von x_{l-1} in $F_l{:}F_{l-1}$ total verzweigt. Das hat zur Folge, daß $x_0, x_1, \ldots, x_m$ genau eine Polstelle $\mathfrak{P}_\infty$ besitzen und diese in $F_m{:}F_0$ total verzweigt mit Index $e_{\mathfrak{P}_\infty}(F_m{:}F_0) = q^m$ ist. Das beweist die Aussage (b). Desweiteren besitzt $x_{l-1}^{q+1} - x_{l-1}^2$ in F_{l-1} den Polstellendivisor

$$(x_{l-1}^{q+1} - x_{l-1}^2)_\infty = \mathfrak{P}_\infty^{(q+1)^l}.$$

Somit ist nach Satz 18.2

$$\deg(\mathfrak{D}(F_l{:}F_{l-1})) = (q-1)((q+1)^l + 1)$$

der Differentengrad der Erweiterungen $F_l{:}F_{l-1}$. Dies impliziert für den Differentengrad von $F_m{:}F_0$ vermöge der Formel für geometrischen Reihen

$$\begin{aligned}
\deg(\mathfrak{D}(F_m{:}F_0)) &= \sum_{l=1}^{m} q^{m-l} \deg(\mathfrak{D}(F_l{:}F_{l-1})) = \sum_{l=1}^{m} q^{m-l}(q-1)((q+1)^l + 1) \\
&= q^m(q-1)\left(\frac{q+1}{q} \cdot \frac{(q+1)^m - q^m}{q^{m-1}} + \frac{1}{q} \cdot \frac{q^m - 1}{q^{m-1}(q-1)}\right) \\
&= (q^2-1)((q+1)^m - q^m) + q^m - 1 = d_\infty.
\end{aligned}$$

Da nur $\mathfrak{P}_\infty$ in $F_m{:}F_0$ verzweigt ist, folgt hieraus die Aussage (c). □

Satz 20.3. (Geschlecht und Anzahl rationaler Stellen)
Für einen gewöhnlichen Spurturm F_m über $\mathbb{F}_q$ gelten:

(a) *Das Geschlecht von $F_m{:}\mathbb{F}_q$ beträgt*

$$g_m = \frac{q-1}{2}\left((q+1)^{m+1} - \frac{q^{m+2}-1}{q-1}\right).$$

(b) *Die Anzahl der rationalen Stellen in F_m ist*

$$\#\mathbb{P}_{F_m:\mathbb{F}_q}^{(1)} = q^{m+1} + 1.$$

Beweis. Das Geschlecht berechnen wir mit der *Hurwitzschen Relativgeschlechtformel* und Bemerkung 20.2 vermöge

$$\begin{aligned}
g_m &= 1 - [F_m{:}F_0] + \frac{\deg(\mathfrak{D}(F_m{:}F_0))}{2} = \frac{1}{2}\left((q^2-1)\left((q+1)^m - q^m\right) - q^m + 1\right) \\
&= \frac{1}{2}\left((q-1)(q+1)^{m+1} - q^{m+2} + 1\right).
\end{aligned}$$

Nach dem *Dedekind-Kriterium* sind die Nullstellen von $x_{l-1}^q - x_{l-1}$ voll zerlegt in F_l:F_{l-1}. Daher sind alle rationalen Stellen von F_0 außer dem Nennerprimteiler $\mathfrak{P}_\infty$ von x_0 voll zerlegt in F_m:F_0, und es ist $(x_0^q - x_0)_0$ das Produkt von $q \cdot [F_m{:}F_0] = q^{m+1}$ rationalen Stellen in F_m. Somit ergibt sich die Anzahl rationaler Stellen

$$\#\mathbb{P}^{(1)}_{F_m:\mathbb{F}_q} = q^{m+1} + 1. \qquad \square$$

Korollar 20.4. (Vektorraumstruktur der rationalen Zählerstellen von $x_m^q - x_m$)
Die Abbildung

$$\alpha : \begin{cases} \mathbb{P}^{(1)}_{F_m:\mathbb{F}_q} \setminus \{\mathfrak{P}_\infty\} & \longrightarrow & \mathbb{F}_q^{m+1} \\ \mathfrak{P} & \longmapsto & (x_0(\mathfrak{P}), x_1(\mathfrak{P}), \ldots, x_m(\mathfrak{P})) \end{cases}$$

ist eine bijektive Abbildung von der Menge der Zählerprimteiler von $x_m^q - x_m$ im gewöhnlichen Spurturm F_m:$\mathbb{F}_q$ auf $\mathbb{F}_q^{m+1}$.

Beweis. Nach dem *Dedekind-Kriterium* ist jede rationale Stelle $\mathfrak{Q} \neq \mathfrak{P}_\infty$ aus F_{l-1} zerlegbar in ein Produkt rationaler Stellen aus F_l und es gilt dabei

$$\mathfrak{Q} = \prod_{a \in \mathbb{F}_q} \mathfrak{Q}_a \qquad \text{mit} \quad x_l \equiv a \pmod{\mathfrak{Q}_a}.$$

Ist also ein Vektor $(a_0, \ldots, a_m) \in \mathbb{F}_q^{m+1}$ gegeben, so besitzt die Stelle $(x - a_0)_0 \in \mathbb{P}^{(1)}_{F_0:\mathbb{F}_q}$ rationale Fortsetzungen $\mathfrak{P}^{(l)}$ in F_l mit

$$x_i \equiv a_i \pmod{\mathfrak{P}^{(l)}} \qquad \text{für } i = 1, \ldots, l.$$

Es ist dann $\mathfrak{P}^{(m)}$ das Urbild von $(a_0, \ldots, a_m)$ unter α. Das zeigt die Surjektivität und damit die Bijektivität von α. $\square$

20.2 Lineare Standardräume im Spurturm

Satz 20.5. (Pol- und Fehlzahlen von $\mathfrak{P}_\infty$)
Es seien F_m:$\mathbb{F}_q$ ein gewöhnlicher Spurturm und $\mathfrak{P}_\infty$ der Nennerprimteiler von x_0. Dann werden die Polzahlen von $\mathfrak{P}_\infty$ durch die Variablen $x_0, x_1, \ldots, x_m$ erzeugt. Genauer gelten:

(a) *$\mathfrak{P}_\infty$ hat die Polzahlhalbgruppe*

$$\mathbb{H}_m := \left\{ \sum_{i=0}^{m} a_i q^{m-i} (q+1)^i : a_i \in \mathbb{N} \right\}.$$

(b) *Der lineare Raum $\mathcal{L}(\mathfrak{P}_\infty^r)$ wird erzeugt von den Funktionen der Form*

$$x_0^{a_0} \cdots x_m^{a_m} \qquad \textit{mit } a_i \in \mathbb{N} \textit{ und } \sum_{i=0}^{m} a_i q^{m-i} (q+1)^i \leq r.$$

Beweis. Aus den definierenden Relationen des gewöhnlichen Spurturms F_m gelten

$$(x_0)_\infty^{q^m} = \mathfrak{P}_\infty, \quad (x_1)_\infty = (x_0)_\infty^{\frac{q+1}{q}} = \mathfrak{P}_\infty^{q^{m-1}(q+1)}$$

und allgemein

$$(x_i)_\infty = \mathfrak{P}_\infty^{q^{m-i}(q+1)^i}$$

für die Nennerdivisoren der Variablen $x_0, x_1, \ldots, x_m$. Daher ist $\mathbb{H}_m$ in der Polzahlhalbgruppe von $\mathfrak{P}_\infty$ enthalten und es gilt

$$\mathcal{L}(\mathfrak{P}_\infty^r) \geq \mathbb{F}_q\langle x_0^{a_0} \cdots a_m^{a_m} \ : \ a_i \in \mathbb{N} \text{ mit } \textstyle\sum_{i=0}^m a_i q^{m-i}(q+1)^i \leq r\rangle.$$

Mit dem Satz von *Weierstraß* folgen dann die entgegengesetzten Inklusionen aus

$$\#(\mathbb{N}\backslash\mathbb{H}_m) = g_m,$$

was wir in Lemma 20.7 nachweisen werden. □

Lemma 20.6. *Für $l \in \mathbb{N}$ bezeichne wie in Satz 20.5*

$$\mathbb{H}_l := \left\{ \sum_{i=0}^{l} a_i q^{m-i}(q+1)^i : a_i \in \mathbb{N} \right\}.$$

Desweiteren sei $m \in \mathbb{N}$ eine natürliche Zahl. Dann ist jede ganze Zahl $l \in \mathbb{Z}$ eindeutig darstellbar als $l = uq + v(q+1)^m$ mit $u, v \in \mathbb{Z}$ und $0 \leq v < q$. Für $m \geq 1$ gilt zusätzlich: Es ist l genau dann Element der Halbgruppe $\mathbb{H}_m$, wenn u Element von $\mathbb{H}_{m-1}$ ist.

Beweis. Die erste Aussage ist klar, da mit v auch $v(q+1)^m \equiv v \pmod q$ alle Restklassen modulo q durchläuft. Im folgenden sei nun $m \geq 1$. Ist $l = uq + v(q+1)^m$ mit $0 \leq v < q$ ein Element von $\mathbb{H}_m$, so gibt es natürliche Zahlen $a_0, \ldots, a_m \in \mathbb{N}$ mit $l = \sum_{i=0}^m a_i q^{m-i}(q+1)^i$. Den Koeffizienten a_m schreiben wir als $a_m = aq + b$ mit $a, b \in \mathbb{N}$ und $0 \leq b < q$ und erhalten somit die Zerlegung

$$\begin{aligned} l &= \sum_{i=0}^{m-1} a_i q^{m-i}(q+1)^i + (aq+b)(q+1)^m \\ &= \left(\sum_{i=0}^{m-1} a_i q^{m-i-1}(q+1)^i + a(q+1)^m \right) q + b(q+1)^m. \end{aligned}$$

Wir haben oben bereits gezeigt, daß die Zerlegung dieser Art eindeutig ist und es folgt daher

$$u = \sum_{i=0}^{m-2} a_i q^{m-1-i}(q+1)^i + (a_{m-1} + a(q+1))(q+1)^{m-1} \in \mathbb{H}_{m-1}.$$

Ist umgekehrt u Element von $\mathbb{H}_{m-1}$, so gilt $u = \sum_{i=0}^{m-1} \tilde{a}_i q^{m-1-i}(q+1)^i$ mit Zahlen $\tilde{a}_0, \ldots, \tilde{a}_{m-1} \in \mathbb{N}$. Daher gilt dann

$$l = uq + v(q+1)^m = \sum_{i=0}^{m-1} \tilde{a}_i q^{m-i}(q+1)^i + v(q+1)^m \in \mathbb{H}_m.$$ □

Der Beweis zu Satz 20.5 schließt mit

Lemma 20.7. *Die Differenzmenge $\mathbb{N}\backslash\mathbb{H}_m$ enthält genau g_m Elemente.*

Beweis. Dieses Lemma beweisen wir per Induktion nach m. Im Fall $m = 1$ ist $\mathbb{H}_1 = \{a_0 q + a_1(q+1) : a_i \in \mathbb{N}\}$ und es gilt

$$\mathbb{N}\backslash\mathbb{H}_1 = \{1, \ldots, q-1, q+2, \ldots, 2q-1, 2q+3, \ldots, 3q-1, 3q+4, \ldots\}.$$

Somit enthält $\mathbb{N}\backslash\mathbb{H}_1$ genau $(q-1)+(q-2)+\cdots+1 = \frac{q(q-1)}{2}$ Elemente. Das Geschlecht des gewöhnlichen Spurturms F_1 der Stufe 1 ist nach Satz 20.3

$$g_1 = \frac{q-1}{2}\left((q+1)^2 - \frac{q^3-1}{q-1}\right) = \frac{q(q-1)}{2}$$

und stimmt daher mit $\#(\mathbb{N}\backslash\mathbb{H}_1)$ überein.
Es sei nun $m > 1$ und die Behauptung gelte für alle Zahlen $l \leq m-1$. Nach Lemma 20.6 läßt sich die Menge der natürlichen Zahlen disjunkt zerlegen in

$$\mathbb{N} = \{uq + v(q+1)^m : u \geq 0, 0 \leq v < q\} \dot\cup \{uq + v(q+1)^m : u < 0, 0 \leq v < q\}.$$

Wir bezeichnen die erste Menge der Zerlegung mit $\mathbb{N}_1$ und die zweite mit $\mathbb{N}_2$. Nach Lemma 20.6 ist $\mathbb{N}_2 \cap \mathbb{H}_m = \emptyset$, denn aus $uq + v(q+1)^m \in \mathbb{N}_2 \cap \mathbb{H}_m$ folgte $u < 0$ und $u \in \mathbb{H}_{m-1}$ im Widerspruch zur Definition von $\mathbb{H}_{m-1}$. Es gilt also

$$\#(\mathbb{N}\backslash\mathbb{H}_m) = \#(\mathbb{N}_1\backslash\mathbb{H}_m) + \#\mathbb{N}_2.$$

Wir bestimmen zunächst die Kardinalität von $\mathbb{N}_1\backslash\mathbb{H}_m$. Nach Lemma 20.6 ist $uq + v(q+1)^m$ genau dann Element von $\mathbb{N}_1\backslash\mathbb{H}_m$, wenn $u \in \mathbb{H}_{m-1}$ gilt. Also induziert jedes $u \in \mathbb{H}_{m-1}$ wegen $0 \leq v < q$ genau q Elemente der Form $uq + v(q+1)^m$ in $\mathbb{H}_m$. Nach der Induktionsvoraussetzung gilt daher

$$\#(\mathbb{N}_1\backslash\mathbb{H}_m) = q \cdot \#(\mathbb{N}\backslash\mathbb{H}_{m-1}) = q g_{m-1}.$$

Zur Bestimmung von $\#\mathbb{N}_2$ müssen wir nun alle Zahlen $uq + v(q+1)^m \geq 0$ mit $u < 0$ abzählen. Eine solche Zahl erfüllt

$$-uq \leq v(q+1)^m = v\left(1 + \sum_{i=1}^{m} \binom{m}{i} q^i\right).$$

Wegen $0 \leq v < q$ ist diese Ungleichung äquivalent zu

$$-u \leq v \sum_{i=1}^{m} \binom{m}{i} q^{i-1}.$$

Die Mächtigkeit der Menge $\mathbb{N}_2$ ist also

$$\begin{aligned}\#\mathbb{N}_2 &= \sum_{v=1}^{q-1} \# \left\{ u < 0 : -u \leq v \sum_{i=1}^{m} \binom{m}{i} q^{i-1} \right\} = \sum_{v=1}^{q-1} \left(v \sum_{i=1}^{m} \binom{m}{i} q^{i-1} \right) \\ &= \left(\sum_{v=1}^{q-1} v \right) \frac{1}{q} \sum_{i=1}^{m} \binom{m}{i} q^i = \frac{q-1}{2} \cdot ((q+1)^m - 1).\end{aligned}$$

Addieren wir schließlich $\#(\mathbb{N}_1 \backslash \mathbb{H}_m)$ und $\#\mathbb{N}_2$, so ergibt sich

$$\begin{aligned}\#(\mathbb{N}\backslash\mathbb{H}_m) &= q g_{m-1} + \frac{q-1}{2} \left((q+1)^m - 1 \right) \\ &= q \, \frac{q-1}{2} \left((q+1)^m - \frac{q^{m+1}-1}{q-1} \right) + \frac{q-1}{2} \left((q+1)^m - 1 \right) \\ &= \frac{q-1}{2} \left(q(q+1)^m + (q+1)^m - \frac{q(q^{m+1}-1)}{q-1} - \frac{q-1}{q-1} \right) \quad = \quad g_m,\end{aligned}$$

was zu zeigen war. □

Korollar 20.8. *Es seien F_m:$\mathbb{F}_q$ ein gewöhnlicher Spurturm, $\mathfrak{P}_\infty$ der Nennerprimteiler von x_0 in F_m und j eine natürliche Zahl mit*

$$r := q^{m-j}(q+1)^j < 2q^m.$$

Dann ist $1, x_0, \ldots, x_j$ eine $\mathbb{F}_q$−Basis von $\mathcal{L}(\mathfrak{P}_\infty^r)$.

Beweis. Da $\sum_{i=0}^{m} a_i q^{m-i}(q+1)^i \geq 2q^m$ für $\sum_{i=0}^{m} a_i \geq 2$ gilt, folgt nach Satz 20.5 $\mathcal{L}(\mathfrak{P}_\infty^r) \leq \mathbb{F}_q\langle x_0, \ldots, x_m \rangle$. Wegen $(q+1)^i q^{m-i} > (q+1)^j q^{m-j} = r$ für $i > j$ sind $x_{j+1}, \ldots, x_m$ nicht in $\mathcal{L}(\mathfrak{P}_\infty^r)$ enthalten. Hieraus folgt die Behauptung, da Funktionen mit paarweise verschiedener Polordnung bei $\mathfrak{P}_\infty$ über $\mathbb{F}_q$ linear unabhängig sind. □

20.3 Darstellung linearer Codes als arithmetische Codes

Bemerkung 20.9. *Zu jedem linearen Code C über $\mathbb{F}_q$ mit $(1, \ldots, 1) \in C$ gibt es eine Potenz $\tilde{q}$ von q und einen arithmetischen Code $\tilde{C}$ über $\mathbb{F}_{\tilde{q}}$ mit $C = \tilde{C}|_{\mathbb{F}_q}$.*

Beweis. Es sei C ein linearer $[n,k]_q$−Code mit $(1, \ldots, 1) \in C$. Dann besitzt C eine Erzeugermatrix der Gestalt

$$G = \begin{pmatrix} 1 & \cdots & 1 \\ g_{21} & \cdots & g_{2n} \\ \vdots & \ddots & \vdots \\ g_{k1} & \cdots & g_{kn} \end{pmatrix}.$$

Jede Spalte von G definiert einen Vektor

$$\boldsymbol{g}_j := (g_{2j}, \ldots, g_{kj}) \in \mathbb{F}_q^{k-1}.$$

Es sei s die maximale Anzahl gleicher Vektoren aus $\{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_n\}$ und es bezeichne $m := \lfloor k + \log_q(s) \rfloor$. Diese Zahlen erfüllen die Ungleichung $q^{m+1} \geq q^k \cdot s$ beziehungsweise $s \leq q^{m-(k-1)}$. Wir können also für $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_n$ paarweise verschiedene Urbilder unter der Projektion

$$\pi_{k-1}^m : \begin{cases} \mathbb{F}_q^m & \longrightarrow\!\!\!\!\!\rightarrow \quad \mathbb{F}_q^{k-1} \\ (a_1, \ldots, a_m) & \longmapsto \quad (a_1, \ldots, a_{k-1}) \end{cases}$$

finden, d.h. es gibt paarweise verschiedene Vektoren $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n \in \mathbb{F}_q^m$ mit

$$\pi_{k-1}^m(\boldsymbol{a}_j) = \boldsymbol{g}_j \qquad \text{für } j = 1, \ldots, n.$$

Für eine hinreichend große Potenz $\tilde{q}$ von q gilt $r := \tilde{q}^{\,m-k+1}(\tilde{q}+1)^{k-2} < 2\tilde{q}^{\,m-1}$. Der gewöhnliche Spurturm $F := F_{m-1}$ über $\mathbb{F}_{\tilde{q}}$ besitzt nach Korollar 20.4 für $j = 1, \ldots, n$ jeweils genau eine rationale Stelle $\mathfrak{P}_j$ mit

$$(x_0(\mathfrak{P}_j), \ldots, x_{m-1}(\mathfrak{P}_j)) = \boldsymbol{a}_j \in \mathbb{F}_q^m.$$

Wir betrachten nun den arithmetischen Code $C(\mathfrak{A}, \mathfrak{G})$ über F definiert durch

$$\mathfrak{A} := \mathfrak{P}_1 \cdots \mathfrak{P}_n \qquad \text{und} \qquad \mathfrak{G} := \mathfrak{P}_\infty^r.$$

Nach Korollar 20.8 ist $1, x_0, \ldots, x_{k-2}$ eine Basis von $\mathcal{L}(\mathfrak{G})$. Somit hat $C(\mathfrak{A}, \mathfrak{G})$ die Erzeugermatrix

$$\begin{pmatrix} 1 & \cdots & 1 \\ x_0(\mathfrak{P}_1) & \cdots & x_0(\mathfrak{P}_n) \\ \vdots & \ddots & \vdots \\ x_{k-2}(\mathfrak{P}_1) & \cdots & x_{k-2}(\mathfrak{P}_n) \end{pmatrix}.$$

Konstruktionsgemäß ist diese Matrix identisch zu G. Also stimmt der Code C mit dem arithmetischen Teilkörpercode $C(\mathfrak{A}, \mathfrak{G})|_{\mathbb{F}_q}$ überein. Hieraus folgt unsere Behauptung. □

Satz 20.10. *Jeder lineare Code kann als Teilkörpercode eines arithmetischen Codes gewonnen werden.*

Beweis. Es seien C ein linearer Code der Länge n und $\hat{C}$ der durch ein Paritätsbit erweiterte Code der Länge $n+1$ von C (vgl. Bemerkung 4.1). Dann verschwindet für alle Codewörter aus $\hat{C}$ die Quersumme ihrer Einträge, d.h. es gilt $\langle (1, \ldots, 1), \boldsymbol{x} \rangle = 0$ für $\boldsymbol{x} \in \hat{C}$. Somit besitzt der zu $\hat{C}$ duale Code $\hat{C}^\perp$ das Wort $(1, \ldots, 1)$. Nach Bemerkung 20.9 ist daher $\hat{C}^\perp$ nach Erweiterung des Konstantenkörpers $\mathbb{F}_q$ nach $\mathbb{F}_{\tilde{q}}$ ein arithmetischer Code. Da die Klasse arithmetischer Codes abgeschlossen ist bezüglich Dualisierung, ist auch $\hat{C}$ arithmetisch. Durch geeignetes Punktieren von $\hat{C}$ erhält einen Code $\tilde{C}$ mit $\tilde{C}|_{\mathbb{F}_q} = C$ (vgl. Bemerkung 4.2). Da aber das Punktieren lediglich der Ersetzung des Auswertungsdivisor $\mathfrak{A}$ von $\hat{C}$ durch $\mathfrak{P}^{-1}\mathfrak{A}$ mit $\mathfrak{P}|\mathfrak{A}$ entspricht, ist auch $\tilde{C}$ ein arithmetischer Code und es gilt schließlich $C = \tilde{C}|_{\mathbb{F}_q}$. □

Anmerkung 20.11. Codes über $\mathbb{F}_q$, die man durch Einschränkung arithmetischer Codes über $\mathbb{F}_{\tilde{q}}$ (vgl. Kapitel 16) erhält, gehören zu den sogenannten *verallgemeinerten arithmetischen Codes* über $\mathbb{F}_q$. Bei diesen ist zugelassen, daß der Auswertungsdivisor $\mathfrak{A}$ Primteiler $\mathfrak{P}$ vom Grad $\deg(\mathfrak{P}) > 1$ besitzt (siehe [OS99]).

20.4 Standardcodes im gewöhnlichen Spurturm

In diesem Abschnitt untersuchen wir Standardcodes über dem gewöhnlichen Spurturm F_m. Diese sind unter anderem deswegen interessant, weil ihr Singletondefekt nur einen Bruchteil des Geschlechts g_m beträgt. Desweiteren vergleichen wir die Parameter dieser Standardcodes mit denen der korrespondierenden Hermiteschen Standardcodes (Kapitel 17).

Definition 20.12. (Standardcode im gewöhnlichen Spurturm)
Es seien F_m ein gewöhnlicher Spurturm über $\mathbb{F}_q$ und $\mathfrak{P}_\infty$ der Nennerprimteiler von x_0 sowie $n := q^{m+1}$. Desweiteren sei $\mathfrak{A} := \prod_{i=1}^{n} \mathfrak{P}_i$ das Produkt der von $\mathfrak{P}_\infty$ verschiedenen rationalen Stellen in F_m. Dann heißen die Codes

$$C_r := C(\mathfrak{A}, \mathfrak{P}_\infty^r)$$

Standardcodes in F_m.

Bemerkung 20.13. (Dimension und Erzeugermatrix von Standardcodes in F_m)
Es seien C_r ein Standardcode in F_m und

$$B_r := \left\{ x_0^{a_0} \cdots x_m^{a_m} : 0 \le a_i < q, \sum_{i=0}^{m} a_i q^{m-i} (q+1)^i \le r \right\}.$$

Dann bildet

$$G_r := (x(\mathfrak{P}_1), \ldots, x(\mathfrak{P}_n))_{x \in B_r}$$

eine Erzeugermatrix von C_r. Insbesondere ist die Dimension des Codes C_r durch die Elementanzahl

$$k_r := \# \left\{ (a_0, \ldots, a_m) : 0 \le a_i < q, \sum_{i=0}^{m} a_i q^{m-i} (q+1)^i \le r \right\}$$

von B_r gegeben.

Beweis. Nach Satz 20.5 wird $\mathcal{L}(\mathfrak{P}_\infty^r)$ von den Funktionen der Gestalt $x_0^{a_0} \cdots x_m^{a_m}$ mit

$$\mathrm{ord}_{\mathfrak{P}_\infty}(x_0^{a_0} \cdots x_m^{a_m}) = -\sum_{i=0}^{m} a_i q^{m-i} (q+1)^i \ge -r$$

erzeugt. Da jeder Primteiler $\mathfrak{P}$ des Auswertungsdivisors $\mathfrak{A}$ eine Nullstelle von $x_i^q - x_i$ für alle $i = 0, \ldots, m$ bildet, gilt insbesondere $x_i^{q+a_i} \equiv x_i^{a_i} \pmod{\mathfrak{P}}$ und daher wird C_r schon von den Funktionen aus B_r erzeugt, d.h. es ist

$$C_r = \mathbb{F}_q\langle \boldsymbol{x} : x \in B_r \rangle.$$

Es bleibt also lediglich die lineare Unabhängigkeit der Elemente aus B_r über $\mathbb{F}_q$ zu zeigen. Setzt man

$$s := -\operatorname{ord}_{\mathfrak{P}_\infty}\left(\prod_{i=0}^{m} x_i^{q-1}\right) = (q-1)\sum_{i=0}^{m} q^{m-i}(q+1)^i,$$

so gilt $k_{\tilde{r}} = q^{m+1} = n$ für $\tilde{r} \geq s$. Nach dem *starken Approximationssatz* gibt es für $j = 1, \ldots, n$ Funktionen $y_j \in \cup_{r\in\mathbb{N}}\mathcal{L}(\mathfrak{P}_\infty^r)$ mit

$$y_j(\mathfrak{P}_j) \neq 0 \qquad \text{und} \qquad y_j(\mathfrak{P}_i) = 0 \qquad \text{für } j \neq i \in \{1, \ldots, n\}.$$

Für $\tilde{r} \geq \max\{s, -\operatorname{ord}_{\mathfrak{P}_\infty}(y_1), \ldots, -\operatorname{ord}_{\mathfrak{P}_\infty}(y_n)\}$ besitzt demnach der Code $C_{\tilde{r}}$ die Dimension n. Das zeigt die lineare Unabhängigkeit der Funktionen aus B_r. □

Satz 20.14. *Die Klasse der Standardcodes in einem gewöhnlichen Spurturm F_m ist abgeschlossen bezüglich Dualisierung. Genauer gilt für den Code C_r*

$$C_r^\perp = C_{s-r-1}$$

mit $s = -\operatorname{ord}_{\mathfrak{P}_\infty}\left(\prod_{i=0}^{m} x_i^{q-1}\right) = (q-1)((q+1)^{m+1} - q^{m+1})$.

Beweis. Das Differential $\delta = z^{-1}dz$ mit $z := x_0^q - x_0 = \prod_{a\in\mathbb{F}_q}(x_0 - a)$ besitzt nach Korollar 20.4 und der *Differentialdivisorformel* den Divisor

$$(\delta) = (z^{-1}) \cdot (dz) = \mathfrak{P}_\infty^n \mathfrak{A}^{-1} \cdot \mathfrak{D}(F_m{:}F_0)(z)_\infty^2 = \mathfrak{A}^{-1}\mathfrak{P}_\infty^{2g_m-2+n}.$$

Folglich ist δ ein Differential in F_m mit Ordnung -1 und dem Residuum 1 an den Stellen $\mathfrak{P}|\mathfrak{A}$. Nach Satz 11.12 ist dann C_r dual zum arithmetischen Code $C(\mathfrak{A}, \mathfrak{G}^*)$ mit Goppadivisor

$$\mathfrak{G}^* = (\delta)\mathfrak{A}\mathfrak{G}^{-1} = \mathfrak{P}_\infty^{2g_m-2+n-r}.$$

Aus

$$2g_m - 2 + n - r = (q-1)(q+1)^{m+1} - q^{m+2} + q^{m+1} - r - 1 = s - r - 1$$

ergibt sich $C_r^\perp = C^*(\mathfrak{A}, \mathfrak{G}^*) = C_{s-r-1}$. □

Satz 20.15. (Distanz der Standardcodes in F_m)
Es seien C_r ein Standardcode in F_m und k, l ganze Zahlen mit $0 \leq k \leq m$, $1 \leq l < q$ und

$$-\operatorname{ord}_{\mathfrak{P}_\infty}(x_0^{q-1}\cdots x_{k-1}^{q-1}x_k^{l-1}) \leq r < -\operatorname{ord}_{\mathfrak{P}_\infty}(x_0^{q-1}\cdots x_{k-1}^{q-1}x_k^{l}).$$

Dann besitzt C_r die Minimaldistanz

$$d_r = (q - l + 1)q^{m-k}$$

und den Singletondefekt $n - k_r + 1 - (q - l + 1)q^{m-k}$.

Beweis. Es sei $\mathbb{F}_q = \{w_1, \ldots, w_q\}$ mit $w_q = 0$. Wir betrachten zunächst die Funktion

$$y_{kl} := (x_0^{q-1} - 1) \cdots (x_{k-1}^{q-1} - 1)(x_k - w_1) \cdots (x_k - w_{l-1})$$

aus $\mathcal{L}(\mathfrak{P}_\infty^r)$. Unter Verwendung der Bijektion α aus Korollar 20.4 gilt

$$(x_0^{q-1} - 1)_0 = \prod_{a_0 \neq 0} \alpha^{-1}(a_0, \ldots, a_m), \quad (x_1^{q-1} - 1)_0 = \prod_{\substack{a_0 = 0 \\ a_1 \neq 0}} \alpha^{-1}(a_0, \ldots, a_m)$$

und allgemein

$$(x_i^{q-1} - 1)_0 = \prod_{\substack{a_0 = \ldots = a_{i-1} = 0 \\ a_i \neq 0}} \alpha^{-1}(a_0, \ldots, a_m).$$

Die Funktion y_{kl} verschwindet also in genau

$$(q-1)(q^m + q^{m-1} + \cdots + q^{m-k+1}) + (l-1)q^{m-k} = q^{m+1} - (q-l+1)q^{m-k}$$

rationalen Stellen aus F_m und das zugehörige Codewort $\boldsymbol{y_{kl}}$ besitzt Hamming - Gewicht $w(\boldsymbol{y_{kl}}) = n - (q^{m+1} - (q-l+1)q^{m-k}) = (q-l+1)q^{m-k}$. Wir erhalten somit die Ungleichung

$$d_r \leq (q-l+1)q^{m-k}.$$

Nun sei $t := (q-l+1)q^{m-k}$. Für den Nachweis der umgekehrten Ungleichung reicht es nach Bemerkung 2.16 zu zeigen, daß jeweils $t-1$ Spalten der Kontrollmatrix zu C_r linear unabhängig sind. Dazu nehmen wir zunächst an, daß r einen der Werte

$$r = -\operatorname{ord}_{\mathfrak{P}_\infty}(x_0^{q-1} \cdots x_{k-1}^{q-1} x_k^l) - 1 = s + \operatorname{ord}_{\mathfrak{P}_\infty}(x_m^{q-1} \cdots x_{k+1}^{q-1} x_k^{q-l-1}) - 1$$

für $0 \leq k \leq m$ und $1 \leq l \leq q-1$ annimmt. Die Ungleichung für allgemeine $\tilde{r}$ mit $\tilde{r} \leq r$ folgt dann aus $d_{\tilde{r}} \geq d_r$.
Die Kontrollmatrix zu C_r wird nach Satz 20.14 erzeugt von allen Funktionen aus

$$B_{s-r-1} = \left\{ x_0^{a_0} \cdots x_m^{a_m} : 0 \leq a_i < q, \sum_{i=0}^{m} a_i q^{m-i}(q+1)^i \leq s - r - 1 \right\}.$$

Wir betrachten die Teilmenge

$$\tilde{B} := \left\{ x_0^{a_0} \cdots x_m^{a_m} : 0 \leq a_i < q, \sum_{i=0}^{m} a_i \leq (m-k)(q-1) + t \right\}$$

und die hiervon erzeugte Matrix

$$A := \left(\prod_{i=0}^{m} x_i(\mathfrak{P}_1)^{a_i}, \ldots, \prod_{i=0}^{m} x_i(\mathfrak{P}_n)^{a_i} \right)_{\prod_{i=0}^{m} x_i^{a_i} \in \tilde{B}}.$$

Für unsere Behauptung genügt es zu zeigen, daß je $t-1$ Spalten von A linear unabhängig sind. Im Spezialfall $m = 0$ ergibt sich dies einfach daraus, daß A aus $t-1$ Zeilen einer Vandermondeschen Matrix besteht. Der allgemeine Fall kann schließlich durch Induktion nach m auf den Fall $m = 0$ zu geführt werden. Damit schließt der Beweis. □

Korollar 20.16. (Vergleich mit Hermiteschen Standardcodes)
Es seien

$$F = \mathbb{F}_{q^2}(u,v) \qquad \textit{mit} \qquad v^q + v = u^{q+1}$$

ein Hermitescher Funktionenkörper und

$$F_1 = \mathbb{F}_{q^2}(x_0,x_1) \qquad \textit{mit} \qquad x_1^q - x_1 = x_0(x_0^q - x_0)$$

ein gewöhnlicher Spurturm der Höhe 1. *Dann gelten:*

(a) *Für* $2 \le d \le q$ *gibt es Hermitesche Standardcodes über* $F{:}\mathbb{F}_{q^2}$ *mit den Parametern* $[q^3, q^3 - \binom{d}{2}, d]_{q^2}$ *und Singletondefekt* $\binom{d-1}{2}$.

(b) *Für* $2 \le d \le q^2$ *gibt es Standardcodes im gewöhnlichen Spurturm* $F_1{:}\mathbb{F}_{q^2}$ *mit den Parametern* $[q^4, q^4 - \binom{d}{2}, d]_{q^2}$ *und Singletondefekt* $\binom{d-1}{2}$.

Insbesondere gibt es bei vorgebener Distanz $d \le q$ *Standardcodes in* F_1 *mit höherer Informationsrate als die der korrespondierenden Standardcodes über* F.

Beweis. Bei $2 \le d \le q$ haben Hermitesche Standardcodes C_t mit

$$(q+1)(q^2+q-d) \le t \le (q+1)(q^2+q-d)+q$$

nach Zusatz 17.14 Minimaldistanz d. Unter diesen Hermiteschen Codes besitzt C_r mit

$$r := (q+1)(q^2+q-d)+q = q^3+q^2-q-2-(d-2)(q+1)$$

die größte Dimension, nämlich (ebenfalls nach 17.14)

$$\dim(C_r) = q^3 - \#\{(i,j) : i,j \in \mathbb{N}, j < q, iq+j(q+1) \le (d-2)(q+1)\} = q^3 - \binom{d}{2}.$$

Das Pseudogeschlecht von C_r beträgt dann

$$q^3 - \dim(C_r) + 1 - d = \binom{d}{2} - (d-1) = \binom{d-1}{2}.$$

Standardcodes C_t in $F_1{:}\mathbb{F}_{q^2}$ mit vorgebener Distanz $d \le q^2$ erhalten wir nach Satz 20.15 für

$$-\operatorname{ord}_{\mathfrak{P}_\infty}(x_0^{q^2-1}x_1^{q^2-d}) = 2q^4 - dq^2 - d \le t < -\operatorname{ord}_{\mathfrak{P}_\infty}(x_0^{q^2-1}x_1^{q^2-d+1}) = 2q^4 - (d-1)(q^2+1).$$

Die maximale Dimension unter diesen Codes hat C_r mit

$$r := 2q^4 - (d-1)(q^2+1) - 1 = 2q^4 - q^2 - 2 - (d-2)(q^2+1),$$

nämlich (unter Verwendung von Satz 20.14)

$$\begin{aligned} k_r &= q^4 - k_{2q^4-q^2-2-r} = q^4 - k_{(d-2)(q^2+1)} \\ &= q^4 - \#\{(i,j) : 0 \le i,j \le q^2, iq^2 + j(q^2+1) \le (d-2)(q^2+1)\} = q^4 - \binom{d}{2}. \end{aligned}$$

Der Singletondefekt ergibt sich wie oben zu

$$q^4 - k_r + 1 - d = \binom{d-1}{2}.$$

Das Verhältnis der Informationsraten zwischen Standardcodes in F_1 und F bei gleicher Distanz d beträgt daher

$$1 - \frac{\binom{d}{2}}{q^4} \qquad \text{zu} \qquad 1 - \frac{\binom{d}{2}}{q^3}.$$

Das beweist unsere Behauptung. □

Anhang A

Sätze über algebraische Funktionenkörper

Für die Theorie der arithmetischen Codes benötigt man grundlegende Kenntnisse über algebraische Funktionkörper. Wir empfehlen das Buch *Algebraic Functions Fields and Codes* von *Henning Stichtenoth* [Sti93]. Ohne Anspruch auf Vollständigkeit sei hier eine kleine Sammlung von fundamentalen Aussagen, die im Skript durch kursive Schrift gekennzeichnet sind, zum schnellen Nachschlagen zusammengestellt.

A.1 Grundlagen und Satz von Riemann-Roch

Es sei stets $F{:}K$ ein algebraischer Funktionenkörper. Wir bezeichnen die Menge aller Primdivisoren von $F{:}K$ mit $\mathbb{P}_{F:K}$, die von den Primdivisoren erzeugte freie abelsche Gruppe mit $\mathbb{D}_{F:K}$ und es seien $\mathbf{H}_{F:K}$ die Klasse aller Hauptdivisoren und $\mathbf{W}_{F:K}$ die kanonische Klasse von $F{:}K$. Den Bewertungsring eines Primdivisors $\mathfrak{P}$ kennzeichnen wir mit $\mathcal{O}_{\mathfrak{P}}$. Der Grad $\deg(\mathfrak{P})$ eines Primdivisors ist der Körpergrad $[\mathcal{R}_{\mathfrak{P}}{:}K]$ des Restklassenkörpers $\mathcal{R}_{\mathfrak{P}} = \mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ über den Konstantenkörper K. Für einen Divisor $\mathfrak{A} \in \mathbb{D}_{F:K}$ bezeichne $\mathcal{L}(\mathfrak{A}) = \{z \in F : \mathrm{ord}_{\mathfrak{P}}(z) \geq -\mathrm{ord}_{\mathfrak{P}}(\mathfrak{A})\} \cup \{0\}$ den K-linearen Riemann-Roch-Raum von $\mathfrak{A}$ und wir defineren Grad und Dimension von $\mathfrak{A}$ durch

$$\deg(\mathfrak{A}) = \sum_{\mathfrak{P} \in \mathbb{P}_{F:K}} \mathrm{ord}_{\mathfrak{P}}(\mathfrak{A}) \deg(\mathfrak{P}) \qquad \text{und} \qquad \dim(\mathfrak{A}) = \dim_K(\mathcal{L}(\mathfrak{A})).$$

Das Geschlecht eines algebraischen Funktionenkörpers $F{:}K$ ist die natürliche Zahl $\max\{\deg(\mathfrak{A}) - \dim(\mathfrak{A}) + 1 : \mathfrak{A} \in \mathbb{D}_{F:K}\}$ und wird von uns mit $g_{F:K}$ oder - falls im Zusammenhang klar ist, welcher Funktionenkörper gemeint ist - auch kürzer mit g gekennzeichnet.

Satz von Riemann-Roch

Für die Dimension eines Divisor $\mathfrak{A} \in \mathbb{D}_{F:K}$ hat man stets die Abschätzungen

$$\deg(\mathfrak{A}) + 1 \geq \dim(\mathfrak{A}) \geq \deg(\mathfrak{A}) - g + 1.$$

Der Satz von Riemann-Roch besagt, daß $i(\mathfrak{A}) = \dim(\mathfrak{W}/\mathfrak{A})$ für den Spezialitätsindex $i(\mathfrak{A}) := \dim(\mathfrak{A}) - \deg(\mathfrak{A}) + g - 1$ und einen kanonischen Divisor $\mathfrak{W} \in \mathbf{W}_{F:K}$ gilt, d.h.

$$\dim(\mathfrak{A}) = \deg(\mathfrak{A}) + g - 1 + \dim(\mathfrak{W}/\mathfrak{A}). \qquad \text{[Sti93, I.5.15.]}$$

Desweiteren verschwindet der Spezialitätsindex für Divisoren mit Grad $\geq 2g - 1$, d.h. es gilt

$$\dim(\mathfrak{A}) = \deg(\mathfrak{A}) + g - 1 \qquad \text{falls } \deg(\mathfrak{A}) \geq 2g - 1.$$

Satz von Clifford

Für einen Divisor $\mathfrak{A} \in \mathbb{D}_{F:K}$ vom Grad $0 \leq \deg(\mathfrak{A}) \leq 2g - 2$ gilt

$$\dim(\mathfrak{A}) \leq 1 + \tfrac{1}{2} \deg(\mathfrak{A}). \qquad \text{[Sti93, I.6.11.]}$$

Desweiteren gilt für Divisoren $\mathfrak{A}, \mathfrak{B}$ mit Dimension > 0 die Abschätzung

$$\dim(\mathfrak{A}) + \dim(\mathfrak{B}) \leq 1 + \dim(\mathfrak{A}\mathfrak{B}).$$

Approximationssätze

Es seien $\mathfrak{P}_1, \ldots, \mathfrak{P}_n \in \mathbb{P}_{F:K}$ paarweise verschiedene Primdivisoren aus $F{:}K$, sowie $x_1, \ldots, x_n$ Funktionen aus F und $r_1, \ldots, r_n \in \mathbb{Z}$ ganze Zahlen. Dann gibt es nach dem schwachen Approximationssatz eine Funktion $x \in F$ mit

$$\mathrm{ord}_{\mathfrak{P}_i}(x - x_i) = r_i \qquad \text{für } i = 1, \ldots, n. \qquad \text{[Sti93, I.3.1.]}$$

Sei zudem $S \neq \mathbb{P}_{F:K}$ eine echte Untermenge der Primdivisoren in $F{:}K$ und es seien $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ aus S. Dann gibt es nach dem starken Approximationssatz eine Funktion $x \in F$ mit

$$\mathrm{ord}_{\mathfrak{P}_i}(x - x_i) = r_i \qquad (i = 1, \ldots, n),$$

und $$\mathrm{ord}_{\mathfrak{P}}(x) \geq 0 \quad \text{für alle } \mathfrak{P} \in S \backslash \{\mathfrak{P}_1, \ldots, \mathfrak{P}_n\} \qquad \text{[Sti93, I.6.4.]}$$

Rationale Stellen, Satz von Weierstraß

Ein Primdivisor vom Grad 1 nennen wir rationale Stelle und die Menge aller rationalen Stellen kennzeichnen wir mit $\mathbb{P}_{F:K}^{(1)}$. In rationalen Funktionenkörpern $K(t):K$ sind das genau die Null- und Polstellen der Linearfaktoren $x-a$ für $a \in K$. Es gelten

$$\mathbb{P}_{K(t):K}^{(1)} = \{(t-a)_0, (t)_\infty : a \in K\} \cong \mathbb{P}^{(1)}(K). \qquad \text{[Sti93, I.2.]}$$

Eine natürliche Zahl $n \geq 0$ nennen wir Polzahl einer rationalen Stelle $\mathfrak{P}$, falls $\mathfrak{P}^n$ der Polstellendivisor $(x)_\infty$ einer Funktion $x \in F$ ist, d.h. falls $(x)_\infty = \mathfrak{P}^n$ gilt. Andernfalls heißt n Fehlzahl. Rationale Funktionenkörper haben keine Fehlzahlen. Für Funktionenkörper vom Geschlecht $g > 0$ gilt nach dem Satz von Weierstraß : Es gibt genau g Fehlzahlen $n_1 < \ldots < n_g$ zu einer rationalen Stelle $\mathfrak{P}$ und es gilt dabei $n_1 = 1$ und $n_g \leq 2g-1$. [Sti93, I.6.7.]

A.2 Erweiterungen algebraischer Funktionenkörper

Einen algebraischer Funktionenkörper $E:K'$ wir eine algebraische Erweiterung von $F:K$, falls $E:F$ und $K':K$ algebraische Erweiterungen sind. Die Erweiterung $E:F$ heißt geometrisch, falls $E:F$ endlich separabel ist und $K' = K$ gilt. Für eine Divisorenerweiterung $\mathfrak{P}'|\mathfrak{P} = \mathfrak{P}' \cap F$ eines Primdivisors $\mathfrak{P} \in \mathbb{P}_{F:K}$ bezeichnen $e_{\mathfrak{P}'}(E:F)$ den Verzweigungs- und $f_{\mathfrak{P}'}(E:F)$ den Trägheitsheitsgrad. Bei galoischen Erweiterungen sind alle Divisorenerweiterung bezüglich der Galoisgruppe $\mathrm{Gal}(E:F)$ zueinander konjugiert und haben gleichen Verzweigungs- und Trägheitsgrad [Sti93, III.7.2.].

Differente

Die Differente $\mathfrak{D}(E:F)$ einer Erweiterung algebraischer Funktionenkörper ist das Produkt aller verzweigter Primdivisoren $\mathfrak{P}'$ mit Differentengrad $d_{\mathfrak{P}'}(E:F)$, d.h. es ist

$$\mathfrak{D}(E:F) = \prod_{\mathfrak{P} \in \mathbb{P}_{F:K}} \prod_{\mathfrak{P}'|\mathfrak{P}} \mathfrak{P}'^{\, d_{\mathfrak{P}'}(E:F)}$$

Nach dem Dedekindschen Differentensatz gilt für jede Divisorenerweiterung $\mathfrak{P}'|\mathfrak{P}$

$$d_{\mathfrak{P}'}(E:F) \geq e_{\mathfrak{P}'}(E:F) - 1$$

und $\quad d_{\mathfrak{P}'}(E:F) = e_{\mathfrak{P}'}(E:F) - 1 \Leftrightarrow \mathrm{char}(K)$ teilt nicht $e_{\mathfrak{P}'}(E:F)$ [Sti93, III.5.1.]

Ist $E:F$ eine Galoiserweiterung mit Galoisgruppe G, so läßt sich der Differentenexponent $d_{\mathfrak{P}'}(E:F)$ einer (und damit aller Erweiterungen) von $\mathfrak{P}$ mit Hilfe der i-ten Verzweigungsgruppen $G_i(\mathfrak{P}') = \{\sigma \in G : \mathrm{ord}_{\mathfrak{P}'}(\sigma t - t) \geq i+1, \mathrm{ord}_{\mathfrak{P}'}(t) = 1\}$ berechnen. Diese bilden eine absteigende und stationäre Kette von Normalteilern in G_{-1}. Die Hilbertsche Differentenformel besagt

$$d_{\mathfrak{P}'}(E:F) = \sum_{i=0}^{\infty} (\#G_i(\mathfrak{P}') - 1) \qquad \text{[Sti93, III.8.8.]}$$

Relativgeschlechtformel von Hurwitz

Für eine endlich separable Erweiterung $E{:}F$ von algebraischen Funktionenkörpern mit Konstantenkörpern K' bzw. K gilt folgende Relation zwischen $g_{F:K}$ und $g_{E:K'}$:

$$(2g_{E:K'} - 2) = \tfrac{[E:F]}{[K':K]}(2g_{F:K} - 2) + \deg(\mathfrak{D}(E{:}F)). \qquad \text{[Sti93, III.4.12.]}$$

Differentialdivisorformel

Ein Differential der Gestalt $\delta = z\,dx \neq 0$ hat den kanonischen Divisor

$$(z\,dx) = (z)(dx) = (z)(x)_\infty^{-2}\mathfrak{D}(F{:}K(x)). \qquad \text{[Sti93, IV.3.7.]}$$

Dedekind-Kriterium

Es seien $E{:}F$ eine galoissche Erweiterung algebraischer Funktionenkörper vom Grad n mit primitivem Element y und $\mathfrak{P} \in \mathbb{P}_{F:K}$ eine Primstelle zu $F{:}K$. Desweiteren sei y ganz über $\mathfrak{P}$ und das Minimalpolynom $g(T) \in \mathcal{O}_\mathfrak{P}[T]$ von y zerfalle bei der Reduktion modulo $\mathfrak{P}$ in r paarweise verschiedene Primpolynome, d.h. es gelte

$$\overline{g}(T) = \prod_{i=1}^{r} \overline{g}_i(T) \in (\mathcal{O}_\mathfrak{P}/\mathfrak{P})[T]$$

mit paarweise verschiedenen Primpolynomen $g_i(T) \in \mathcal{O}_\mathfrak{P}[T]$. Dann zerfällt $\mathfrak{P}$ in $E{:}F$ in r unverzweigte Fortsetzungen mit Trägheitsgrad $f = \deg(g_i(T))$ und die Fortsetzungen $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ sind eindeutig bestimmt durch $g_i(y) \in \mathfrak{P}_i$. [Sti93, III.3.7.]

Konstantenerweiterungen

Für eine algebraische Erweiterung $K'{:}K$ heißt das Kompositum $E = FK'$ eine Konstantenerweiterung von F. Es bezeichne $\deg_F(\mathfrak{A})$ den Divisorgrad in $F{:}K$ und $\deg_E(\mathfrak{A})$ den Divisorgrad der kanonischen Einbettung $\mathfrak{A}^\varepsilon$ in $\mathbb{D}_{E:K'}$. Analog gelten die Bezeichnungen für die Dimensionen $\dim_F(\mathfrak{A})$ und $\dim_E(\mathfrak{A})$. Es gelten dann:

(a) Die Erweiterung $E{:}F$ ist unverzweigt, d.h. die Differente $\mathfrak{D}(E{:}F)$ hat Grad 0.

(b) $E{:}K'$ hat das gleiche Geschlecht wie $F{:}K$.

(c) Ein Primdivisor $\mathfrak{P} \in \mathbb{P}_{F:K}$ zerlegt sich in E in das Produkt

$$\mathfrak{P}^\varepsilon = \prod_{i=1}^{r} \tilde{\mathfrak{P}}_i \qquad \text{mit } \deg(\tilde{\mathfrak{P}}_i) = \frac{\deg_F(\mathfrak{P})}{r},$$

wobei r den größten gemeinsamen Teiler von $\deg_F(\mathfrak{P})$ und $[K'{:}K]$ bezeichne.

(d) Für $\mathfrak{A} \in \mathbb{D}_{F:K}$ gelten $\deg_E(\mathfrak{A}) = \deg_F(\mathfrak{A})$ und $\dim_E(\mathfrak{A}) = \dim_F(\mathfrak{A})$.

[Sti93, III.6.,V.1.9.]

Kummererweiterungen

Die natürliche Zahl $n > 1$ sei prim zur Charakteristik von K und K enthalte die primitiven n-ten Einheitswurzel. Desweiteren seien $u \in F$ mit $u \neq v^d$ für alle Funktionen $v \neq u$ aus F und alle Teiler $d|n$. Dann heißt die Erweiterung $E = F(z)$ mit $z^n = u$ Kummererweiterung von F und es gelten:

(a) Das Polynom $T^n - u$ ist irreduzibel über F und $E{:}F$ ist galoissch vom Grad n. Die Galoisgruppe $\mathrm{Gal}(E{:}F)$ ist zyklisch und wird erzeugt von den Automorphismen $z \mapsto wz$, wobei w eine n-te Einheitswurzel aus K ist.

(b) Es sei $\mathfrak{P}'$ eine Erweiterung einer Primstelle $\mathfrak{P} \in \mathbb{P}_{F:K}$. Dann gelten

$$e_{\mathfrak{P}'}(E{:}F) = \frac{n}{r_{\mathfrak{P}}} \qquad \text{und} \qquad d_{\mathfrak{P}'}(E{:}F) = \frac{n}{r_{\mathfrak{P}}} - 1,$$

wobei $r_{\mathfrak{P}} := (n, \mathrm{ord}_{\mathfrak{P}}(u)) \in \mathbb{N}$ den größten gemeinsamen Teiler von n und $\mathrm{ord}_{\mathfrak{P}}(u)$ bezeichne.

(c) Nach der Relativgeschlechtformel von Hurwitz gilt dann

$$g_{E:K'} = 1 + \frac{n}{[K'{:}K]} \left(g_{F:K} - 1 + \frac{1}{2} \sum_{\mathfrak{P} \in \mathbb{P}_{F:K}} \left(1 - \frac{r_{\mathfrak{P}}}{n}\right) \deg(\mathfrak{P}) \right).$$

Es ist $E{:}F$ genau dann geometrisch, wenn mindestens eine Primstelle $\mathfrak{P} \in \mathbb{P}_{F:K}$ total verzweigt bzw. falls $r_{\mathfrak{P}} = 1$ für mindestens ein $\mathfrak{P} \in \mathbb{P}_{F:K}$ gilt. In diesen Fall gilt

$$g_{E:K} = 1 + n(g_{F:K} - 1) + \tfrac{1}{2} \sum_{\mathfrak{P} \in \mathbb{P}_{F:K}} (n - r_{\mathfrak{P}}) \deg(\mathfrak{P}). \qquad \text{[Sti93, III.7.3.]}$$

A.3 Kongruenzfunktionenkörper

Für die Anwendung in der Codierungstheorie beschränkt man sich auf algebraische Funktionenkörper mit endlichem Konstantenkörper, sogenannte Kongruenzfunktionenkörper. Wichtige Invarianten sind neben dem Geschlecht g die (endliche) Klassenzahl h, die Anzahl rationaler Stellen $\#\mathbb{P}^{(1)}_{F:\mathbb{F}_q}$ und die Weilzahlen ω_i bzw. das L-Polynom.

L-Polynom, Satz von Hasse-Weil

Die Zetafunktion eines Kongruenzfunktionenkörpers $F{:}\mathbb{F}_q$ ist die Potenzreihe $Z(t) = \sum_{n=0}^{\infty} A_n t^n$, wobei A_n die Anzahl ganzer Divisoren vom Grad n bezeichne. Das L-Polynom von $F{:}\mathbb{F}_q$ ist das ganzzahlige Polynom $L(t) = (1-t)(1-qt)Z(t)$ vom Grad $2g$. Die Koeffizienten $a_0, \ldots, a_{2g}$ erfüllen

$$a_0 = 1, \quad a_1 = \#\mathbb{P}^{(1)}_{F:\mathbb{F}_q} - (q+1), \quad a_{2g-i} = q^{g-i} a_i \quad (0 \leq i \leq g).$$

Die Klassenzahl h ist Elementanzahl der Divisorenklassen $[\mathfrak{A}]$ vom Grad 0 und wird als Wert des L-Polynoms $L(1) = h$ angenommen. Das L-Polynom ist über den Ring der ganzen algebraischen Zahlen zerlegt in

$$L(t) = \sum_{i=0}^{2g} a_i t^i = \prod_{i=1}^{2g} (1 - \omega_i t).$$

Das L-Polynom des unter einer Konstantenerweiterung vom Grad r gewonnenen Kongruenzfunktionenkörpers $F{:}\mathbb{F}_{q^r}$ hat die Gestalt

$$L_{F:\mathbb{F}_{q^r}}(t) = \prod_{i=1}^{2g} (1 - \omega_i^r t).$$

Die Kehrbrüche ω_i der Nullstellen des L-Polynoms heißen Weilzahlen und können derart sortiert werden, daß $\omega_i \omega_{g+i} = q$ für $0 \leq i \leq g$ gilt. Für ihren Betrag gilt nach dem Satz von Hasse-Weil

$$|\omega_i| = \sqrt{q} \qquad \text{für } i = 1, \ldots, 2g. \qquad \text{[Sti93, V.1.15., V.2.1.]}$$

Schranke von Hasse-Weil

Die Anzahl rationaler Stellen $\#\mathbb{P}^{(1)}_{F:\mathbb{F}_q}$ eines Kongruenzfunktionenkörpers $F{:}\mathbb{F}_q$ vom Geschlecht g ist beschränkt durch

$$|\#\mathbb{P}^{(1)}_{F:\mathbb{F}_q} - (q+1)| \leq 2g\sqrt{q} \qquad \text{[Sti93, V.2.3.]}$$

Beweis. Diese Schranke folgt direkt aus dem Satz von Hasse-Weil durch Abschätzen von $\#\mathbb{P}^{(1)}_{F:\mathbb{F}_q} - (q+1) = a_1 = -\sum_{i=1}^{2g} \omega_i$. □

Satz von F.K. Schmidt

Der kleinste positive Divisorgrad eines Kongruenzfunktionenkörper ist 1.

[Sti93, V.1.11.]

Index

Literaturverzeichnis

[Bie06] Daniel Bierbrauer. Codes auf hyperellitptischen und trigonalen Kurven. *Diplomarbeit an der Universität Heidelberg*, 2006.

[DS89] Y. Driencourt and H. Stichtenoth. A criterion for self-duality of codes. *Commun. Algebra*, 17:885–898, 1989.

[Gop02] V.D. Goppa. *Geometry and Codes*. Springer Netherlands, 2002.

[GS96] Arnoldo Garcia and Henning Stichtenoth. On the behaviour of some towers of functions fields over finite fields. *J. Number Theory*, 61:248–273, 1996.

[HP03] W.C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. Cambridge, 2003.

[Hup67] Bertram Huppert. *Endliche Gruppen I*. Springer Verlag, 1967.

[Kre02] Ulrich Krengel. *Einführung in die Wahrscheinlichkeitstheorie und Statistik*. Vieweg Studium Verlag, 6. edition, 2002.

[KS80] Knapp and Schmid. Codes with pescribed permutation group. *J. Algebra*, 67:415–435, 1980.

[KW90] Knörr and Willems. The automorphism groups of generalized reed-muller codes. *Astérique*, 181/182:195 – 207, 1990.

[KY91] P.V. Kumar and K. Yang. On the true distance of hermitian codes. *Coding theory and algebraic geometry (Luminy), Lect. Notes in Math. 1518, Springer*, pages 99–107, 1991.

[Lag06] Thorsten Lagemann. Codes und Automorphismen optimaler Artin-Schreier-Türme. *Diplomarbeit an der Universität Heidelberg*, 2006.

[Lan02] Serge Lang. *Algebra*. Springer Verlag, revised third edition, 2002.

[Leo96] H.-W. Leopoldt. Über die Automorphismengruppe des Fermatkörpers. *J. Number Theory*, 56:156–282, 1996.

[Lin99] J.H. van Lint. *Introduction to Coding Theory.* Springer Verlag, 1999.

[Lü89] Lüneburg. Transitive Erweiterungen endlicher Permutationsgruppen. *SLN84*, 1989.

[Lü03] Werner Lütkebohmert. *Codierungstheorie.* Vieweg Studium Verlag, 1. edition, 2003.

[Mat92] B.Heinrich Matzat. Kanonische Codes auf einigen Überdeckungskurven. *Manuscripta Math.*, 77:321–335, 1992.

[MS77] MacWilliams, F.J. and Sloane, N.J.A. *The Theory of Error-Correcting Codes.* North-Holland, Amsterdam, 1977.

[Mum86] David Mumford. *Abelian Varieties.* OUP India, 1986.

[Mun92] Carlos Munuera. On the main conjecture on geometric mds codes. *IEEE Trans. Information Theory*, 38:1573–1577, 1992.

[OS99] F. Özbudak and H. Stichtenoth. Constructing codes from algebraic curves. *IEEE Trans. Information Theory*, 45:2502–2505, 1999.

[Pre96] Oliver Pretzel. *Error-Correcting Codes and Finite Fields.* Clarendon Press, Oxford, 1996.

[Pre98] Oliver Pretzel. *Codes and Algebraic Curves.* Clarendon Press, Oxford, 1998.

[RBG91] R.Pellikaan, B.-Z. Shen, and G.J.M. van Wee. Which linear codes ar algebraic-geometric? *IEEE Trans. Information Theory*, 37:583–662, 1991.

[Rei92] Stefan Reiter. Gewichtsverteilung hyperelliptischer Codes. *Diplomarbeit an der Universität Heidelberg*, 1992.

[Sch89] W. Scharlau. Selbstduale Goppa Codes. *Math.Nachrichten*, 143:119–122, 1989.

[Ste99] Serguei Stephanov. *Codes on Algebraic Curves.* Kluwer Academic / Plenum Publisher, 1999.

[Sti88] Henning Stichtenoth. Self-dual goppa codes. *J. Pure Appl. Algebra*, 55:199–211, 1988.

[Sti90] Henning Stichtenoth. On automorphisms of geometric goppa codes. *J. Algebra*, 130:113–121, 1990.

[Sti93] Henning Stichtenoth. *Algebraic Function Fields and Codes.* Springer Verlag, 1993.

[TV02] Tsfasman and Vladut. *Algebraic-geometric Codes*. Kluwer Academic Publishers, 2002.

[VS06] G.D. Villa Salvador. *Topics in the Theory of Algebraic Function Fields*. Birkhäuser Verlag, 2006.

[Wil99] Wolfgang Willems. *Codierungstheorie*. de Gruyter Verlag, 1999.

[Xin91] C. Xing. Hyperelliptic function fields and codes. *J. Pure Appl. Algebra*, 74:109–118, 1991.