Codierungstheorie

Vorlesung Sommersemester 2005

Prof. Dr. M. E. Pohst

Technische Universität Berlin
Institut für Mathematik
pohst@math.tu-berlin.de

II

Inhaltsverzeichnis

Einleitung

C. Shannon schrieb 1948 in seinem Artikel “A mathematical theory of communication”den bemerkenswerten Satz: “The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point.”
Dies war gewissermaßen die Geburtsstunde der “Coding Theory”.
Es folgt die Beschreibung der grundlegenden Ideen an Hand eines mathematischen Modells: Binärer symmetrischer Kanal (BSC).
Es werden zwei mögliche Symbole $0, 1$ gesendet und zwar mit der Übertragungsrate R Stück ($R \in \mathbb{R}^{\geq 0}$) pro Zeiteinheit. Das Senden von Nullen bzw. Einsen erfolgt zufallsmäßig. Es wird angenommen, dass der Output mit der Wahrscheinlichkeit $p \in \left[0, \frac{1}{2}\right]$ vom Input verschieden ist.
Problem Wie gut kann eine sendende Person mit einer empfangenden kommunizieren?
Kritik Der BSC ist im Allgemeinen ein idealisiertes Modell, zum Beispiel bei Satellitenübertragungen produziert ein Blitzeinschlag Fehler, die nicht unabhängig voneinander sind. Dasselbe gilt etwa für Kratzer auf einer CD oder DVD. Die Korrektur solcher “error bursts”wird später diskutiert.
Beispiele

1. $R = 1/3$, das heißt der Kanal überträgt 1 Bit dreimal so schnell, wie die Quelle es produziert. Dann kann man zum Beispiel jedes erzeugte Bit dreifach übermitteln. Dass heißt $1\ 0\ 1\ 0\ 0$ würde zunächst ”codiert” in $111\ 000\ 111\ 000\ 000$. Der Empfänger des “gestörten”Kanals würde aber vielleicht nur $101\ 011\ 111\ 001\ 100$ empfangen (Bits 2, 4, 5, 12, 13 fehlerhaft). Die naheliegende Strategie des “Decodierens”wäre dann, für jede Gruppe von 3 Bits dasjenige zu wählen, was mindestens doppelt auftritt. Ergebnis: $1\ 1\ 1\ 0\ 0$, fehlerhaft in Bit 2. Ein Fehler tritt stets dann auf, wenn zwei oder alle drei Kopien eines Quell-Bits falsch übertragen werden.
   P_f bezeichne die Fehlerwahrscheinlichkeit für die Übertragung eines Bit:

$$\begin{aligned} P_e &= P\{2 \text{ Übertragungsfehler}\} &&+P\{3 \text{ Übertragungsfehler}\} \\ &= 3p^2(1-p) &&+p^3 \\ &= 3p^2 - 2p^3 \\ &< p \text{ für } 0 < p < \tfrac{1}{2}. \end{aligned}$$

   Die Verbesserung ist dabei für kleines p nicht unbeträchtlich!

2. $R > 1$. Dann lassen sich nur $\frac{1}{R}$ der erzeugten Bits übertragen und der Empfänger muss den Rest raten. (Etwa mittels Werfen einer Münze). Hierfür ist dann

$$P_e = \frac{1}{R}p + \frac{R-1}{R} \cdot \frac{1}{2} = \frac{1}{2} - \left(\frac{1}{2} - p\right)/R.$$

Das heißt, im Allgemeinen ist dies sehr unbefriedigend.

3. $R = \frac{4}{7}$. Für vier Quell-Bits kann man je drei "parity-check" Bits hinzufügen:

$$\begin{array}{rlll} & (x_1,\ldots,x_4) & \mapsto & (x_1,\ldots,x_7) \text{ mittels} \\ & x_5 & \equiv & x_2+x_3+x_4 \bmod 2 \\ & x_6 & \equiv & x_1+x_3+x_4 \bmod 2 \\ & x_7 & \equiv & x_1+x_2+x_4 \bmod 2, \\ \text{beispielsweise} & (0\ 1\ 1\ 0) & \mapsto & (0\ 11\ 0\quad 0\ 1\ 1). \end{array}$$

Zur Decodierung durch den Empfänger beachte man, dass in $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ gilt:

$$\underbrace{\left(\begin{array}{ccccc|ccc} 0 & 1 & 1 & 1 & \vdots & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & \vdots & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & \vdots & 0 & 0 & 1 \end{array}\right)}_{H} \left(\begin{array}{c} x_1 \\ \\ \vdots \\ \\ x_7 \end{array}\right) = \underline{0}$$

Jedes der möglichen 16 Codeworte $\underline{x} \in \mathbb{F}_2^7$ genügt $H\underline{x} = \underline{0}$. Wird der Vektor $\underline{x}$ gesendet und $\underline{y}$ empfangen, so ist $\underline{z} := \underline{y} - \underline{x} = \underline{y} + \underline{x}$ der Fehlervektor. Für den Empfänger ist nur $\underline{y}$ bekannt, er möchte $\underline{x}$ wissen. Er berechnet $\underline{s} = H\underline{y} = H(\underline{x} + \underline{z}) = H\underline{z}$, $\underline{s}$ heißt Syndrom von $\underline{y}$ (Schema von Krankheitssymptomen), es hängt nicht von $\underline{x}$ ab, nur vom Fehler $\underline{z}$. Die Kenntnis von $\underline{z}$ genügt aber oft zur Berechnung von $\underline{x}$. Es gilt:
$\underline{s} = \sum_{z_i \neq 0}$ (Spalte i von H). Man erhält 3 Gleichungen für 7 Unbekannte, das heißt für jedes $\underline{s}$ existieren 16 Möglichkeiten für $\underline{z}$. Wie soll daher die Wahl des Empfängers aussehen?
Würde zum Beispiel $(0\ 111\ 001) = \underline{y}^{tr}$ empfangen, so ist $\underline{s} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$, und man erhält folgende 16 Möglichkeiten für $\underline{z}$:

$$\begin{array}{ccccccc|ccccccc} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1. \end{array}$$

Da die pro-Bit Fehlerwahrscheinlichkeit $p < \frac{1}{2}$ ist, ist ein $\underline{z}$ mit wenig Koordinaten 1 wahrscheinlicher als eins mit vielen. Man wird also ein $\underline{z}$ mit möglichst wenig Einsen wählen, hier $0\ 1\ 0\ 0\ 0\ 0\ 0$. Im Allgemeinen besteht jedoch keine Eindeutigkeit. Es folgt bei unserer Wahl $\underline{x} = \underline{y} + \underline{z} = (0\ 0\ 1\ 1\ 0\ 0\ 1)$,

dass heißt die 4 Quell-Symbole werden als $(0\ 0\ 1\ 1)$ übersetzt.

In diesem Falle ist Eindeutigkeit gewährleistet (Forderung an guten Code): $\underline{s} = \underline{0} \Longrightarrow \underline{z} = \underline{0}$ ist gewünschte Lösung. $\underline{s} \neq \underline{0}$: Es ist $\underline{s}$ Spalte von H (!), etwa die i-te Spalte von H, also ist $\underline{z} = (0 - 0\ 1\ 0 - 0)$ der einzige Fehlervektor mit einer Eins und sonst Nullen.

Decodierungs-Verfahren (Maximum - likelyhood - decoding): Gegeben $\underline{y}, H$.

1. Berechne Syndrom $\underline{s} = H\underline{y}$.
2. Für $\underline{s} = \underline{0}$ setze $\hat{\underline{z}} = \underline{0}$ und gehe nach 4.
3. Bestimme i, so dass Spalte i von H gleich $\underline{s}$ ist. Setze $\hat{\underline{z}} = (0 - 0\ 1\ 0 - 0)$.
4. Setze $\hat{\underline{x}} = \underline{y} + \hat{\underline{z}}$ und drucke als Output die ersten vier Bit von $\hat{\underline{x}}$.

Verursacht der Kanal höchstens einen Fehler, ist $\hat{\underline{z}} = \underline{z}$, also das Resultat richtig. Der gegebene Code - $(7, 4)$ Hamming Code - ist also ein 1-Fehler - korrigierender Code. Es ist leicht zu sehen, dass das Decodierungs-Verfahren bei 2 oder mehr Fehlern schiefgeht.
Man erhält für die Fehlerwahrscheinlichkeit eines Codeworts:

$$P_e = \sum_{k=z}^{7} \binom{7}{k} p^k (1-p)^{7-k} = 21p^2 - 70p^3 + p^4(\ldots).$$

Die Bit-Fehler-Wahrscheinlichlkeit für das i-te Bit ergibt sich zu:

$$P_e^{(i)} = 9p^2 + p^3(\ldots).$$

Beweis. Bei keinem oder einem auftretenden Fehler wird korrekt decodiert. Den Koeffizienten für p^2 erhält man, wenn genau 2 Fehler auftreten (vgl. die vorangehende Formal für P_f). Diese liegen dann etwa in den Positionen j und k vor. Ist etwa $i = j$ und k von i verschieden, so ist die Summe der i-ten und k-ten Spalte von H von der i-ten verschieden. Die Korrektur mit $\hat{\underline{z}}$ lässt Bit i falsch. Dabei bestehen für festes i genau 6 Möglichkeiten für k. Ist dagegen $j \neq i \neq k$, so kann Spalte i von H sehr wohl die Summe der Spalten j und k sein. Für jedes mögliche j (6 Möglichkeiten) gibt es demnach genau ein k. Da die Paare (j, k) und (k, j) dasselbe Ergebnis liefern, gibt es genau 3 Möglichkeiten zu einer Fehlerkorrektur, die Bit i verfälscht. □

Das heißt für einen BSC mit kleinem p ist der Hamming-code mit $R = \frac{4}{7} = 0,571$ genauso gut wie das Wiederholungsschema mit $R = \frac{1}{3} = 0.333$.

Bemerkung Man kann den $(7, 4)$ Hamming-code auch dazu benutzen, für $R = 7/4$ zu kommunizieren, indem man die Rolle von Sender und Empfänger vertauscht.
Die Folge der Quell-Bits wird in Blocks à 7 aufgeteilt (Block-Codes), die 7 Bit werden jeweils mit

dem Decodierungsalgorithmus auf 4 reduziert und übertragen. Der Empfänger berechnet die Nachricht, indem er die parity-check Bits für die empfangenen 4 Bits anhängt. Man erhält die Fehlerwahrscheinlichkeit:

$$P_e = \sum_{i=1}^{7} P_e^{(i)}/7 = \frac{1}{8} + \frac{39}{28}p + \dots \ .$$

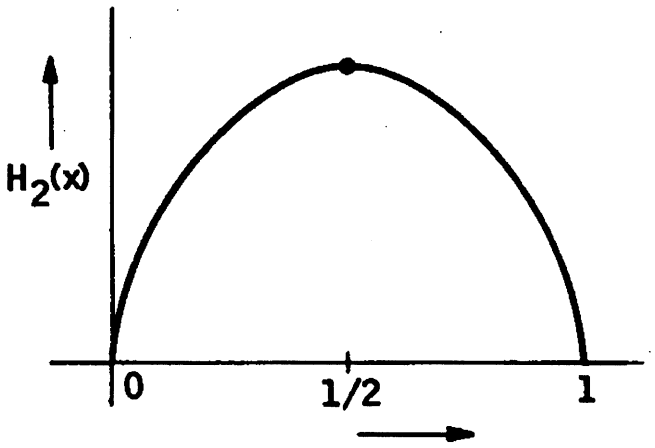
Für $p \sim 0$ ist dies gegenüber dem Münzenwerfen stark überlegen (letzteres würde $P_e = \frac{3}{14} = 0,214$ liefern).

Um nun eine Übersicht über mögliche Codes (dass heißt erreichbare Übertragungseigenschaften zu gewinnen), studieren wir den BSC mit Mitteln aus der Wahrscheinlichkeitstheorie. Hierin geht man von einem (n,k)-Code aus: k-Bit der Quelle (Quellwort) $\underline{u}$ werden zu einem n-Bit Codewort $\underline{x}$ codiert, welches übertragen wird in $\underline{y}$ und decodiert zu $\underline{v}$. Das Verhältnis ist $R = k/n$, die Bit-Fehler-Wahrscheinlichkeit $P_e = \frac{1}{k}\sum_{i=1}^{k} P_e^{(i)}$ mit $P_e^{(i)} = P\{v_i \neq u_i\} \quad (i = 1, \dots, k)$. Ein wichtiges Hilfsmittel ist nun die sogenannte Entropie des gegebenen endlichen Wahrscheinlichkeitsraumes:

$$H_2(x) := -x \log_2 x - (1-x)\log_2(1-x) \quad (0 < x < 1).$$

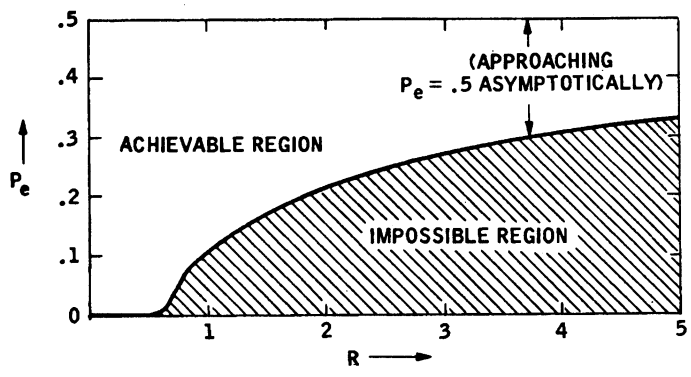
Hierin steht x für die Wahrscheinlichkeit p (raw Bit error probability), mit der ein Bit durch den BSC falsch übertragen wird. Die Funktion H_2 stellt ein Maß für die Unbestimmtheit des endlichen Wahrscheinlichkeitsraumes dar. Wir setzen dazu noch $H_2(0) = H_2(1) = 0$. Dann lassen sich die folgenden Eigenschaften leicht nachrechnen:

$$\begin{array}{lll} 0 \leq H_2(x) & \leq & 1 \quad (\text{“}=\text{”} \iff x = \frac{1}{2}), \\ H_2(x) & = & H_2(1-x), \\ H_2(x) & \text{ist} & \text{konkav.} \end{array}$$



Zeichnung aus McEliece

Dann ist die Begrenzungskurve für die erreichbaren Codes gerade $R = \frac{1-H_2(p)}{1-H_2(P_e)}$.



Zeichnung aus McEliece

Für $R < 1 - H_2(p)$ ist jedes noch so kleine positive P_e erreichbar! $(p = 0,1 : 1 - H_2(p) = 0,531)$, also $R \geq 0,5$ mit $P_e < 10^{-500}$ etwa erreichbar.) $C = 1 - H_2(p)$ heißt Kapazität des Kanals. "Arbitrarily reliable communication is possible at any rate below C."(Wiederholungscode: $P \longrightarrow 0$, aber auch $R \longrightarrow 0$).

1 Satz. (Shannon): *Es sei* $0 < R < C$ *und* $k = Rn, M = 2^k$. *Dann existiert zu* $n \in \mathbb{N}$ *ein* (n,k)*-Code mit* $P = \frac{1}{M} \sum_{i=1}^{M} p_i \longrightarrow 0$ *für* $n \longrightarrow \infty$.

Bekannte Beweise sind leider nicht konstruktiv!

Beweis. Der Beweis des Satzes von Shannon erfolgt in mehreren Schritten.

1. Die Anzahl W der Fehler in einem übertragenen Wort ist eine Zufallsvariable mit Erwartungswert

$$E = \sum_{i=1}^{n} i \underbrace{\binom{n}{i} p^i (1-p)^{n-i}}_{P_i}.$$

Aus $1 = \sum_{i=0}^{n} \binom{n}{i} p^i (1-p)^{n-i} = (p + (1-p))^n$ folgt durch Differentiation nach p:

$$\begin{aligned}
0 &= \sum_{i=1}^{n-1} \left(\binom{n}{i} i p^{i-1}(1-p)^{n-i} + \binom{n}{i} p^i (n-i)(1-p)^{n-i-1}(-1)\right) + n(1- \\
&\quad p)^{n-1}(-1) + np^{n-1} \\
&= \sum_{i=1}^{n-1} \{\binom{n}{i} i p^{i-1}(1-p)^{n-i-1}(1-p+p) - n\binom{n}{i} p^i (1-p)^{n-i-1}\} + n(1- \\
&\quad p)^{n-1}(-1)) + np^{n-1} \\
&= \sum_{i=1}^{n} \{i\binom{n}{i} p^{i-1}(1-p)^{n-i-1} - n\binom{n}{i} p^i (1-p)^{n-i-1}\} - \tfrac{np^{n-1}}{1-p} + np^{n-1} - \\
&\quad n(1-p)^{n-1} + \tfrac{np^n}{1-p} \\
&= E\tfrac{1}{p(1-p)} - \tfrac{n}{1-p} - n\tfrac{p^{n-1}}{1-p} + np^{n-1} + \tfrac{np^n}{1-p}
\end{aligned}$$

und damit $\frac{E}{P} = n + np^{n-1} - np^{n-1} + np^n - np^n$, also $E = np$.

Entsprechend gilt für die Varianz (Streuung)

$$V = \sum_{i=1}^{n} (i-E)^2 P_i : V = np(1-p).$$

Offenbar gilt für $b \in \mathbb{R}^{>0}$:

$$V \geq \sum_{|i-E| \geq \sqrt{b}} (i-E)^2 P_i \geq b \sum_{|i-E| \geq \sqrt{b}} P_i,$$

also

$$\frac{V}{b} \geq P(\mid W - E \mid > \sqrt{b}) \geq P(W > E + \sqrt{b}).$$

2. Wir setzen $\rho := \lfloor np + b \rfloor \left(< \frac{n}{2}\right)$. Dann erhalten wir für die Anzahl der Elemente in der Kugel um $\underline{x}$ vom Radius ρ im $\mathbb{F}_2^n$:

$$\begin{aligned}
\sharp S_\rho(\underline{x}) &= \sharp\{\underline{y} \in \mathbb{F}_2^n \mid\mid\mid \underline{y} - \underline{x} \mid\mid \leq \rho\} \\
&= \sum_{\nu \leq \rho} \binom{n}{\nu} < \tfrac{1}{2} n \binom{n}{s} \leq \tfrac{1}{2} n \tfrac{n^n}{\rho^\rho (n-\rho)^{n-\rho}}.
\end{aligned}$$

(Die letzte Ungleichung gilt dabei wegen

$$n^n = (\rho + n - \rho)^n = \ldots + \binom{n}{\rho} \rho^\rho (n-\rho)^{n-\rho} + \ldots .)$$

Außerdem gilt:

$$\begin{aligned} \tfrac{\rho}{n}\log\tfrac{\rho}{n} &= \tfrac{\lfloor np+b\rfloor}{n}\log\lfloor np+b\rfloor n \\ &= p\log p + O\left(\tfrac{1}{\sqrt{n}}\right) \end{aligned}$$

und entsprechend

$$\left(1-\frac{\rho}{n}\right)\log\left(1-\frac{\rho}{n}\right) = (1-p)\log(1-p) + O\left(\frac{1}{\sqrt{n}}\right).$$

3. Für $\underline{x}, \underline{y} \in \{0,1\}^n$ definieren wir

$$f(\underline{x},\underline{y}) := \begin{cases} 0 & \text{für} \quad \| \underline{x}-\underline{y} \| > \rho \\ 1 & \text{für} \quad \| \underline{x}-\underline{y} \| \leq \rho. \end{cases}$$

Für jeden Codevektor $\underline{x}_i$ sei $g_i(\underline{y}) := 1 - f(\underline{x}_i,\underline{y}) + \sum\limits_{j\neq i} f(\underline{y},\underline{x}_j)$
(Es ist $g_i(\underline{y}) = 0$ für $\underline{x}_i \in S_\rho(\underline{y})$, falls kein anderes Codewort in dieser Kugel ist, $g_i(\underline{y}) \geq 1$ sonst.)

4. Eigentlicher Beweis
Die Codeworte $\underline{x}, \ldots, \underline{x}_M \quad (M = 2^k)$ seien zufallsmäßig aus $\{0,1\}^n$ gewählt zur Übertragung von M Quellworten. Die Decodierungsregel wird wie folgt festgelegt: Falls $\underline{y}$ empfangen wird und genau ein Codewort $\underline{x}_i$ mit
$\| \underline{y}-\underline{x}_i \| \leq \rho$ existiert, decodiere $\underline{y}$ nach $\underline{x}_i$. Andernfalls wird ein Fehler deklariert, bzw. nach $\underline{x}_1$ (oBdA) decodiert. P_i bezeichne die Wahrscheinlichkeit, dass $\underline{x}_i$ nicht richtig decodiert wird, falls es gesendet wurde. Es gilt dann:

$$\begin{aligned} P_i &\leq \sum_{\underline{y}\in\{0,1\}^n} P(\underline{y} \mid \underline{x}_i) g_i(\underline{y}) \\ &= \sum_{\underline{y}} P(\underline{y} \mid \underline{x}_i)(1 - f(\underline{y},\underline{x}_i)) + \sum_{\underline{y}}\sum_{j\neq i} f(\underline{y},\underline{x}_i) P(\underline{y} \mid \underline{x}_i) \end{aligned}$$

Die erste Summe ist die Wahrscheinlichkeit für $\underline{y} \notin S_\rho(\underline{x}_i)$. Sie hängt nur von ρ ab und sei etwa α_ρ. Gemäß (i) ist $\alpha_\rho \leq \frac{\varepsilon}{2} \quad$ (wähle $b = \frac{V}{\varepsilon/2}$)). Danach ergibt sich die Wahrscheinlichkeit für die falsche Decodierung eines Wortes durch Mittelung über alle $i \quad (1 \leq i \leq M)$ zu:

$$P \leq \frac{1}{2}\varepsilon + \frac{1}{M}\sum_{i=1}^{M}\sum_{\underline{y}}\sum_{j\neq i} P(\underline{y} \mid \underline{x}_i) f(\underline{y},\underline{x}_j).$$

Für einen optimalen Code gilt erst recht:

$$\begin{aligned} P &\leq \tfrac{1}{2}\varepsilon + M^{-1}\sum_{i=1}^{M}\sum_{\underline{y}}\sum_{j\neq i} E(P(\underline{y} \mid \underline{x}_i)) E(f(\underline{y},\underline{x}_j)) \\ &= \tfrac{1}{2}\varepsilon + M^{-1}\sum_{i=1}^{M}\sum_{\underline{y}}\sum_{j\neq i} E(P(\underline{y} \mid \underline{x}_i))\tfrac{\sharp S_\rho}{2^n} \\ &= \tfrac{1}{2}\varepsilon + (M-1)\tfrac{\sharp S_\rho}{2^n}. \end{aligned}$$

Dazu beachte man $\sum_{\underline{y}} E(P(\underline{y} \mid \underline{x}_i)) = 1$ und $\sum_{j \neq i} \sum_{\underline{y}} E(P(\underline{y} \mid \underline{x}_i)) = M - 1$.

Es folgt $\log\left(P - \frac{\epsilon}{2}\right) \leq \log n + n \log n - \rho \log \rho - (n - \rho) \log(n - \rho) - \log 2 - n \log 2 + \log M$, also

$$\begin{aligned}
\tfrac{1}{n} \log\left(P - \tfrac{\epsilon}{2}\right) &\leq \tfrac{1}{n} \log n + \log_n - \tfrac{\rho}{n} \log \rho - \left(1 - \tfrac{\rho}{n}\right) \log(n - \rho) - \log 2 + \tfrac{1}{n} \log M \\
&= -\tfrac{\rho}{n} \log \tfrac{\rho}{n} - \tfrac{\rho}{n} \log n - \left(1 - \tfrac{\rho}{n}\right) \log\left(1 - \tfrac{\rho}{n}\right) \\
&\quad - \left(1 - \tfrac{\rho}{n}\right) \log n + \log n + \tfrac{1}{n} \log n - \log 2 + \tfrac{1}{n} \log M \\
&\underset{(ii)}{\leq} -p \log p - (1 - p) \log(1 - p) - 1 + \tfrac{1}{n} \log M + \kappa/\sqrt{n} \\
&= \tfrac{1}{n} \log M - C + \kappa/\sqrt{n}
\end{aligned}$$

Dies gilt für geeignetes $\kappa \in \mathbb{R}^{>0}$ bei hinreichend großem n, man beachte zudem $\log 2 = 1$. Gemäß Definition von M ist $\frac{1}{n} \log M - C + \kappa/\sqrt{n} < -\beta < 0$ für $n > n_0$, das heißt $P - \frac{\epsilon}{2} < 2^{-\beta n}$ für $n > n_0$, was den Beweis vollendet. □

Kapitel 1

Lineare Codes

Shannon: hard to find (Zufallscode gut, falls lang genug)
hard to analyze
hard to implement

Im Folgenden sei p stets eine Primzahl und $q = p^l$ für einen natürlichen, festen Exponten l.

1.1 Definition. Ein $[n, k]$ linearer Code über $\mathbb{F}_q$ ist ein k-dimensionaler Unterraum von $\mathbb{F}_q^n$. n heit Lnge, k die Dimension des Codes. (Verhltnis $R = \frac{k}{n}$)
Beschreibung mittels Basis: $\underline{x}_1, \ldots, \underline{x}_k$.

1.2 Definition. Es sei C ein $[n, k]$ linearer Code über $\mathbb{F}_q$ und $\underline{x}_1, \ldots, \underline{x}_k$ eine Basis von C. Dann heit $G_C := \begin{pmatrix} \underline{x}_1^{tr} \\ \vdots \\ \underline{x}_k^{tr} \end{pmatrix} \in \mathbb{F}_q^{kn}$ erzeugende Matrix für C.

1.3 Definition. Auf $\mathbb{F}_q^n$ wird mittels

$$<,>: \mathbb{F}_q^n \mathbb{F}_q^n \longrightarrow \mathbb{F}_q : (\underline{x}, \underline{y}) \mapsto \sum_{i=1}^{n} x_i y_i$$

ein skalares Produkt definiert. Für einen Teilraum C von $\mathbb{F}_q^n$ heit

$$C^{\perp} := \{\underline{x} \in \mathbb{F}_q^n \mid < \underline{x}, C >= 0\}$$

der zu C duale Code. (Im Fall $C = C^{\perp}$ heit C selbstdual.)

Beispiel $U =< (1100), (0011) >$ in $\mathbb{F}_2^4$.

1.4 Definition. Eine erzeugende Matrix $G_C^{\perp}$ des zu C dualen Codes $C^{\perp}$ heit Paritätskontrollmatrix (Prüfmatrix) von C.

Bemerkung Es gilt $G_C^{\perp}\underline{x} = 0 \quad \forall \underline{x} \in C$ sowie $G_C^{\perp}G_C^{tr} = O^{(n-k)n}$.

Encoding $\underline{x}^{tr} = (x_1, \ldots, x_n)$ sei Codewort mit $x_1, \ldots, x_k$ bekannt, $x_{k+1}, \ldots, x_n$ gesucht. Es gilt $\underline{x} = \alpha_1\underline{x_1} + \ldots + \alpha_n\underline{x_k} \quad (\alpha_i \in \mathbb{F}_q), \quad \underline{x_i}$ Zeilen von G_C. Angewendet auf $x_1, \ldots, x_k$ erhält man Gleichungen für $\alpha_1, \ldots, \alpha_k$ mit Koeffizientenmatrix $\begin{pmatrix} x_{11} & \ldots & x_{1k} \\ \vdots & & \vdots \\ x_{k1} & \ldots & x_{kk} \end{pmatrix}$. Ist diese regulär, so erhält man eine eindeutige Lösung.

1.5 Definition. Zwei lineare $[n, k]$ Codes C, C' über $\mathbb{F}_q$ heien äquivalent, falls es eine Permutation $\pi \in \mathfrak{S}_n$ gibt mit $\pi C = C'$. Jeder Code ist äquivalent zu einem mit erzeugender Matrix $G_C = (I_k \mid P)$, $P \in \mathbb{F}_q^{k(n-k)}$, in welchem Fall $G_C^{\perp} = (-P^{tr} \mid I_{n-k})$ gilt.

1.6 Definition. Codes mit solchen erzeugenden Matrizen heien systematische Codes.

Beispiel Für den $[7, 4]$ Hammingcode mit $q = 2$ ist dann

$$G_C = \left[\begin{array}{c|c} I_4 & \begin{matrix} 0\,1\,1 \\ 1\,0\,1 \\ 1\,1\,0 \\ 1\,1\,1 \end{matrix} \end{array}\right], \quad G_C^{\perp} = \left[\begin{array}{c|c} \begin{matrix} 0\,1\,1\,1 \\ 1\,0\,1\,1 \\ 1\,1\,0\,1 \end{matrix} & I_3 \end{array}\right].$$

1.7 Definition. Für $\underline{x}, \underline{y} \in \mathbb{F}_q^n$ definieren wir eine Metrik (“distance”) d mittels: $d(\underline{x}, \underline{y}) := \sharp\{i \in \{1, \ldots, n\} \mid x_i \neq y_i\}$. Das Gewicht (“weight”) von $\underline{x}$ wird dann erklärt als $wt(\underline{x}) := d(\underline{x}, \underline{0})$.

Bemerkung Man rechnet leicht nach, dass d tatsächlich die Axiome einer Metrik erfüllt: $d(\underline{x}, \underline{x}) = 0, d(\underline{x}, \underline{y}) = d(\underline{y}, \underline{x}), d(\underline{x}, \underline{z}) \leq d(\underline{x}, \underline{y}) + d(\underline{y}, \underline{z}) \quad \forall \underline{x}, \underline{y}, \underline{z} \in \mathbb{F}_q^n$. Auerdem gilt $d(\underline{x}, \underline{y}) = w(\underline{x} - \underline{y})$.

1.8 Definition. Für einen Code $C \subseteq \mathbb{F}_q^n$ heit $d_C := \min\{w(\underline{x}) \mid \underline{0} \neq \underline{x} \in C\}$ Minimalgewicht.

Bemerkung Es gilt bei (linearen) Codes $\mathcal{C}$ offenbar $D = \min\{d(\underline{x}, \underline{y}) \mid \underline{x}, \underline{y} \in \mathcal{C}, \underline{x} \neq \underline{y}\}$. Man beachte, dass für $\rho < D$ und $\underline{x} \in \mathcal{C}$ stets $\{\underline{y} \in \mathcal{C} \mid \underline{y} \in S_\rho(\underline{x})\} = \{\underline{x}\}$ ist.

Wie weit kann ein empfangenes Wort von einem Codewort entfernt sein?

1.9 Definition. Für einen Code $\mathcal{C} \subset \mathbb{F}_q^n$ heit

$$r_C := \max\{\min\{d(\underline{x}, \underline{y}) \mid \underline{y} \in \mathcal{C}\} \mid \underline{x} \in \mathbb{F}_q^n\}$$

Überdeckungsradius (“covering radiu”).

Also gilt: $\bigcup_{\underline{y} \in C} S_{d_C}(\underline{y}) \subseteq \mathbb{F}_q^n \subseteq \bigcup_{\underline{y} \in \mathcal{C}} S_{r_C}(\underline{y})$.

Im Hinblick auf Decodierung ergibt sich unmittelbar:
Ist $\underline{x} \in \mathcal{C}$ mit $w(\underline{x}) = \kappa$, enthält die parity check matrix $H_{\mathcal{C}} = G_C^{\perp}$ folglich κ linear abhängige Spalten.
Umgekehrt: Sind je κ Spalten von $H_{\mathcal{C}}$ linear unabhängig, so gilt $d_{\mathcal{C}} \geq \kappa + 1$.

Maximum likelyhood decoding: Zu empfangenem $\underline{y} \in \mathbb{F}_q^n$ bestimme $\underline{x} \in C$ mit $w(\underline{y} - \underline{x})$ minimal. Ist etwa $d_C = 2e + 1$, dann gilt für $\underline{x}_0 \in \mathbb{F}_q^n$ und $S(\underline{x}_0, r) = \{\underline{x} \in \mathbb{F}_q^n \mid w(\underline{x} - \underline{x}_0) \leq r\}$ (Kugel um $\underline{x}_0$ vom Radius $r \in \mathbb{R}^{>0}$):

1. $S(\underline{x}_0, 2e) \cap (C \backslash \{x_0\}) = \emptyset$ für $\underline{x}_0 \in C$.

2. $S(\underline{x}_0, e) \cap S(\underline{y}_0, e) = \emptyset \quad \forall \underline{x}_0, \underline{y}_0 \in C$ mit $\underline{x}_0 \neq \underline{y}_0$.

Hieraus folgt unmittelbar:

1.10 Satz. *Ein linearer Code C korrigiert alle Fehler(vektoren) $\underline{z}$ mit $w(\underline{z}) \leq \lfloor (d_C - 1)/2 \rfloor$, er entdeckt alle mit $w(\underline{z}) \leq d_C - 1$.*

1.11 Korollar. *d_C = Minimalzahl linear abhängiger Spalten von H_C.*

Beweis. Es sei κ die Minimalanzahl linear abhängiger Spalten von H_C. Dann ist $d_C \geq \kappa$, wie wir bereits gesehen haben. Sind andererseits die Spalten $\underline{s}_{i_1}, \ldots, \underline{s}_{i_\kappa}$ von H_C linear abhängig, so existiert $\underline{x} \in \mathbb{F}_g^n \backslash \{\underline{0}\}$ mit $x_\nu \begin{cases} \neq 0 \text{ für } \nu \in \{i_1, \ldots, i_\kappa\} \\ = 0 \text{ sonst} \end{cases}$ und $H_C \underline{x} = \underline{0}$. Dies besagt aber $\underline{x} \in C$ und $w(\underline{x}) = \kappa$. Also gilt auch $d_C \leq \kappa$ und insgesamt die Behauptung. □

1.12 Definition. Für $q = 2$ und $m \in \mathbb{N}$ sei $H_m \in \mathbb{F}_2^{m(2^m - 1)}$, so dass die Spalten von H_m gerade die Vektoren aus $\mathbb{F}_2^m \backslash \{\underline{0}\}$ bilden. (Die letzten m Spalten seien zudem I_m.) Der Unterraum $C = C_H^{(m)}$ von $\mathbb{F}_2^{2^m - 1}$ bestehend aus allen $\underline{y} \in \mathbb{F}_2^{2^m - 1}$ mit $H_m \underline{y} = \underline{0}$ heit Hamming Code der Länge $n = 2^m - 1$.

1.13 Hilfssatz. *Für $m \geq 2$ gilt: $C = C_H^{(m)}$ ist ein $[2^m - 1, 2^m - 1 - m, 3]$-Code, das heit, es ist speziell $3 = d_C$.*

Beweis. Die Aussagen $n = 2^m - 1$ und $k = 2^m - 1 - m$ sind aufgrund der Definition von C klar. Je zwei Spalten (mit verschiedenen Indizes) von H_C sind linear unabhängig, da sie verschieden sind. Es gibt stets 3 linear abhängige Spalten, etwa $(11000 \ldots 0)^{tr}, (10100 \ldots 0)^{tr}, (01100 \ldots 0)^{tr}$. Also ist $d_C = 3$ nach Korollar (1.11). □

1.14 Definition. Ein $[n, k, d]$-Code $C \subset \mathbb{F}_q^n$ heit perfekt, falls $\dot{\bigcup}_{\underline{x} \in C} S(\underline{x}_1 \frac{d-1}{2}) = \mathbb{F}_q^n$ ist.

1.15 Hilfssatz. *$C = C_H^{(m)}$ ist für $m \geq 2$ perfekt.*

Beweis. Die Kugelvereinigung ist disjunkt und in $\mathbb{F}_2^n$ enthalten. Die Gleichheit wird durch Anzahlaussagen bewiesen. $\sharp S(\underline{x}, 1) = 1 + n$, also $\sum_{\underline{x} \in C} \sharp S(\underline{x}, \frac{d-1}{2}) = 2^{2^m - 1 - m}(1 + 2^m - 1) = 2^{2^m - 1}$. □

1.1 Gewichtszähler

1.16 Definition. Für $i = 0, 1, \ldots, n$ und einen $[n, k, d]$-Code C setzen wir $A_i := \sharp\{\underline{x} \in C \mid wt(\underline{x}) = i\}$. Dann heit $A(t) = \sum_{i=0}^{n} A_i t^i \quad \in \mathbb{Z}[t]$ Gewichtszähler ("weight enumerator") zu C.

Bemerkung Es gilt $A_0 = 1, A_i = 0 \quad (2 \leq i < d), A(1) = q^k$.

Es sei Z_p die Gruppe der p-ten Einheitswurzeln $e^{2\pi i\kappa/p} \quad (0 \leq \kappa \leq p-1)$ sowie $\zeta = e^{2\pi i/p}$. Da $(\mathbb{F}_q, +)$ eine abelsche Gruppe vom Exponenten p ist, existieren Gruppenhomorphismen von der additiven Gruppe $(\mathbb{F}_q, +)$ in die multiplikative Gruppe Z_p, sogenannte Charaktere ψ. Wir konstruieren explizit einen surjektiven Homomorphismus. Es ist $\mathbb{F}_q$ ein Körper mit $q = p^l$ Elementen, speziell also $\mathbb{F}_p$-Vektorraum mit einer Basis $w_1 = 1, w_2, \ldots, w_l$. Wir bilden dann wie folgt ab: $(\mathbb{F}_q, +) \xrightarrow{\pi_1} \mathbb{F}_p \xrightarrow{\iota} Z_p$ mittels $\pi_1(x_1 w_1 + \ldots + x_l w_l) = x_1 \cdot 1 = x_1$, $\iota(x_1) = \zeta^{x_1}$. Man überlegt sich leicht, dass $\iota \circ \pi_1$ ein surjektiver Gruppenhomomorphismus ist.

1.17 Satz. *(MacWilliams Identität) Für die Gewichtszähler $A(t)$ eines $[n, k]$-Codes C und $B(t)$ von $C^\perp$ besteht die Gleichung:*

$$q^k B(t) = (1 + (q-1)t)^n A\left(\frac{1-t}{1+(q-1)t}\right).$$

Beweis. Es sei $\psi : (\mathbb{F}_q, +) \longrightarrow Z_p$ ein Gruppenepimorphismus.

1. Für $\underline{y} \in \mathbb{F}_q^n$ gilt: $\sum_{\underline{x} \in C} \psi(\underline{x}^{tr}\underline{y}) = \begin{cases} q^k \text{ für } \underline{y} \in C^\perp \\ 0 \text{ sonst} \end{cases}$.

   Ist $\underline{y} \in C^\perp$, so gilt $\underline{x}^{tr}\underline{y} = 0 \quad \forall \underline{x} \in C$, die fragliche Summe besteht also aus $\sharp C = q^k$ Summanden Eins. Ist $\underline{y}$ nicht aus $C^\perp$, so existiert $\underline{x} \in C$ mit $\underline{x}^{tr}\underline{y} \neq 0$. Hiernach existiert auch ein skalares Vielfaches von $\underline{x}$ mit $\underline{x}^{tr}\underline{y} = 1$ bzw. $\underline{x}^{tr}\underline{y} = i$ für $0 \leq i \leq p-1$. Also ist die Abbildung $\varphi_{\underline{y}} : C \longrightarrow Z_p : \underline{x} \mapsto \psi(\underline{x}^{tr}\underline{y})$ in diesem Fall ein surjektiver Homomorphismus. Wir setzen $H = \ker \varphi_{\underline{y}}$ mit $\sharp H = q^k/p$ sowie $C = \dot{\bigcup_{i=1}^{p}} \underline{x}_i H$. Es folgt

$$\begin{aligned}
\sum_{\underline{x} \in C} \psi(\underline{x}^{tr}\underline{y}) &= \sum_{i=1}^{p} \sum_{\underline{z} \in H} \psi(\underline{y}^{tr}(\underline{x}_i + \underline{z})) \\
&= \sum_{i=1}^{p} \sum_{\underline{z} \in H} \psi(\underline{y}^{tr}\underline{x}_i)\psi(\underline{y}^{tr}\underline{z}) \\
&= \sum_{i=1}^{p} \psi(\underline{y}^{tr}\underline{x}_i)\tfrac{q^k}{p} \\
&= \tfrac{q^k}{p} \sum_{i=1}^{p} \zeta^i \\
&= 0.
\end{aligned}$$

Die letzte Gleichung ist eine Konsequenz von $t^p - 1 = \prod_{i=1}^{p}(t - \zeta^i)$ in $\mathbb{C}[t]$ und davon, dass dann $-\sum_{i=1}^{p}\zeta^i$ der Koeffizient von t^{p-1} im Polynom $t^p - 1$ ist, also gleich 0.

2. Für $\underline{x} \in \mathbb{F}_q^n$ gilt

$$\sum_{\underline{y}\in\mathbb{F}_q^n} \psi(\underline{y}^{tr}\underline{x})t^{wt(\underline{y})} = (1-t)^{wt(\underline{x})}(1+(q-1)t)^{n-wt(\underline{x})}.$$

Es ist für $\underline{x} = (x_1, \ldots, x_n)^{tr}, \underline{y} = (y_1, \ldots, y_n)^{tr}$:

$$\begin{aligned}
\sum_{\underline{y}\in\mathbb{F}_q^n} \psi(\underline{y}^{tr}\underline{x})t^{wt(\underline{y})} &= \sum_{y_1\in\mathbb{F}_q} \cdots \sum_{y_n\in\mathbb{F}_q} (\prod_{i=1}^{n} \psi(y_i x_i))t^{wt(\underline{y})} \\
&= \sum_{y_1\in\mathbb{F}_q} \cdots \sum_{y_n\in\mathbb{F}_q} \prod_{i=1}^{n} (\psi(y_i x_i)t^{wt(y_i)}) \\
&= \prod_{i=1}^{n} (\sum_{y\in\mathbb{F}_q} \psi(yx_i)t^{wt(y)}) \\
&= \prod_{i=1}^{n} \begin{cases} 1+(q-1)t \text{ für } x_i = 0 \\ 1-t \text{ für } x_i \neq 0 \end{cases} .
\end{aligned}$$

Für $x_i = 0$ ist die Aussage evident. Für $x_i \neq 0$ folgt sie aus
$\sum_{y\in\mathbb{F}_q\setminus\{0\}} \psi(yx_i)t^{wt(y)} = t(\sum_{y\in\mathbb{F}_q} \psi(yx_i) - 1)$, da hier - wie in Teil (1) -
$\sum_{y\in\mathbb{F}_q} \psi(yx_i) = 0$ ist.

3. Wir berechnen $S := \sum_{\underline{x}\in C}\sum_{\underline{z}\in C}\sum_{\underline{y}\in\mathbb{F}_q^n} \psi(\underline{y}^{tr}(\underline{x}-\underline{z}))t^{wt(\underline{y})}$ auf 2 Arten.
Zunächst gilt nach (2):

$$S = \sum_{\underline{x}\in C}\sum_{\underline{z}\in C}(1-t)^{wt(\underline{x}-\underline{z})}(1+(q-1)t)^{n-wt(\underline{x}-\underline{z})}.$$

Für $i \in \{0, 1, \ldots, n\}$ und $i = wt(\underline{x} - \underline{z})$ erhalten wir bei festem $\underline{x} \in C$:
$\sharp\{\underline{z} \in C \mid wt(\underline{x} - \underline{z}) = i\} = \sharp\{\underline{y} \in C \mid wt(\underline{y}) = i\} = A_i$, also
$\tilde{A}_i := \sharp\{(\underline{x}, \underline{z}) \in C^2 \mid wt(\underline{x} - \underline{z}) = i\} = q^k A_i$.
Damit bekommen wir für S:

$$\begin{aligned}
S &= \sum_{i=0}^{n} q^k A_i(1-t)^i \quad (1+(q-1)t)^{n-i} \\
&= q^k \sum_{i=0}^{n} A_i(1+(q-1)t)^n \left(\tfrac{(1-t)}{1+(q-1)t}\right)^i,
\end{aligned}$$

also das q^k-fache der rechten Seite in der Behauptung des Satzes.

Ordnen wir dagegen die Summationsreihenfolge bei S um, so erhalten wir

$$\begin{aligned}
S &= \sum_{\underline{y}\in\mathbb{F}_q^n}\sum_{\underline{x}\in C}\sum_{\underline{z}\in C}\psi(\underline{y}^{tr}(\underline{x}-\underline{z}))t^{wt(\underline{y})}\\
&= \sum_{\underline{y}\in\mathbb{F}_q^n} t^{wt(\underline{y})}\sum_{\underline{x}\in C}\sum_{\underline{z}\in C}\psi(\underline{y}^{tr}\underline{x})\psi(\underline{y}^{tr}(-\underline{z})) \text{ (beachte: mit } -\underline{z} \text{ durchläuft auch } \underline{z} \text{ ganz } C)\\
&= \sum_{\underline{y}\in\mathbb{F}_q^n} t^{wt(\underline{y})}\prod_{i=1}^{2}\left(\sum_{\underline{x}\in C}\psi(\underline{y}^{tr}\underline{x})\right)\\
&\underset{(1)}{=} \sum_{\underline{y}\in\mathbb{F}_q^n} t^{wt(\underline{y})}\begin{cases} q^{2k} \text{ für } \underline{y}\in C^\perp\\ 0 \text{ für } \underline{y}\notin C^\perp\end{cases}\\
&= q^{2k}B(t).
\end{aligned}$$

□

Bemerkung Für k gro ist die Berechnung der Gewichte aller Codeworte zu aufwendig. Ist $n-k$ dafür "klein", gelingt die Berechnung aber für $C^\perp$.

Beispiele:

1. $C=\{\underline{0},(11111)\}$ in $\mathbb{F}_2^5$ hat $A(t)=1+t^5$.

2. C sei $[5,3]$ - Code in $\mathbb{F}_2^5$, er hat 8 Codeworte, $C^\perp$ nur 4. $C^\perp$ habe $G^\perp=H=\begin{pmatrix}1&1&1&0&1\\1&0&0&1&0\end{pmatrix}$.

   $C^\perp$ hat als Gewichtszähler $B(t)=1+t^2+2t^4$; es folgt

$$\begin{aligned}
2^2A(t) &= (1+t)^5B\left(\tfrac{1-t}{1+t}\right)\\
&= (1+t)^5\left(1+\left(\tfrac{1-t}{1+t}\right)^2+2\left(\tfrac{1-t}{1+t}\right)^4\right)\\
&= 1+5t+10t^2+10t^3+5t^4+t^5\\
&\quad +(1-2t+t^2)(1+3t+3t^2+t^3)\\
&\quad +2(1+t)(1-4t+6t^2-4t^3+t^4),\\
A(t) &= 1+3t^2+3t^3+t^5.
\end{aligned}$$

3. $C^\perp$ habe $H=\begin{pmatrix}0&1&1&1&1&0&0\\1&0&1&1&0&1&0\\1&1&0&1&0&0&1\end{pmatrix}$; man berechnet leicht $B(t)=1+7t^4$ und damit

$$\begin{aligned}
2^3A(t) &= (1+t)^7\left(1+7\left(\tfrac{1-t}{1+t}\right)^4\right)\\
&= 1+7t+21t^2+35t^3+35t^4+21t^5+7t^6+t^7\\
&\quad +7\underbrace{(1-t)^4(1+t)^3}_{},\\
&\quad (1-4t+6t^2-4t^3-t^4)(1+3t+3t^2+t^3)
\end{aligned}$$

   also $A(t)=1+7t^3+7t^4+t^7$.

1.2 Schranken für Codes

1.18 Lemma. - (Hamming Schranke) *C binärer $[n,k,d]$ - Code mit $d \in \{2e+1, 2e+2\}$ enthält höchstens $2^n \left(\sum_{i=0}^{e} \binom{n}{i}\right)^{-1}$ Codeworte.*

Beweis. $\bigcup_{\underline{x} \in C} S(\underline{x}, e)$ ist disjunkt und in $\mathbb{F}_2^n$ enthalten.

Also gilt: $\sharp$ Codeworte $\cdot \left(\sum_{i=0}^{e} \binom{n}{i}\right) \leq 2^n$. □

1.19 Lemma. (Gilbert-Varshamov Schranke) *Unter allen linearen binären $[n,k,d]$ Codes über $\mathbb{F}_2$ gibt es einen mit mindestens $2^n \left(\sum_{i=0}^{d-1} \binom{n}{i}\right)^{-1}$ Codewörtern.*

Beweis. Annahme, der beste lineare Code C hätte weniger Codewörter. Dann hätte $\underline{x} + C$ mit $\underline{x} \in \mathbb{F}_2^n$ passend lauter Vektoren vom Gewicht $\geq d$.
(Es gibt $\underline{x} \in \mathbb{F}_2^n$, welches in keiner Kugel vom Radius $d-1$ um Codewörter $\underline{y} \in C$ liegt, $\underline{x} \notin S(\underline{0}, d-1)$, also $wt(\underline{x}) \geq d$. Sei ferner $\underline{x} + \underline{y} \in \underline{x} + C$, für $d > wt(\underline{x} + \underline{y}) = wt(\underline{x} - \underline{y})$ wäre $\underline{x} \in S(y, d-1)$.) Hiernach ist (!) $C \dot{\cup} (\underline{x} + C)$ Code mit Minimalgewicht $\geq d$ und zweimal so vielen Codewörtern. □

1.20 Lemma. (Singleton Bound) *Für einen $[n,k,d]$ Code C in $\mathbb{F}_q^n$ gilt: $k + d \leq n + 1$.*

Beweis. Es ist $W := \{(a_1, \ldots, a_n)^t \in \mathbb{F}_q^n \mid a_i = 0 \quad \forall i \geq d\}$ Unterraum von $\mathbb{F}_q^n$. Alle $\underline{x} \in W$ haben $wt(\underline{x}) \leq d-1$, es folgt $W \cap C = \{\mathbf{0}\}$. Wegen $\dim W = d-1$ folgt $k + (d-1) = \dim(C+W) \leq n$. □

Bemerkung Codes mit $k + d = n + 1$ heien MDS Codes (maximum distance separable Codes).

In einer Hinsicht ist die Singleton Bound schwächer als die von Hamming. Sei etwa
$n = 15, d = 5 \overset{Si}{\Longrightarrow} k \leq 11$,

$n = 15, d = 5 \overset{Ha}{\Longrightarrow} 2^k \leq 2^{15}(1 + 15 + 105)^{-1} \Longrightarrow k \leq 8$.

1.21 Satz. *Für einen Code mit $[n,k,d]$ sind äquivalent:*

1. *C ist MDS-Code;*
2. *$d = n - k + 1$;*
3. *je $n-k$ Spalten der Parity Check Matrix sind linear unabhängig;*
4. *je k Spalten der Erzeugermatrix sind linear unabhängig.*

Beweis. (1) $\Longrightarrow$ (3) Wir haben

$$\begin{array}{rcll} d = n-k+1 & \Longleftrightarrow & \forall \underline{x} \in C \backslash \{\underline{0}\} & : wt(\underline{x}) \geq n-k+1 \\ & & \wedge\, \exists \underline{x} \in C & : wt(\underline{x}) = n-k+1 \\ & \Longleftrightarrow & \text{je } n-k & \text{Spalten der “parity check matrix”} \\ & & & \text{sind linear unabhängig.} \end{array}$$

(1) $\Longleftrightarrow$ (3) Es genügt zu zeigen:
$d \leq n-k \Longleftrightarrow$ die Erzeugermatrix hat k linear abhängige Spalten.
Die sieht man folgendermaen:

$$\begin{array}{rcl} d \leq n-k & \Longleftrightarrow & \exists \rho_1, \ldots, \rho_k \in \mathbb{F}_q, \text{ nicht alle } 0, \text{ mit } wt(\sum_{\mu=1}^{k} \rho_\mu * \text{ (Zeile } \mu \text{ von } G_C)) \leq n-k \\ & \Longleftrightarrow & \exists \rho_1, \ldots, \rho_k \in \mathbb{F}_q, \text{ nicht alle } 0, \text{ sowie Indizes } 1 \leq j_1 < j_2 < \ldots < j_k \leq n, \\ & & \text{so dass die } j_i \text{ -te Koordinate von } \underline{0} \neq \sum_{\mu=1}^{k} \rho_\mu * \text{ (Zeile } \mu \text{ von } G_C) \\ & & \text{verschwindet } (1 \leq i \leq k) \\ & \Longleftrightarrow & \exists 1 \leq j_1 < j_2 < \ldots < j_k \leq n, \text{ so dass die Teilmatrix von } G_C \\ & & \text{bestehend aus den Spalten } j_1, \ldots, j_k \text{ einen Rang } < k \text{ hat} \\ & \Longleftrightarrow & \exists 1 \leq j_1 < j_2 < \ldots < j_k \leq n, \text{ so dass die Spalten } j_i \text{ von } G_C \\ & & \text{linear abängig sind } \quad (1 \leq i \leq k). \end{array}$$

□

1.22 Korollar. *Ein Code C ist genau dann MDS-Code, wenn $C^\perp$ MDS-Code ist.*

1.3 Decoding of linear codes

1.23 Definition. Let C be a linear code of length n over $\mathbb{F}_q$, and let $\mathbf{u} \in \mathbb{F}_q^{1n}$ be any vector of length n; we define the coset of C determined by $\mathbf{u}$ to be set

$$C + \mathbf{u} = \{\mathbf{v} + \mathbf{u} : \mathbf{v} \in C\} (= \mathbf{u} + C).$$

From group theory we recall

1.24 Theorem. *Let C be an $[n,k,d]$-linear code over the finite field $\mathbb{F}_q$. Then,*

1. *every vector of $\mathbb{F}_q^{1n}$ is contained in some coset of C;*
2. *for all $\mathbf{u} \in \mathbb{F}_q^{1n}$, $\mid C + \mathbf{u} \mid = \mid C \mid = q^k$;*
3. *for all $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^{1n}$, $\mathbf{u} \in C + \mathbf{v}$ implies that $C + \mathbf{u} = C + \mathbf{v}$;*
4. *two cosets are either identical or they have empty intersection;*
5. *there are q^{n-k} different cosets of C;*

6. *for all* $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^{1n}, \mathbf{u} - \mathbf{v} \in C$ *if and only if* $\mathbf{u}$ *and* $\mathbf{v}$ *are in the same coset.*

Example The cosets of the binary linear code $C = \{0000, 1011, 0101, 1110\}$ are as follows:

$0000 + C:$	0000	1011	0101	1110
$0001 + C:$	0001	1010	0100	1111
$0010 + C:$	0010	1001	0111	1100
$1000 + C:$	1000	0011	1101	0110

1.25 Definition. A word of the least (Hamming) weight in a coset is called a coset leader.

Nearest neighbour decoding for linear codes

Let C be a linear code. Assume the codewort $\mathbf{v}$ is transmitted and the word $\mathbf{w}$ is received, resulting in the error pattern (or error string) $\mathbf{e} = \mathbf{w} - \mathbf{v} \in \mathbf{w} + C$.
Then $\mathbf{w} - \mathbf{e} = \mathbf{v} \in C$, so, by part (vi) of Theorem (1.24), the error pattern $\mathbf{e}$ and the received word $\mathbf{w}$ are in the same coset.
Since error patterns of small weight are the most likely to occur, nearest neighbour decoding works for a linear code C in the following manner. Upon receiving the word $\mathbf{w}$, we choose a word $\mathbf{e}$ of least weight in the coset $\mathbf{w} + C$ and conclude that $\mathbf{v} = \mathbf{w} - \mathbf{e}$ was the codeword transmitted.

Example Let $q = 2$ and $C = \{0000, 1011, 0101, 1110\}$. Decode the following received words:

1. $\mathbf{w} = 1101$;
2. $\mathbf{w} = 1111$.

From the standard array of C (see example above) we conclude:

1. $\mathbf{w} = 1101 : w + C$ is the fourth coset. The word of least weight in this coset is 1000 (note that this is the unique coset leader of this coset). Hence, $1101 - 1000 = 1101 + 1000 = 0101$ was the most likely codeword transmitted (note that this is the word at the top of the column where the received word 1101 is found).
2. $\mathbf{w} = 1111 : w + C$ is the second coset. There are two words of smallest weight, 0001 and 0100, in this coset. (This means that there are two choices for the coset leader. In the array above, we have chosen 0001 as the coset leader. If we had chosen 0100, we would have obtained a slightly different array.)

Syndrome decoding

The decoding scheme based on the standard array works reasonably well when the length n of the linear code is small, but it may take a considerable amount of time when n is large. Some time can be saved by making use of the syndrome to identify the coset to which the received word belongs.

1.26 Definition. Let C be an $[n,k,d]-$linear code over $\mathbb{F}_q$ and let H be a parity-check matrix for C. For any $\mathbf{w} \in \mathbb{F}_q^{1n}$, the syndrome of $\mathbf{w}$ is the word $S(\mathbf{w}) = \mathbf{w}H^{tr} \in \mathbb{F}_q^{n-k}$. (Strictly speaking, as the syndrome depends on the choice of the parity-check matrix H, it is more appropriate to denote the syndrome of $\mathbf{w}$ by $S_H(\mathbf{w})$ to emphasize this dependence. However, for simplicity of notation, the suffix H is dropped whenever there is no risk of ambiguity.)

1.27 Theorem. *Let C be an $[n,k,d]$-linear code and let H be a parity-Check matrix for C. For $\mathbf{u},\mathbf{v} \in \mathbb{F}_q^{1n}$, we have*

1. $S(\mathbf{u}+\mathbf{v}) = S(\mathbf{u}) + S(\mathbf{v})$;
2. $S(\mathbf{u}) = \mathbf{0}$ *if and only if* $\mathbf{u}$ *is a codeword in* C;
3. $S(\mathbf{u}) = (\mathbf{v})$ *if and only if* $\mathbf{u}$ *and* $\mathbf{v}$ *are in the same coset of* C.

1.28 Remark.
1. *Part (3) of Satz (1.27) says that we can identify a coset by its syndrome; conversely, all the words in a given coset yield the same syndrome, so the syndrome of a coset is the sydrome of any word in the coset. In other words, there is a one-to-one correspondence between the cosets and the sydromes.*
2. *Since the syndromes are in $\mathbb{F}_q^{n-k}$, there are at most q^{n-k} syndromes. Theorem (1.24)5 says that there are q^{n-k} cosets, so there are q^{n-k} corresponding sydromes (all distinct). Therefore, all the vectors in $\mathbb{F}_q^{n-k}$ appear as syndromes.*

1.29 Definition. A table which matches each coset leader with its sydrome is called a syndrome look-up table. (Sometimes such a table is called a standard decoding array (SDA).)

Steps to construct a syndrome look-up table assuming complete nearest neighbour decoding

Step 1: List all the cosets for the code, choose from each coset a word of least weight as coset leader $\mathbf{u}$.
Step 2: Find a parity-check matrix H for the code and, for each coset leader $\mathbf{u}$, calculate its syndrome $S(\mathbf{u}) = \mathbf{u}H^{tr}$.

1.30 Remark. *For incomlete nearest neighbour decoding, if we find more than one word of smallest weight in Step 1 of the above procedure, place the symbol " $*$ " in that entry of the syndrome look-up table to indicate that retransmission is required.*

Example Assume complete nearest neighbour decoding. Construct a syndrome look-up table for the binary linear code $C = \{0000, 1011, 0101, 1110\}$. From the cosets computed earlier, we choose the words $0000, 0001, 0010$ and 1000 as coset leaders. Next, a parity-check matrix for C is

$$H = \begin{pmatrix} 1\,0\,1\,0 \\ 1\,1\,0\,1 \end{pmatrix}.$$

Example Assuming complete nearest neighbour decoding, construct a syndrome look-up table for the binary linear code C with parity-check matrix H, where

$$H = \begin{pmatrix} 1\,0\,1\,1\,0\,0 \\ 1\,1\;\;1\,0\,1\,0 \\ 0\,1\,1\,0\,0\,1 \end{pmatrix}.$$

First, we claim that the distance of C is $d = 3$. This easily follows from the fact that no two columns of H are linearly dependent while the second, third and fourth columns are linearly dependent. As $\lfloor (d-1)/2 \rfloor = 1$, all the error patterns with weight 0 or 1 will be coset leaders. We then compute the syndrome for each of them and obtain the first seven rows of the syndrome look-up table. Since every word of length 3 must occur as a syndrome, the remaining coset leader $\mathbf{u}$ has syndrome $\mathbf{u}H^T = 101$. Moreover, $\mathbf{u}$ must have weight ≥ 2 since all the words of weight 0 or 1 have already been included in the syndrome look-up table. Since we are looking for a coset leader, it is reasonable to start looking among the raiming words of the smallest available weight, i.e., 2. Doing so, we find three possible coset leaders: $000101, 001010$ and 110000. Since we are using complete nearest neighbour decoding, we can arbitrarily choose 000101 as a coset leader and complete the syndrome look-up table (Table 1.31).

1.31 Table.

Coset leader $\mathbf{u}$	*Syndrome S(*$\mathbf{u}$*)*
000000	*000*
100000	*110*
010000	*011*
001000	*111*
000100	*100*
000010	*010*
000001	*001*
$*$ *000101*	*101*

Note that, if incomplete nearest neighbour decoding is used, the coset leader 000101 in the last row of Table (1.31) will be replaced by " $*$ ".

Decoding procedure for syndrome decoding

Step 1: For the received word $\mathbf{w}$, compute the syndrome $S(\mathbf{w})$.
Step 2: Find the coset leader $\mathbf{u}$ next to the syndrome $S(\mathbf{w}) = S\mathbf{u}$ in the syndrome look-up table.
Step 3: Decode $\mathbf{w}$ as $\mathbf{v} = \mathbf{w} - \mathbf{u}$.

Operations-Name	**Operation**	**standardmäig**	$(\mathbf{n}, \mathbf{k}, \mathbf{d}) \longrightarrow$
1) Erweiterung	Hinzufügen eines Prüf-Bits	Paritätsbit in zus. Spalte	$(n+1, k, d' \in \{d, d+1\})$
2) Punktierung	Auslassen eines Prüf-Bits	letztes Bit weglassen	$(n-1, k, d' \in \{d, d-1\})$
3) Reinigung	Elimination von Codewörtern	elim. Codeworte unger. Gewichts	$(n$, (i. a.) $k-1, d' \geq d)$
4) Vermehrung	Addition neuer Codeworte	$C \longrightarrow C \cup (1+C)$	$(n$, (i.a.) $k+1, d' = \min\{d, n-\tilde{d}\})$ mit $\tilde{d}$ largest weight $< n$
5) Verlängerung	Addition eines Nachrichtenbits	$4)+1)$	$(n+1, k+1, d' \leq d)$
6) Verkürzung	Weglassen einer Koordinate durch Querschnittbildung	nimm alle Codeworte, die mit 0 beginnen, streiche 1. Spalte	$(n-1, k-1, d' \geq d)$

Beispiel Hamming

$$(2^m-1, 2^m-1-m, 3) \quad \longrightarrow \quad \begin{matrix} H_{erw}\,(2^m, 2^m-1-m, 4) \\ \overset{\perp}{H_{erw}}(2^m, m+1, \overset{?}{2^{m-1}}) \end{matrix}$$

Abbildung 1.1: Gewinnung neuer Codes aus gegebenen

1.4 Reed-Muller-Codes

Es sei $n = 2^m$, $\mathbb{F}_2^m = \{\underline{x}_0, \underline{x}_1, \ldots, \underline{x}_{2^m-1}\}$, wobei $\underline{x}_i$ den Koeffizientenvektor der dualen Darstellung von i bezeichnet. Eine Basis bilden die Einheitsvektoren $\underline{u}_1, \ldots, \underline{u}_m$; dabei entspricht dann $\underline{u}_i$ der Dualdarstellung von 2^{i-1} :
$\underline{u}_1 = (1\ 0 \ldots 0)^{tr}, \underline{u}_2 = (0\ 1\ 0 \ldots 0)^{tr}, \ldots, \underline{u}_m = (0 \ldots 0\ 1)^{tr}$. Dann gilt:
$\underline{x}_j = \sum_{i=1}^{m} \xi_{ij}\underline{u}_i (j = 0, \ldots, 2^m - 1, \xi_{ij} \in \mathbb{F}_2)$.
Definiere für $i = 1, \ldots, m$: $A_i := \{\underline{x}_j \in \mathbb{F}_2^m \mid \xi_{ij} = 1\}$.

Andererseits betrachten wir den Zeilenraum $\mathbb{F}_2^{1n}$, insbesondere hat die Matrix $\mathfrak{M} = (\underline{x}_0 \ldots \underline{x}_{2^m-1})$ die Zeilen $\mathfrak{v}_1, \ldots, \mathfrak{v}_m$. Dann lässt sich $\mathfrak{v}_j$ mittels $\mathbb{F}_2^m \longrightarrow \mathbb{F}_2 : \underline{x}_j \mapsto \xi_{ij}$ als charakteristische Funktion von $A_i \subset \mathbb{F}_2^m$ auffassen. Wir versehen nun $\mathbb{F}_2^{1n}$ mit einer koordinatenweisen Multiplikation: $\mathbb{F}_2^{1n}\mathbb{F}_2^{1n} \longrightarrow \mathbb{F}_2^{1n} : (\mathfrak{a}, \mathfrak{b}) \mapsto (\alpha_1\beta_1, \ldots, \alpha_n\beta_n)$. Hierfür gilt: $\mathfrak{a} \circ \mathfrak{a} = \mathfrak{a} \circ \mathbf{1} = \mathfrak{a}$ mit $\mathbf{1} = (1, \ldots, 1) \in \mathbb{F}_2^{1n}, \mathfrak{a} \circ \mathfrak{b} = \mathfrak{b} \circ \mathfrak{a}, \mathfrak{a} \circ (\mathfrak{b} \circ \mathfrak{c}) = (\mathfrak{a} \circ \mathfrak{b}) \circ \mathfrak{c}, \mathfrak{a} \circ (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \circ \mathfrak{b} + \mathfrak{a} \circ \mathfrak{c}$, das heit $\mathbb{F}_2^{1n}$ wird mit $\circ$ zu einer $\mathbb{F}_2-$ Algebra mit Einselement $\mathbf{1}$. Dann ist die charakteristische Funktion für $\mathbb{F}_2^m \backslash A_i$ gerade $\mathbf{1} + \mathfrak{v}_i$.

Es seien nun $1 \leq i_1 < \ldots < i_s \leq m$. Dann ist $\mathfrak{v}_{i_1} \circ \ldots \circ \mathfrak{v}_{i_s}$ charakteristische Funktion (!) von $A_{i_1} \cap \ldots \cap A_{i_s}$. Dieser Durchschnitt hat 2^{m-s} Elemente, folglich gilt $w(\mathfrak{v}_{i_1} \circ \ldots \circ \mathfrak{v}_{i_s}) = 2^{m-s}$.

1.32 Satz. $\mathfrak{v}_0 = \mathbf{1}, \mathfrak{v}_1, \ldots, \mathfrak{v}_m, \mathfrak{v}_{i_1} \circ \ldots \circ \mathfrak{v}_{i_j} \quad (1 \leq i_1 < i_2 < \ldots < i_j \leq m, \quad j = 2, \ldots, m)$ *bilden eine Basis von* $\mathbb{F}_2^{1n}$.

Beweis. Die Anzahl dieser Vektoren ist

$$\binom{m}{0} + \binom{m}{1} + \ldots + \binom{m}{m} = 2^m = n.$$

Also bleibt zu zeigen, dass diese Vektoren den ganzen Raum aufspannen. Es bezeichne $\mathfrak{e}_j \quad (j = 1, \ldots, n)$ die kanonische Basis von $\mathbb{F}_2^{1n}$, das heit $\mathfrak{e}_j$ hat alle Koordinaten 0 mit Ausnahme einer Eins an der j-ten Stelle. Offenbar ist $\mathfrak{e}_j$ charakteristische Funktion für $\underline{x}_j$. Damit gilt wegen $\{\underline{x}_j\} = \bigcap_{\substack{i=1 \\ \xi_{ij}=1}}^{m} A_i \bigcap_{\substack{i=1 \\ \xi_{ij}=0}}^{m} (\mathbb{F}_2^{m1} \backslash A_i)$ dann

$$\begin{aligned} \mathfrak{e}_j &= \prod_{\substack{i=1 \\ \xi_{ij}=1}}^{m} \mathfrak{v}_i \prod_{\substack{i=1 \\ \xi_{ij}=0}}^{m} (\mathfrak{v}_0 + \mathfrak{v}_i) \\ &= \prod_{i=1}^{m} (\mathfrak{v}_i + (1 + \xi_{ij})\mathfrak{v}_0). \end{aligned}$$

□

Beispiel $n = 8, m = 3$

$$\begin{array}{rl}
\mathfrak{v}_0 & (1\,1\,1\,1\,1\,1\,1\,1) \\
\mathfrak{v}_1 & (0\,0\,0\,0\,1\,1\,1\,1) \\
\mathfrak{v}_2 & (0\,0\,1\,1\,0\,0\,1\,1) \\
\mathfrak{v}_3 & (0\,1\,0\,1\,0\,1\,0\,1) \\
\mathfrak{v}_1 \circ \mathfrak{v}_2 & (0\,0\,0\,0\,0\,0\,1\,1) \\
\mathfrak{v}_2 \circ \mathfrak{v}_3 & (0\,0\,0\,1\,0\,0\,0\,1) \\
\mathfrak{v}_1 \circ \mathfrak{v}_3 & (0\,0\,0\,0\,0\,1\,0\,1) \\
\mathfrak{v}_1 \circ \mathfrak{v}_2 \circ \mathfrak{v}_3 & (0\,0\,0\,0\,0\,0\,0\,1)
\end{array}$$

1.33 Definition. Es sei $n = 2^m$. Der lineare Teilraum C von $\mathbb{F}_2^{1n}$ mit der Basis $\mathfrak{v}_0$ und allen Produkten $\mathfrak{v}_{i_1} \circ \ldots \circ \mathfrak{v}_{i_j} (1 \leq i_1 < i_2 < \ldots < i_j \leq m; \quad j = 1, 2, \ldots, r \leq m)$ heit Reed-Muller-Code r-ter Ordnung der Länge n. (Hierfür ist $k = \binom{m}{0} + \binom{m}{1} + \ldots + \binom{m}{r}$.)

1.34 Satz. *Der duale Code zum Reed-Muller-Code r-ter Ordnung der Länge $n = 2^m$ ist der R-M-Code $(m - r - 1)$−ter Ordnung der Länge 2^m.*

Beweis. Es sei $n = 2^m, k = \binom{m}{0} + \binom{m}{1} + \ldots + \binom{m}{r}$. Der hierzu duale Code hat $n = 2^m, n - k = 2^m - \binom{m}{0} \ldots - \binom{m}{r} = \binom{m}{0} + \ldots + \binom{m}{m-r-1}$. Zu zeigen bleibt die Orthogonalität (für Basisvektoren): Dazu sei
$\mathfrak{a} = \mathfrak{v}_{i_1} \circ \ldots \circ \mathfrak{v}_{i_k}$ Basisvektor mit $k \leq r$,
$\mathfrak{b} = \mathfrak{v}_{j_1} \circ \ldots \circ \mathfrak{v}_{j_l}$ Basisvektor mit $l \leq m - r - 1$.
$\Longrightarrow \mathfrak{a} \circ \mathfrak{b}$ ist Basisvektor von $\mathbb{F}_2^{1n}$ mit Anzahl der Faktoren $0 \leq a \leq k + l \leq m - 1$
$\Longrightarrow wt(\mathfrak{a} \circ \mathfrak{b}) = 2^{m-a}$ gerade
$\Longrightarrow \mathfrak{a}\mathfrak{b}^{tr} = 0$ in $\mathbb{F}_2$
(Falls $\mathfrak{a} = \mathbf{1}$ oder $\mathfrak{b} = \mathbf{1}$ gilt, ist die Behauptung ohnehin klar!) □

Zur Entwicklung von Codierungs- bzw. Decodierungsmethoden sind wiederum einige Vorbereitungen erforderlich. Es sei $1 \leq i_1 < \ldots < i_s \leq m$. Dann definieren wir $C(i_1, \ldots, i_s) = \{j \in \{0, 1, \ldots, 2^m - 1\} \mid \xi_{ij} = 0 \quad \forall i \notin \{i_1, \ldots, i_s\}\}$ (Menge aller Indizes j von $\underline{x}_j \in \mathbb{F}_2^m$, in deren Basisdarstellung $\underline{x}_j = \sum_{i=1}^{m} \xi_{ij} \underline{u}_i$ auerhalb der Koordinaten $i_1, \ldots, i_s$ nur Nullen auftreten).

Beispiel:
$C(\oslash) = \{0\}$
$C(1, \ldots, m) = \{0, 1, \ldots, 2^m - 1\}$
$C(1) = \{0, 2^{m-1}\}$

Konkretes Beispiel $n = 8, m = 3$

$$\begin{aligned} C(\oslash) &= \{0\} \\ C(1) &= \{0,4\} \\ C(2) &= \{0,2\} \\ C(3) &= \{0,1\} \\ C(1,2) &= \{0,2,4,6\} \\ C(2,3) &= \{0,1,2,3\} \\ C(1,3) &= \{0,1,4,5\} \\ C(1,2,3) &= \{0,1,2,3,4,5,6,7\} \end{aligned}$$

Nun ist für $\mathfrak{a} \in \mathbb{F}_2^{1n}$:

$$\begin{aligned} \mathfrak{a} &= \sum_{j=0}^{n-1} \alpha_j \mathfrak{e}_j \quad (\alpha_j \in \mathbb{F}_2) \\ &= \sum_{j=0}^{n-1} \alpha_j \prod_{i=1}^{m} (\mathfrak{v}_i + (1+\xi_{ij})\mathfrak{v}_0) \\ &= \sum_{s=0}^{m} \sum_{1 \le i_1 < \ldots < i_s \le m} \kappa_{i_1,\ldots,i_s} \prod_{\nu=1}^{s} \mathfrak{v}_{i_\nu} \\ &= \sum_{s=0}^{m} \sum_{1 \le i_1 < \ldots < i_s \le m} \left(\sum_{j \in C(i_1,\ldots,i_s)} \alpha_j \right) \prod_{\nu=1}^{s} \mathfrak{v}_{i_\nu} \end{aligned}$$

($\mathfrak{v}_{i_1} \circ \ldots \circ \mathfrak{v}_{i_s}$ tritt genau dann in der Darstellung von $\mathfrak{e}_j$ auf, wenn $\xi_{ij} = 0$ für alle $i \notin \{i_1, \ldots, i_s\}$ ist.)

Damit bekommt man die folgenden Verfahren für Codierung bzw. Decodierung: Wähle feste Reihenfolge der Code-Basis. $(a_1, \ldots, a_k)$ seien die $k = \binom{m}{0} + \binom{m}{1} + \ldots + \binom{m}{r}$ Quell-Bits. Codiere $(a_1, \ldots, a_k) \mapsto a_1\mathfrak{v}_0 + a_2\mathfrak{v}_1 + \ldots + a_{m+1}\mathfrak{v}_m + a_{m+2}\mathfrak{v}_1 \circ \mathfrak{v}_2 + \ldots + a_k\mathfrak{v}_{m-r+1} \circ \ldots \mathfrak{v}_m = (f_0, \ldots, f_{n-1})$.

Induktiv: Zu jedem Quell-Bit a_s, welches als Koeffizient eines r-gliedrigen Produktes auftritt, lässt sich $\{0, 1, \ldots, 2^m - 1\}$ in 2^{m-r} disjunkte Teilmengen C von je 2^r Elementen aufspalten, so dass stets $a_s = \sum_{j \in C} f_j$ gilt.

Sei nun $\mathfrak{x} = (x_1, \ldots, x_n)$ der empfangene Vektor und a_s wie bisher. Falls kein Fehler auftritt, erhalten wir 2^{m-r} verschiedene Gleichungen $a_s = \sum_{j \in C} x_j$.
Falls $\mathfrak{x}$ daher weniger als $\frac{1}{2}2^{m-r}$ Fehler enthält, ist die Mehrzahl dieser Gleichungen noch gültig. Daher lässt sich a_s aus ihnen durch Mehrheitsentscheid bestimmen.
Nach Bestimmung der Koeffizienten aller r-gliedrigen Produkte wird die entsprechende Linearkombination von $\mathfrak{x}$ subtrahiert, man erhält eine Nachricht, die einem R-M-Code $(r-1)-$ter Ordnung angehört.

Durch iteriertes Anwenden erhält man schlielich die Botschaft.

Gleichzeitig haben wir gesehen, dass die Korrekturfähigkeit $2^{m-r-1}-1$ ist, dass heit $d \geq 2^{m-r}-1$ gilt. Alle Codeworte haben jedoch gerades Gewicht, und $\mathfrak{v}_{i_1} \circ \ldots \circ \mathfrak{v}_{i_r}$ hat Gewicht 2^{m-r}. Daraus erhalten wir unmittelbar

1.35 Satz. *Der R-M-Code r-ter Ordnung hat das Minimalgewicht 2^{m-r}.*

Bemerkung: Die Fehler-Korrektur ist besser, je kleiner r ist, dafür existieren jedoch auch viel weniger Codeworte ($k = \binom{m}{0} + \binom{m}{1} + \ldots + \binom{m}{r}$).

Die Decodierung erfolgt rekursiv, indem man zuerst die Koeffizienten der beteiligten r-gliedrigen Produkte bestimmt, dann der $(r-1)-$gliedrigen, usw. .

Sei also ein r-gliedriges Produkt $\mathfrak{v}_{i_1} \circ \ldots \circ \mathfrak{v}_{i_r}$ mit $1 \leq i_1 < \ldots < i_r \leq m$ gegeben mit Koeffizient a_s. Dann war ja $a_s = \sum\limits_{j \in C(i_1,\ldots,i_r)} f_j$.
Ist hingegen $t \in \{1,\ldots,m\} \backslash \{i_1,\ldots,i_r\}$, so gilt $\sum\limits_{j \in C(i_1,\ldots,i_r,t)} f_j = 0$, da in der Basisdarstellung keine $(r+1)-$gliedrigen Produkte auftreten.
Nun ist aber $C(i_1,\ldots,i_r,t) = C(i_1,\ldots,i_r) \dot\cup [2^{m-t} + C(i_1,\ldots,i_r)]$, also
$a_s = \sum\limits_{j \in C(i_1,\ldots,i_r)+2^{m-t}} f_j$. Entsprechend folgt aus

$$\begin{aligned} C(i_1,\ldots,i_r,t,u) &= C(i_1,\ldots,i_r,t) \dot\cup [2^{m-u} + C(i_1,\ldots,i_r,t)] \\ &= C(i_1,\ldots,i_r) \dot\cup [C(i_1,\ldots,i_r) + 2^{m-t}] \\ &\quad \dot\cup [2^{m-u} + C(i_1,\ldots,i_r)] \dot\cup [2^{m-u} + 2^{m-t} + C(i_1,\ldots,i_r)] \end{aligned}$$

dann $a_s = \sum\limits_{j \in 2^{m-t}+2^{m-u}+C(i_1,\ldots,i_r)} f_i$.

Beispiel: $n = 8, m = 3, r = 1 \Longrightarrow$ 1-Fehler korrigierend

$$\left.\begin{array}{rcl} \mathfrak{v}_0 &=& (1\ 1\ 1\ 1\ 1\ 1\ 1\ 1) \\ \mathfrak{v}_1 &=& (0\ 0\ 0\ 0\ 1\ 1\ 1\ 1) \\ \mathfrak{v}_2 &=& (0\ 0\ 1\ 1\ 0\ 0\ 1\ 1) \\ \mathfrak{v}_3 &=& (0\ 1\ 0\ 1\ 0\ 1\ 0\ 1) \end{array}\right\} \text{Basis von } C$$

Es werde $(a_0,a_1,a_2,a_3) = (0\ 1\ 1\ 0)$ gesendet $\quad (k = \binom{3}{0} + \binom{3}{1} = 4)$.

Codierung: $\mathfrak{v}_1 + \mathfrak{v}_2 = (0\ 0\ 1\ 1\ 1\ 1\ 0\ 0)$.
Empfangen werde $(00111000) = (x_0 \ldots x_7) = \mathfrak{x}$.
Decodierung:

$$\text{Best. von } a_3: \quad a_3 = \underset{\substack{j\in C(3)\\ 0,1\\ 0}}{\sum} x_j = \underset{\substack{j\in C(3)+2^1\\ 2,3\\ 0}}{\sum} x_j = \underset{\substack{j\in C(3)+2^2\\ 4,5\\ 1}}{\sum} x_j = \underset{\substack{j\in C(3)+2^2+2^1\\ 6,7\\ 0}}{\sum} x_j$$

$$\text{Best. von } a_2: \quad a_2 = \underset{\substack{j\in C(2)\\ 0,2\\ 1}}{\sum} x_j = \underset{\substack{j\in C(2)+2^2\\ 4,6\\ 1}}{\sum} x_j = \underset{\substack{j\in C(2)+2^0\\ 1,3\\ 1}}{\sum} x_j = \underset{\substack{j\in C(2)+2^2+2^0\\ 5,7\\ 0}}{\sum} x_j$$

$$a_1 = \underset{\substack{j\in C(1)\\ 0,4\\ 1}}{\sum} x_j = \underset{\substack{j\in C(1)+2\\ 2,6\\ 1}}{\sum} x_j = \underset{\substack{j\in C(1)+2^0\\ 1,5\\ 0}}{\sum} x_j = \underset{\substack{j\in C(1)+2^1+2^0\\ 3,7\\ 1}}{\sum} x_j$$

$\mathfrak{x} - \mathfrak{v}_1 - \mathfrak{v}_2 = \mathfrak{x} + \mathfrak{v}_1 + \mathfrak{v}_2 = (0\ 0\ 0\ 0\ 0\ 1\ 0\ 0)$.

Kapitel 2

Zyklische Codes

Neben der Vektorraum-Struktur von $\mathbb{F}_q^n$ wird jetzt auch die Körperstruktur ausgenutzt. Es sei $\mathbb{F}$ ein endlicher Körper mit $q = p^m$ Elementen, p Primzahl, also $p = \text{char } F$. Dann gelten

1. $\mathbb{F}^\times = \mathbb{F}\backslash\{0\}$ ist zyklisch, etwa $\mathbb{F}^\times =< \alpha >, \text{ord}(\alpha) = p^m - 1$.
2. $\forall x \in \mathbb{F}: \quad x^{p^m} = x; \quad t^{p^m} - t = \prod_{\alpha \in \mathbb{F}} (t - \alpha)$.
3. $\alpha \in \mathbb{F}$ heißt primitiv, falls $\mathbb{F}^\times = \{\alpha^i \mid i = 0, \ldots, p^m - 2\}$ gilt. Jedes $\mathbb{F}$ enthält primitive Elemente.
4. $(x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p$.

2.1 Definition. Ein Code $C \subset \mathbb{F}_q^n$ heißt zyklisch, wenn mit $\underline{x} = (x_1, \ldots, x_n)$ auch $\sigma\underline{x} = (x_n, x_1, \ldots, x_{n-1})$ Codewort ist.

Idee Zur Konstruktion eines 1-Fehler korrigierenden (Hamming-) Codes genügten m Prüf-Bits ($n = 2^m - 1$). Vermutung: Konstruktion eines τ-Fehler korrigierenden Codes mittels τm Prüf-Bits.

Untersuchung für $\tau = 2$ und $n = 2^{m-1}$.
Die Prüfmatrix von H_m enthält als Spalten die Dualdarstellungen $\underline{x}_1, \ldots, \underline{x}_{2^m-1}$ der Zahlen $1, \ldots, 2^{m-1}$ (in beliebiger Reihenfolge). Wir suchen nun eine Prüfmatrix

$$H = \begin{pmatrix} \underline{x}_1 \cdots \underline{x}_{2^m-1} \\ \underline{y}_1 \cdots \underline{y}_{2^m-1} \end{pmatrix} \text{ mit } 2m \text{ Zeilen.}$$

Da $\underline{x}_1, \ldots, \underline{x}_{2^m-1}$ verschieden sind, können wir $\underline{y}_1, \ldots, \underline{y}_{2^m-1}$ als Funktionswerte einer Funktion $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^m : \underline{x}_i \mapsto \underline{y}_i$ auffassen, indem wir zusätzlich $f(\underline{0}) = \underline{0}$ definieren. Entsprechend können wir auch die Syndromvektoren $\underline{s}$ in zwei Komponenten $\underline{s}_1, \underline{s}_2$ aus $\mathbb{F}_2^m$ aufspalten. Damit erhalten wir:
0-Fehler: $H\underline{z} = \underline{0} = \begin{pmatrix} \underline{0} \\ \underline{0} \end{pmatrix} = \begin{pmatrix} \underline{s}_1 \\ \underline{s}_2 \end{pmatrix}$;
1-Fehler in Position i: $\begin{pmatrix} \underline{x}_i \\ f(\underline{x}_i) \end{pmatrix} = \begin{pmatrix} \underline{s}_1 \\ \underline{s}_2 \end{pmatrix}$;

2-Fehler in Positionen $i \neq j$: $\begin{pmatrix} \underline{x}_i + \underline{y}_i \\ f(\underline{x}_i) + f(\underline{y}_i) \end{pmatrix} = \begin{pmatrix} \underline{s}_1 \\ \underline{s}_2 \end{pmatrix}$.
Damit der Code 2-Fehler korrigierend sein kann, darf das Gleichungssystem

$$\begin{matrix} \underline{u} + \underline{v} = \underline{s}_1 \\ f(\underline{u}) + f(\underline{v}) = \underline{s}_2 \end{matrix} \quad \forall \underline{s}_1, \underline{s}_2 \in \mathbb{F}_2^m$$

höchstens eine Lösung haben.

f linear geht dann nicht, denn sonst folgte $f(\underline{s}_1) = \underline{s}_2$ und für $\underline{u}_1 \neq \underline{u}_2$, $\underline{v}_1 \neq \underline{v}_2$ mit $\underline{u}_1 + \underline{v}_1 = \underline{u}_2 + \underline{v}_2$ würde das Gleichungssystem mit rechter Seite $(\underline{u}_1 + \underline{v}_1, f(\underline{u}_1 + \underline{v}_1))^t$ mindestens zwei verschiedene Lösungen besitzen!

Idee Betrachte $\mathbb{F}_2^m$ als Körper. Jede Funktion auf $\mathbb{F}_2^m$ ist Polynom vom Grad höchstens $2^m - 1$. Schreibe $\underline{x}_i = \alpha_i$ als Körperelement!

Ansatz $f(\alpha_i) = \alpha_i^3$ (erfüllt $f(0) = 0$). Bei genau zwei Fehlern in Positionen $i \neq j$ erhalten wir für die Syndrome $\alpha_i + \alpha_j = \sigma_1 \neq 0, \quad \alpha_i^3 + \alpha_j^3 = \sigma_2$. Es folgt

$$\begin{array}{rcl} \sigma_2 = \alpha_i^3 + \alpha_j^3 & = & (\alpha_i + \alpha_j)(\alpha_i^2 + \alpha_i\alpha_j + \alpha_j^2) \\ & = & \sigma_1(\sigma_1^2 + \alpha_i\alpha_j) = \sigma_1^3 + \sigma_1\alpha_i\alpha_j \\ \text{oder } \frac{\sigma_2}{\sigma_1} + \sigma_1^2 & = & \alpha_i\alpha_j. \text{ Wir bemerken } \sigma_1^3 \neq \sigma_2! \end{array}$$

Das heißt, α_i, α_j sind Wurzeln der Gleichung $x^2 + \sigma_1 x + \left(\frac{\sigma_2}{\sigma_1} + \sigma_1^2\right) = 0$.
(Treten keine Fehler auf, gilt $\sigma_1 = \sigma_2 = 0$; bei einem Fehler dagegen $\sigma_2 = \alpha_i^3 = \sigma_1^3$.)
Die Decodierung ist daher bei Syndromen $\underline{s} = \begin{pmatrix} \underline{s}_1 \\ \underline{s}_2 \end{pmatrix} = \begin{pmatrix} \sigma_1 \\ \sigma_2 \end{pmatrix}$ wie folgt möglich:

1. 0-Fehler: $\sigma_1 = \sigma_2 = 0$;
2. 1-Fehler: $\sigma_1 \neq 0, \sigma_2 = \sigma_1^3$; Fehler in Position $i = \sigma_1$.
3. 2-Fehler: $\sigma_1 \neq 0, \sigma_2 \neq \sigma_1^3$, bilde $x^2 + \sigma_1 x + \left(\frac{\sigma_2}{\sigma_1} + \sigma_1^2\right) = 0$. Enthält diese Gleichung 2 verschiedene Wurzeln α_i, α_j, korrigiere Fehler in Positionen i, j.
4. Besitzt $x^2 + \sigma_1 x + \left(\frac{\sigma_2}{\sigma_1} + \sigma_1^2\right) = 0$ keine Wurzeln, bzw. ist $\sigma_1 = 0 \neq \sigma_2$, so entdeckt man, dass mindestens drei Fehler aufgetreten sind.

Bemerkung $x^2 + \sigma_1 x + \left(\frac{\sigma_2}{\sigma_1} + \sigma_1^2\right) = 0$ kann keine Doppelwurzel für $\sigma_1 \neq 0$ besitzen!

Ergebnis $H = \begin{pmatrix} \alpha_1 \dots \alpha_{2^m-1} \\ \alpha_1^3 \dots \alpha_{2^m-1}^3 \end{pmatrix}$ ist Prüfmatrix eines 2-Fehler korrigierenden Codes der Länge $n = 2^m - 1$.
$\underline{x} = (x_1, \dots, x_n)^t$ ist Codewort $\Longleftrightarrow \sum_{i=1}^{n} \alpha_i x_i = \sum_{i=1}^{n} \alpha_i^3 x_i = 0$.
H besitzt $2m$ Zeilen, die nicht notwendig linear unabhängig sind. Die Dimension des Codes ist folglich $\geq n - 2m = 2^m - 1 - 2m$.

2.2 Satz. *Es seien $m \in \mathbb{N}, n = 2^m - 1$ sowie $\alpha_1, \ldots, \alpha_n$ eine (beliebige) Anordnung der Elemente des Körpers $\mathbb{F}_2^m \backslash \{0\}$. Für $\tau \in \mathbb{N}, \tau \leq 2^{m-1} - 1$, ist dann*

$$H = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^3 & \alpha_2^3 & \ldots & \alpha_n^3 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{2\tau-1} & \alpha_2^{2\tau-1} & \ldots & \alpha_n^{2\tau-1} \end{pmatrix}$$

Prüfmatrix eines linearen binären $[n, k]$-Codes C, der τ-Fehler korrigierend ist und die Dimension $k \geq n - m\tau$ besitzt.

Beweis. Gemäß Korollar (1.11) ist zunächst zu zeigen, dass in H je 2τ Spalten linear unabhängig sind. Wir wählen 2τ Spalten aus und bezeichnen diese, etwa $\alpha_{i_1}, \ldots, \alpha_{i_{2\tau}}$, mit $\beta_1, \ldots, \beta_{2\tau}$, die dann paarweise verschiedene Elemente von $\mathbb{F}_2^m$ bilden.
Dann ist der Spaltenrang der untersuchten Matrix
$A = \begin{pmatrix} \beta_1 & \ldots & \beta_{2\tau} \\ \beta_1^3 & & \beta_{2\tau}^3 \\ \vdots & & \vdots \\ \beta_1^{2\tau-1} & \ldots & \beta_{2\tau}^{2\tau-1} \end{pmatrix}$ gerade 2τ, falls die Spalten linear unabhängig sind, das heißt, falls für alle $\underline{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ gilt:

$$(\sum_{i=1}^{n} \beta_i^\nu x_i = 0 \text{ für } \nu = 1, 3, \ldots, 2\tau - 1 \Longrightarrow \underline{x} = \underline{0})$$

$\Longleftrightarrow (\sum_{i=0}^{n} \beta_i^\nu x_i = 0$ für $\nu = 1, \ldots, 2\tau - 1 \Longrightarrow \underline{x} = \underline{0})$ (Rechnen über $\mathbb{F}_2$!)
$\Longleftrightarrow \det((\beta_i^j)_{1 \leq i,j \leq 2\tau}) \neq 0.$
Es gilt hierfür

$$\begin{vmatrix} \beta_1 & \ldots & \beta_{2\tau} \\ \beta_1^2 & & \beta_{2\tau}^2 \\ \vdots & & \vdots \\ \beta_1^{2\tau} & \ldots & \beta_{2\tau}^{2\tau} \end{vmatrix} = (\beta_1 \ldots \beta_{2\tau}) \begin{vmatrix} 1 & \ldots & 1 \\ \beta_1 & & \beta_{2\tau} \\ \vdots & & \vdots \\ \beta_1^{2\tau-1} & \ldots & \beta_{2\tau}^{2\tau-1} \end{vmatrix}.$$

Die letzte Determinante ist dabei vom Vandermonde-Typ. Also gilt:

$$\det((\beta_i^j)) = \beta_1 \cdot \ldots \cdot \beta_{2\tau} \prod_{1 \leq i < j \leq 2\tau} (\beta_j - \beta_i) \neq 0.$$

Folglich ist C τ-Fehler korrigierend. H besitzt zudem $\tau \cdot m$ Zeilen; falls diese linear unabhängig sind, wird $\dim C = n - m\tau$, ansonsten größer. Damit ist Satz (2.2) bewiesen. □

Die Bedeutung dieser Codes liegt allerdings weniger in ihrer Eigenschaft, Fehler zu korrigieren; es gibt Codes mit besserem Verhältnis k/n und größerer Minimal-distanz der Codeworte. Dafür haben diese Codes hier hervorragende Codierungs- und Decodierungsverfahren.

2.3 Definition. Die Codes aus Satz (2.2) heißen Bose-Chaudhuri-Hocquenghem Codes (BCH-Codes).

In der Matrix H von Satz (2.2) stehen die Körperelemente $\alpha_1, \ldots, \alpha_n$ in beliebiger Reihenfolge. Eine Änderung der Reihenfolge führt zu einem äquivalenten Code. Für Codierungs- bzw. Decodierungszwecke sind bestimmte Anordnungen vorteilhaft.
Die Spalten der Matrix H von Satz (2.2) werden nun wie folgt angeordnet. Es sei α ein primitives Element von $\mathbb{F}_2^{m\times}$ sowie $\alpha_i = \alpha^{i-1}$. Dann ist $\underline{x} = (x_1, \ldots, x_n)$ genau dann ein Codewort, wenn

$$\sum_{i=1}^{n} x_i \alpha^{(i-1)\nu} = 0 \text{ für } \nu = 1, 3, \ldots, 2t-1 \text{ bzw. } \nu = 1, \ldots, 2t$$

gilt.

Bemerkung In dieser Notation sind BCH-Codes zyklisch. Es gilt nämlich:

$$\begin{aligned} 0 = \sum_{i=1}^{n} x_i \alpha^{(i-1)\nu} &= \alpha^{\nu} \sum_{i=1}^{n} x_i \alpha^{(i-1)\nu} \\ &= \sum_{i=1}^{n-1} x_i \alpha^{i\nu} + x_n \alpha^{n\nu} \\ &= \sum_{i=2}^{n} x_{i-1} \alpha^{(i-1)\nu} + x_n \alpha^{0} \\ &= \sum_{i=2}^{n} x_{i-1} \alpha^{(i-1)\nu} + x_n \alpha^{(1-1)\nu}. \end{aligned}$$

Wir ordnen nun jedem Codewort $(x_1, \ldots, x_n)^{tr}$ ein Polynom aus $\mathbb{F}_2[t]$ zu:

$$\mathbb{F}_2^n \longrightarrow \mathbb{F}_2[t] : (x_1, \ldots, x_n)^{tr} \mapsto x_1 + x_2 t + \ldots + x_n t^{n-1}.$$

Damit lässt sich der Code als Menge von Polynomen vom Grad höchstens $(n-1)$ im Polynomring $\mathbb{F}_2[t]$ auffassen. Ein Polynom $f(t) \in \mathbb{F}_2[t]$ ist genau dann Codewort, wenn $\deg(f) \leq n-1$ und $f(\alpha^\nu) = 0$ für $\nu = 1, \ldots, 2\tau$ gilt.

Wir erinnern an Aussagen der Algebra, speziell an Eigenschaften von Polynomringen über Körpern F:

1. $F[t]$ ist Euklidischer Ring, folglich Hauptidealring.
2. Ein Ideal in $F[t]$ ist genau dann maximal, wenn sein erzeugendes Polynom irreduzibel ist.
3. Ist R kommutativer Ring mit Eins und $\mathfrak{a}$ ein Ideal in R, so gilt:
   $R/\mathfrak{a}$ Körper $\Longleftrightarrow$ $\mathfrak{a}$ maximal.

2.4 Satz. *Es sei $\mathfrak{M}$ die Menge aller Polynome $f(t) \in \mathbb{F}_2[t]$ mit $\deg(f) \leq n-1$ und $f(\alpha^\nu) = 0 \quad (\nu = 1, \ldots, 2\tau)$. Dann existiert (eindeutig) $g(t) \in \mathbb{F}_2[t]$ normiert mit: $f(t) \in \mathfrak{M} \Longleftrightarrow \left\{ \begin{array}{l} (1) f(t) \in g(t)\mathbb{F}_2[t] \\ (2) \deg(f) \leq n-1 \end{array} \right\}$.*
Dieses Polynom $g(t)$ heißt erzeugendes Polynom des entsprechenden BCH-Codes.

Beweis. $\tilde{\mathfrak{M}} := \{f(t) \in \mathbb{F}_2[t] \mid f(\alpha^\nu) = 0 \quad (\nu = 1, \ldots, 2t)\}$ ist ein Ideal in $\mathbb{F}_2[t]$, also Hauptideal, etwa $\tilde{\mathfrak{M}} =< g(t) >$.
Die Eindeutigkeit von $g(t)$ wird durch die Forderung "$g(t)$ normiertërreicht. □

2.5 Korollar. *Die Dimension des entsprechenden BCH-Codes ist* $k = n - \deg(g)$.

Beweis. $f(t) \in g(t)\mathbb{F}_2[t] \iff f(t) = g(t)h(t)$ mit $h(t) \in \mathbb{F}_2[t]$. Ist nun $\deg(f) \leq n-1$, so gilt auch $\deg(gh) = \deg(g) + \deg(h) \leq n-1$, also $\deg(h) \leq n - 1 - \deg(g) \stackrel{!}{=} k - 1$, das heißt $h(x) = \alpha_0 + \alpha_1 t + \ldots + \alpha_k t^{k-1} \in \mathbb{F}_2[t]$; es gibt also 2^k Möglichkeiten für die Wahl von k. □

Bemerkung Offenbar lässt sich $g(t)$ normiert wählen. $g(t)$ ist damit dasjenige normierte Polynom kleinsten Grades, welches $\alpha^\nu \quad (\nu = 1, \ldots, 2\tau)$ bzw.
$\alpha^1, \alpha^3, \ldots, \alpha^{2\tau-1}$ als Nullstellen besitzt.

Aus der Algebra-Vorlesung gilt als bekannt ($\mathbb{F} = \mathbb{F}_p^m$):

1. Das Minimalpolynom von $\alpha \in \mathbb{F}$ über $\mathbb{F}_p$ ist dasjenige normierte Polynom $m_\alpha t = m_{\alpha/\mathbb{F}_p}(t)$ kleinsten Grades aus $\mathbb{F}_p[t]$, welches α als Nullstelle besitzt.

2. Eigenschaften von $m_\alpha(t)$ als Minimalpolynom von α: $m_\alpha(t)$ ist irreduzibel in $\mathbb{F}_p[t]$. Für jedes $f(t) \in \mathbb{F}_p[t]$ mit $f(\alpha) = 0$ gilt $m_\alpha(t)$ teilt; $f(t)$ in $\mathbb{F}_p[t] : m_\alpha(t) \mid f(t)$. Speziell folgt: $m_\alpha(t) \mid (t^{p^m} - t)$. Es gilt: $\deg(m_\alpha) \leq m$, denn $1, \alpha, \ldots, \alpha^{m-1}$, α^m sind linear abhängig wegen $[\mathbb{F} : \mathbb{F}_p] = m$.

3. Ist α primitiv, so gilt $\deg(m_\alpha) = m$. (m_α heißt in diesem Fall primitives Polynom). Gilt etwa $\deg(m_\alpha) = d$, so erzeugt α einen Oberkörper von $\mathbb{F}_p$ mit p^d Elementen. Wegen $\alpha \in \mathbb{F}$ folgt $p^d \leq p^m$, also $d \leq m$. (Man beachte: $\mathbb{F}_p(\alpha) \cong \mathbb{F}_p[t]/_{m_\alpha(t)\mathbb{F}_p[t]}$ ist ein Körper mit $p^{\deg(m_\alpha)}$ vielen Elementen.)

4. Ist α Nullstelle von $f(t) \in \mathbb{F}_p[t]$, so gilt auch $f(\alpha^p) = 0$; denn in Charakteristik p gilt: $f(\alpha^p) = (f(\alpha))^p$. Das Minimalpolynom eines Elementes α enthält damit die Nullstellen $\alpha^{p^\nu} (\nu \in \mathbb{Z}^{\geq 0}, \quad \nu < \deg(m_\alpha))$, die sogenannten Konjugierten von α. Aus der Galoistheorie folgt schließlich $m_\alpha(t) = \prod_{i=0}^{m-1} (t - \alpha^{p^i})$ für α primitiv.

5. Es sei $\mathbb{F}_q$ ein Körper mit $q = p^m$ Elementen, p Primzahl. Dann ist $x^{q^n} - x$ für $n \in \mathbb{N}$ das Produkt aller normierten irreduziblen Polynome aus $\mathbb{F}_q[x]$, deren Grad n teilt.

6. Zu $n \in \mathbb{N}$ existieren stets irreduzible Polynome vom Grad n in $\mathbb{F}_q$.

Beispiel Wir betrachten den BCH-Code der Länge 7, also $n = 7, m = 3$, mit $\tau = 2$. Es sei α eine primitive Wurzel in $\mathbb{F}_2^3$. Dann ist $g(t)$ das Produkt der Minimalpolynome m_α und m_{α^3}, denn die Konjugierten sind hier $\alpha, \alpha^2, \alpha^4$ bzw. $\alpha^3, \alpha^6, \alpha^5$, das heißt, wir erhalten $g(t) = \prod_{i=1}^{6}(t - \alpha^i) = \frac{t^7-1}{t-1} = t^6 + t^5 + t^4 + t^3 + t^2 + t + 1$. Das bedeutet gemäß Korollar (**??**) dann $k = 1$, die Schranke in Satz

(2.2) ($k \geq n - m\tau$) ist in diesem Fall scharf. Dies ist jedoch nicht immer so. Ein Gegenbeispiel ist: $m = 4, \tau = 3$; wir erhalten hier $k = 5$ (statt 3 aus dem Satz).

Um $g(t)$ aus der Produktdarstellung ($kgV(!)$ der Minimalpolynome von α^{2i-1} für $i = 1, \ldots, t$) zu realisieren, benötigt man zunächst eine Gleichung für α. Im letzten Fall ist $m_\alpha(t)$ irreduzibles Polynom vom Grad 4. Wir wählen $t^4 + t + 1$ (andere Möglichkeit: $t^4 + t^3 + 1$). Dann sind die Elemente von $\mathbb{F}_2^4$ einerseits Potenzen von α, andererseits - wegen $\alpha^4 = \alpha + 1, \quad \mathbb{F}_2^4 \cong \mathbb{F}_2[t]/(t^4 + t + 1)\mathbb{F}_2[t]$ -Polynome höchstens dritten Grades in α. Im Einzelnen ist

$$
\begin{array}{lcccccccccc}
\alpha^0 & = & & & & & & & & & 1 \\
\alpha^1 & = & & & & & & & \alpha & & \\
\alpha^2 & = & & \alpha^2 & & & & & & & \\
\alpha^3 & = & \alpha^3 & & & & & & & & \\
\alpha^4 & = & & & & & & \alpha & + & 1 \\
\alpha^5 & = & & & \alpha^2 & + & \alpha & & & & \\
\alpha^6 & = & \alpha^3 & + & \alpha^2 & & & & & & \\
\alpha^7 & = & \alpha^3 & & & & + & \alpha & + & 1 \\
\alpha^8 & = & & & \alpha^2 & & & & + & 1 \\
\alpha^9 & = & \alpha^3 & & & + & \alpha & & & & \\
\alpha^{10} & = & & & \alpha^2 & + & \alpha & & + & 1 \\
\alpha^{11} & = & \alpha^3 & + & \alpha^2 & + & \alpha & & & & \\
\alpha^{12} & = & \alpha^3 & + & \alpha^2 & + & \alpha & & + & 1 \\
\alpha^{13} & = & \alpha^3 & + & \alpha^2 & & & & + & 1 \\
\alpha^{14} & = & \alpha^3 & & & & & & + & 1 \\
\alpha^{15} & = & & & & & & & & & 1.
\end{array}
$$

Um in $\mathbb{F}_2^4$ sinnvoll zu rechnen, benötigt man beide Darstellungen, die Potenzen zum Multiplizieren, die vektorielle Darstellung für die Addition. Das Minimalpolynomm von α war $t^4 + t + 1$. Das Minimalpolynom von α^3 sei $t^4 + at^3 + bt^2 + ct + d$. Wegen α^3 Nullstelle muss $(\alpha^3 + \alpha^2 + \alpha + 1) + a(\alpha^3 + \alpha) + b(\alpha^3 + \alpha^2) + c\alpha^3 + d = 0$ gelten, das heißt $1 + a + b + c = 0, 1 + b = 0 \quad 1 + a = 0, 1 + d = 0$. Wir erhalten $m_{\alpha^3}(t) = t^4 + t^3 + t^2 + t + 1$. Das Minimalpolynom von α^5 hat die Nullstellen α^5, α^{10}. Wir erhalten

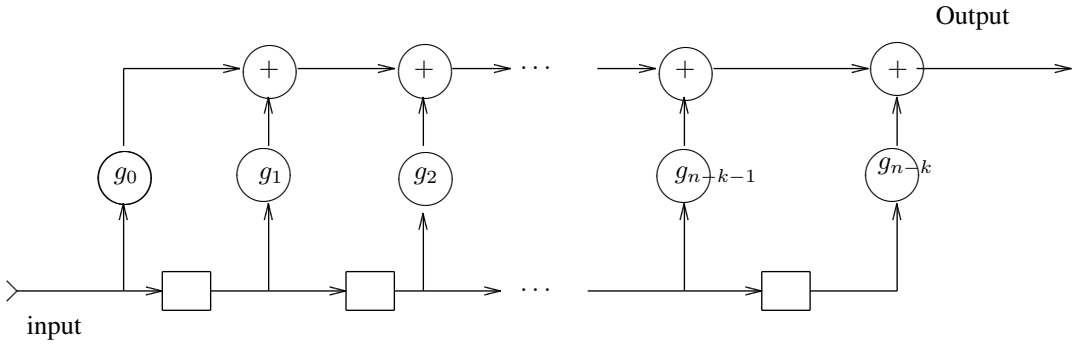
$$
\begin{aligned}
m_{\alpha^5}(t) &= t^2 + (\alpha^5 + \alpha^{10})t + \alpha^5\alpha^{10} \\
&= t^2 + t + 1.
\end{aligned}
$$

Damit ist das erzeugende Polynom $g(t) = m_\alpha(t)m_{\alpha^3}(t)m_{\alpha^5}(t) = t^{10} + t^8 + t^5 + t^4 + t^2 + t + 1$ vom Grad 10. (Folglich hat das Polynom $t^4 + t^3 + 1 \in \mathbb{F}_2[t]$ die Nullstellen $\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$.) Das erzeugende Polynom hängt natürlich im Allgemeinen von der Wahl der primitiven Wurzel α ab.

Codierungsverfahren für BCH-Codes:
Gemäß Satz (**??**) werden k Nachrichtenbits $u_1, \ldots, u_k$ als Polynom $u_1 + u_2t + \ldots + u_kt^{k-1}$ interpretiert und mit dem erzeugenden Polynom $g(t) = kgV\{m_{\alpha^{2i-1}} \mid i = 1, \ldots, \tau\})$ multipliziert. Man erhält dann ein Polynom vom Grad höchstens $n-1$: $\quad x_1 + x_2t + \ldots + x_nt^{n-1}$, dessen Koeffizienten

das Codewort $(x_1, \ldots, x_n)$ bilden.
Polynom-Arithmetik lässt sich in der Praxis besonders effizient mit digitalen Shift-Registern durchführen. Zunächst benötigen wir ein Verfahren zur Multiplikation mit einem konstanten Polynom $g(t)$.

Polynommultiplikation mit Shift-Registern



Takt 0: Input: I_0
Shift-Register: $[0, \ldots, 0]$
Output: $I_0 g_0$

Takt 1: Input: I_1
Shift-Register: $[I_0, 0, \ldots, 0]$
Output: $I_0 g_1 + I_1 g_0$

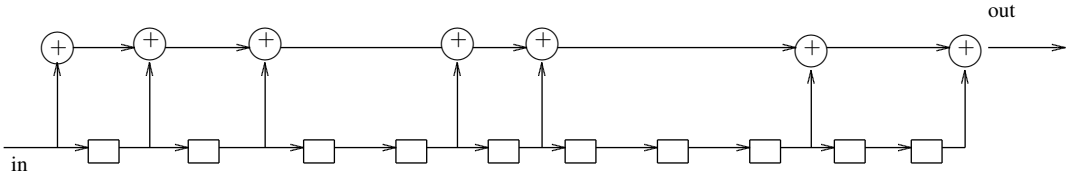
$\vdots$

Takt j: Input: I_j
Shift-Register: $[I_{j-1}, \ldots, I_1, I_0, 0, \ldots, 0]$
Output: $I_0 g_j + I_1 g_{j-1} + \ldots + I_j g_0$

$\vdots$

Takt $n-1$: Input: 0
Shift-Register: $[0, \ldots, 0, I_{k-1}]$
Output: $I_{k-1} g_{n-k}$

Über $\mathbb{F}_2$ gestaltet sich das Verfahren noch sehr viel effizienter, da eine Multiplikation als Resultat nur 0 oder 1 hat.
Wir erhalten als Encoder für $g(t) = t^{10} + t^8 + t^5 + t^4 + t^2 + t + 1$:



Der Euklidische Algorithmus für Polynome
Ausgehend von $r_0, r_1 \in F[t]$ (F beliebiger Körper) bestimmt der Euklidische Algorithmus den

ggT von r_0 und r_1.

Ein Rechenschritt besteht dabei jeweils aus einer Division mit Rest: $r_0(t) = q_1(t)r_1(t) + r_2(t)$ mit dem Quotientenpolynom q_1 und dem Rest r_2, für den $r_2 = 0$ oder $\deg(r_2) < \deg(r_1)$ gilt. $r_2(t)$ lässt sich dann seinerseits berechnen mittels

$$r_2(t) = \quad r_0(t) - q_1(t)r_1(t).$$

Nächster Schritt:

$$\begin{aligned} r_1(t) &= q_2(t)r_2(t) + r_3(t), \\ r_3(t) &= \quad r_1(t) - q_2(t)r_2(t) \\ &= r_1(t) - q_2(t)(r_0(t) - q_1(t)r_1(t)) \\ &= -q_2(t)r_0(t) + (1 + q_1(t)q_2(t)r_1(t)). \end{aligned}$$

Allgemein setzen wir an:

$$\begin{aligned} r_i(t) &= q_{i+1}(t)r_{i+1}(t) + r_{i+2}(t) \\ r_{i+2}(t) &= s_{i+2}(t)r_0(t) + t_{i+2}(t)r_1(t). \end{aligned}$$

Wir erhalten so (abbrechende) Folgen von Polynomen $r_i \quad (i \geq 0), \quad q_j \quad (j \geq 1), s_i, t_i$. Die Berechnung der r_i, q_j ist klar. Wie bestimmen sich aber die s_i, t_i? Zunächst gelten
$s_0(t) = 1, t_0(t) = 0, s_1(t) = 0, t_1(t) = 1$. So dann erhalten wir

$$\begin{aligned} s_{i+2}(t) &= s_i(t) - q_{i+1}(t)s_{i+1}(t) \\ t_{i+2}(t) &= t_i(t) - q_{i+1}(t)t_{i+1}(t) \end{aligned} \quad \left(\begin{array}{c} \text{2 gliedrige} \\ \text{Rekursion} \end{array} \right).$$

Für die Grade der Polynome r_i gilt: $\deg(r_i) > \deg(r_{i+1}) \quad (i \geq 1)$, so dass ein $n \in \mathbb{N}$ mit $r_n(t) \neq 0$ und $r_{n+1}(t) = 0$ existiert. Danach bricht der Prozess ab, da r_n nicht mehr durch r_{n+1} geteilt werden kann, so dass ein Rest von kleinerem Grad herauskommt.

2.6 Satz. *1.* $t_i(t)r_{i-1}(t) - t_{i-1}(t)r_i(t) = (-1)^{i+1}r_0(t) \quad (i = 1, \ldots, n+1)$;

2. $s_i(t)r_{i-1}(t) - s_{i-1}(t)r_i(t) = (-1)^i r_1(t) \quad (i = 1, \ldots, n+1)$;

3. $s_i(t)t_{i-1}(t) - s_{i-1}(t)t_i(t) = (-1)^i \qquad (i = 1, \ldots, n+1)$;

4. $s_i(t)r_0(t) + t_i(t)r_1(t) = r_i(t) \quad (i = 0, \ldots, n+1)$;

5. $\deg(s_i) + \deg(r_{i-1}) = \deg(r_1) \qquad (i = 2, \ldots, n+1)$;

6. $\deg(t_i) + \deg(r_{i-1}) = \deg(r_0) \qquad (i = 1, 3, \ldots, n+1)$.

Beweis. 1. $i = 1: \quad 1 \cdot r_0(t) - 0 \cdot r_1(t) = r_0(t)$.
$i \longrightarrow i+1 : t_{i+1}(t)r_i(t) - t_i(t)r_{i+1}(t)$

$$\begin{aligned} &= (t_{i-1}(t) - q_i(t)t_i(t))r_i(t) - t_i(t)r_{i+1}(t) \\ &= t_{i-1}(t)r_i(t) - t_i(t)(q_i(t)r_i(t) + r_{i+1}(t)) \\ &= t_{i-1}(t)r_i(t) - t_i(t)r_{i-1}(t) \\ &= (-1) \ (-1)^{i+1}r_0(t). \end{aligned}$$

2. Analog!

3. $i = 1 : 0 \cdot 0 - 1 \cdot 1 = -1$.
   $i \longrightarrow i+1 : s_{i+1}(t)t_i(t) - s_i(t)t_{i+1}(t)$
   $= \quad (s_{i-1}(t) - q_i(t)s_i(t))t_i(t) - s_i(t)(t_{i-1}(t) - q_i(t)t_i(t))$
   $= \quad s_{i-1}(t)t_i(t) - q_i(t)s_i(t)t_i(t) - s_i(t)t_{i-1}(t) + s_i(t)q_i(t)t_i(t)$
   $= \quad (-1) \ \ (-1)^i$.

4. Klar nach Konstruktion.

5. $i = 2 : \quad s_1(t) = 0 \quad (s_2(t) = 1)$.
   $\deg(s_{i+1}) > \deg(s_i) \quad (i \geq 1$ infolge Rekursion, $\deg(q_{i+1}) \geq 1)$
   $\deg(r_{i+1}) < \deg(r_i) \quad (i \geq 1$ infolge Definition der $r_i)$
   Gradbetrachtung in (2) liefert dann die Behauptung.

6. $i = 1 : \quad t_0 = 0$.
   $\deg(t_{i+1}) > \deg(t_i) \quad (i \geq 2$ infolge Rekursion, $\deg(q_i) \geq 1, \quad q_1 = 0$ möglich);
   $\deg(r_{i+1}) < \deg(r_i) \quad (i \geq 1$ infolge ihrer Definition);
   Gradbetrachtung in (1) liefert dann die Behauptung für $i \geq 3$.
   Es bleibt der Fall $i = 2$: Hier ist $t_2 = q_1$ und $\deg(r_1) > \deg(r_2)$.
   (Wir haben hier $t_2(t)r_1(t) - r_2(t) = -r_0(t)$.)
   Im Fall $t_2 \neq 0$ folgt also die Behauptung, für $t_2 = 0$ wäre sie ohnehin falsch.

□

2.7 Korollar. $r_n(t) = c\,\mathrm{ggT}(r_0(t), r_1(t)), \quad 0 \neq c \in F$ *mit*
$r_n(t) = s_n(t)r_0(t) + t_n(t)r_1(t)$.

Beweis. Die zweite Aussage Teil ist Punkt (4) des vorrangehenden Satzes. Wegen $r_{n+1}(t) = 0$ gilt $r_n(t) \mid r_{n-1}(t)$ und damit gemäß Konstruktion der $r_i(t) \quad (i = 0, 1, \ldots, n{+}1)$ auch $r_n(t) \mid r_i(t) \quad (i \leq n)$.
Ist umgekehrt $\pi(t)$ ein Teiler von $r_0(t), r_1(t)$, so teilt $\pi(t)$ auch $r_2(t)$, damit dann $r_i(t) \quad (i \geq 2)$. Also: $r_n(t)$ teilt $\mathrm{ggT}(r_0(t), r_1(t))$ und umgekehrt.

Entscheidend ist Punkt (4) des letzten Satzes. Aus jener Gleichung folgt

$$(\alpha) \quad t_i(t)r_1(t) \equiv r_i(t) \mod r_0(t) \quad (i = 0, \ldots, n).$$

Wegen 6. gilt darüber hinaus

$$(\beta) \quad \deg(t_i) + \deg(r_i) < \deg(r_0).$$

(Letzteres gilt sicher für $i \geq 3$. Für $i = 2$ gilt es auch, falls $r_2 \neq 0$ ist. Für $i = 1$ gilt dies nur im Fall $\deg(r_1) < \deg(r_0)$. Für $i = 0$ gilt es wiederum stets.) □

Im folgenden werden wir zeigen, dass die Polynome t_i, r_i durch die letzten beiden Eigenschaften bereits bis auf einen Faktor eindeutig gekennzeichnet sind. Sie lassen sich daher mittels des Euklidischen Algorithmus leicht bestimmen. Dies wird der entscheidende Punkt für das Decodierungsverfahren für BCH-Codes werden.

Beispiel $F = \mathbb{F}_2$.

i	s_i	t_i	r_i	q_i
0	1	0	t^8	$-$
1	0	1	$t^6+t^4+t^2+t+1$	t^2+1
2	1	t^2+1	t^3+t+1	t^3+1
3	t^3+1	$t^5+t^3+t^2$	t^2	t
4	t^4+t+1	$t^6+t^4+t^3+t^2+1$	$t+1$	$t+1$
$n=5$	$t^5+t^4+t^3+t^2$	$t^7+t^6+t^3+t+1$	1	$t+1$
6	$*$	$*$	0	$-$

Insbesondere ist also

$$(t^5+t^4+t^3+t^2)t^8 + (t^7+t^6+t^3+t+1)(t^6+t^4+t^2+t+1) = 1.$$

2.8 Hilfssatz. *Zu $\mu, \nu \in \mathbb{Z}^{\geq 0}$ mit $\nu \geq \deg(\mathrm{ggT}(r_0(t), r_1(t)))$ und $\mu + \nu = \deg(r_0(t)) - 1$ existiert eindeutig $j \in \{1, \ldots, n\}$ mit $\deg(t_j) \leq \mu, \quad \deg(t_j) \leq \nu$.*

Beweis. Es gilt $\deg(r_i) < \deg(r_{i-1}) \quad (i = 2, \ldots, n)$. Definiere j eindeutig durch die beiden Bedingungen $\deg(r_{j-1}) \geq \nu + 1, \deg(r_j) \leq \nu$. Es bleibt noch $\deg(t_j) \leq \mu$ zu zeigen. Gemäß Teil 6. des Satzes (2.6) war aber

$$\begin{aligned} 1 + \mu + \nu = \deg(r_0) &= \deg(t_j) + \deg(r_{j-1}) \\ &\geq \deg(t_j) + \nu + 1, \end{aligned}$$

woraus $\deg(t_j) \leq \mu$ folgt. (Ebenso ergibt sich $\deg(t_{j+1}) \geq \mu + 1$.)

□

2.9 Haupthilfssatz. *Es seien $f, g \in \mathbb{F}[t]$ mit $\deg(f) \geq 0, \deg(g) \geq 0$ gegeben. Für $u, r \in F[t]$ mit $u \cdot r \neq 0$ und $u(t)g(t) \equiv r(t) \mod f(t), \quad \deg(u) + \deg(r) < \deg(f)$ existieren eindeutig $j \in \mathbb{N}$ und $\lambda \in F[t]$ mit $u(t) = \lambda(t)t_j(t), r(t) = \lambda(t)r_j(t)$, wobei sich t_j, r_j aus dem Divisionsalgorithmus für f, g berechnen.*

Beweis. Setze $\nu = \deg(r), \quad \mu = \deg(f) - \nu - 1$. (Hierfür ist $\nu \geq \deg(\mathrm{ggT}(f(t), g(t)))$, da wegen $u(t)g(t) - r(t) = v(t)f(t)$ der ggT von f und g gerade r teilt. Wegen $\deg(u) + \nu < \deg(f)$ und $u \neq$ folgt $\mu \geq 0$.) Wir bestimmen daher gemäß dem Hilfssatz den Index j aus dem Divisionsalgorithmus für f und g eindeutig (!), so dass
$\deg(t_{j+1}) \geq \mu + 1 = \deg(f) - \nu = \deg(f) - \deg(r) \geq \deg(u) + 1$,
$\deg(r_{j-1}) \geq \nu + 1 = \deg(r) + 1$ gilt.
Damit ist die Eindeutigkeit des Index j gezeigt.

Gemäß Teil 4. des Satzes (2.6) und der Voraussetzung gilt für $j \geq 0$:
$s_j(t)f(t) + t_j(t)g(t) = r_j(t)$ und $\exists s(t) \in F[t]$

$$s(t)f(t) + u(t)g(t) = r(t). \tag{2.10}$$

Hieraus folgt
$s_j(t)f(t)u(t) + t_j(t)u(t)g(t) = r_j(t)u(t)$
$s(t)f(t)t_j(t) + t_j(t)u(t)g(t) = r(t)t_j(t)$,
also $r_j(t)u(t) \equiv r(t)t_j(t) \mod f(t)$.
Gradvergleich:
$\deg(r_j u) = \deg(r_j) + \deg(u) \leq \nu + \deg(u) \qquad = \deg(r) + \deg(u) < \deg(f)$,
$\deg(rt_j) = \deg(r) + \deg(t_j) \leq \nu + \mu < \deg(f)$.
Also muss
$r_j(t)u(t) = r(t)t_j(t)$ gelten, und damit auch
$s_j(t)u(t) = s(t)t_j(t)$.
Nach Teil 3. des Satzes (2.6) sind s_j und t_j jedoch prim zueinander, woraus sich $s(t) = \lambda(t)s_j(t)$ und $u(t) = \lambda(t)t_j(t)$ für ein $\lambda \in F[t]$ ergibt.

Es folgt aus (2.10) so dann
$r(t) = \lambda(t)s_j(t)f(t) + \lambda(t)t_j(t)g(t) = \lambda(t)r_j(t)$, also ist $\lambda(t) = \frac{r(t)}{r_j(t)}$ ebenfalls eindeutig bestimmt.
□

Fortsetzung des Beispiels: Annahme (wie bei der Decodierung später der Fall), wir suchen alle Polynome $u(t), r(t)$ mit $(t^6 + t^4 + t^2 + t + 1)u(t) \equiv r(t) \mod t^8$ und $\deg(u) \leq 3, \quad \deg(r) \leq 4$. Der kleinste Index j mit $\deg(r_j) \leq 4$ ist $j = 2$. Folglich sind alle $(\deg(r_j) \leq \nu = \deg(r))$ gesuchten Lösungen von der Form $u(t) = \lambda(t)(t^2 + 1), \quad r(t) = \lambda(t)(t^3 + t + 1)$ mit Polynomen λ vom Grad ≤ 1. Sollen u, r zudem zueinander prim sein, ist notwendig $\lambda(t) = 1$.

Decodierung von BCH-Codes:
$\underline{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ Codewort
$\iff \sum_{i=1}^{n} x_i \alpha_i^j = 0 \ (j = 1, \ldots, 2\tau, \quad \{\alpha_1, \ldots, \alpha_n\} = \mathbb{F}_2^m \backslash \{0\})$.

Es erweist sich jedoch als günstiger, die Elemente von $\mathbb{F}_2^{m\times}$ so anzuordnen, dass $\underline{x} \in C \iff \sum_{i=1}^{n} x_i \alpha_i^{-j} \quad (j = 1, \ldots, 2\tau)$ gilt.

Für einen beliebigen Vektor $\underline{y} \in \mathbb{F}_2^n$ definieren wir $s_j := \sum_{i=1}^{n} y_i \alpha_i^{-j} \quad (j = 1, \ldots, 2\tau)$.
Dann ist $\underline{y}$ genau dann Codewort, wenn $s(t) := s_1 + s_2 t + \ldots + s_{2\tau} t^{2\tau-1} \in \mathbb{F}_2^m[t]$ identisch verschwindet. Nun ist

$$\begin{aligned} s(t) &= \sum_{j=1}^{2\tau} t^{j-1}\left(\sum_{i=1}^{n} y_i \alpha_i^{-j}\right) = \sum_{i=1}^{n} y_i \sum_{j=1}^{2\tau} t^{j-1}\alpha_i^{-j} \\ &= \sum_{i=1}^{n} y_i \frac{t^{2\tau}\alpha_i^{-2\tau}-1}{t-\alpha_i}. \end{aligned}$$

Damit bekommt man als äquivalente Definition für BCH-Codes:
$\underline{y} \in \mathbb{F}_2^n$ Codewort $\iff \sum_{i=1}^{n} \frac{y_i}{t-\alpha_i} \equiv 0 \mod t^{2\tau}$ in $\mathbb{F}_2^m[t]$.
(Die letzte Kongruenz ist dabei als Gleichheit in $R = \mathbb{F}_2^m[t]/t^{2\tau}\mathbb{F}_2^m[t]$ zu interpretieren. Wegen $\mathrm{ggT}(t-\alpha_i, t^{2\tau}) = 1$ existiert $\frac{1}{t-\alpha_i}$ in R.)
Diese Definition für einen Code lässt sich leicht verallgemeinern:

2.11 Definition. Es seien $n, m \in \mathbb{N}$ und $G(t) \in \mathbb{F}_q^m[t]$ mit $\deg(G) = s, \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_q^m$ mit $G(\alpha_i) \neq 0 \quad (i = 1, \ldots, n)$. Dann bilden die Elemente $\underline{y} \in \mathbb{F}_q^n$ mit
$\sum_{i=1}^{n} \frac{y_i}{t-\alpha_i} \equiv 0 \mod G(t)$ einen linearen (!) Code, den sogenannten Goppa - Code.

2.12 Satz. *Der lineare Code in Definition (2.11) genügt* $d_{\min} \geq s+1$ *und* $k \geq n - ms$.

Beweis. Die Linearität ist klar! Also gilt: $d_{\min} = w_C$.

Es sei $\underline{0} \neq \underline{y}$ Codewort mit $\{j_1, \ldots, j_r\} = \{i \mid y_i \neq 0\}$. Setzte $\{\beta_1, \ldots, \beta_r\} = \{\alpha_{j_1}, \ldots, \alpha_{j_r}\}$.
Dies impliziert $\sum_{i=1}^{r} \frac{y_{j_i}}{t-\beta_i} \equiv 0 \mod G(t)$. Die linke Seite hiervon lässt sich auf den Hauptnenner $q(t) := \prod_{i=1}^{r}(t-\beta_i)$ bringen. Der zugehörige Zähler ist dann $p(t) = \sum_{i=1}^{r} y_{j_i} \prod_{\substack{k=1 \\ k\neq i}}^{r}(t-\beta_k)$.
Da $G(\beta_i) \neq 0$ ist, folgt $\mathrm{ggT}(G(t), q(t)) = 1$. Ferner ist $p(\beta_i) = y_{j_i} \prod_{k\neq i}(\beta_i - \beta_k) \neq 0$, also $\mathrm{ggT}(q(t), p(t)) = 1$. Daher ist wegen $\frac{p(t)}{q(t)} \equiv 0 \mod G(t)$ auch $p(t) \equiv 0 \mod G(t)$. Es folgt $s = \deg(G) \leq \deg(p) \leq r-1$ und damit $w_C \geq s+1$.

Nun zum Beweis von $k \geq n - ms$!
Wegen $-(t-\alpha_i)\frac{G(t)-G(\alpha_i)}{t-\alpha_i}G(\alpha_i)^{-1} \equiv 1 \mod G(t)$ gilt
$\frac{1}{t-\alpha_i} = -\frac{G(t)-G(\alpha_i)}{t-\alpha_i}G(\alpha_i)^{-1}$(in $R = \mathbb{F}_q[t]/G(t)\mathbb{F}_q[t]$)

$= : G_i(t)$ mit $\deg(G_i) \leq s-1$.
Dann liefert die Definition des Goppa-Codes für ein Codewort $\underline{y}$:
$\sum_{i=1}^{n} y_i G_i(t) \equiv 0 \mod G(t)$, also gilt sogar "$= 0$", da der Grad auf der linken Seite $< s$ ist. Per Koeffizientenvergleich ergeben sich s Gleichungen

$$\sum_{i=1}^{n} y_i g_{i_j} = 0 \quad (G_i(t) := \sum_{j=1}^{s} g_{i_j} t^{j-1}).$$

Da die $g_{i_j} \in \mathbb{F}_q^m$ sind, erhält man in $\mathbb{F}_q$ gerade ms lineare homogene Gleichungen für die y_i. Der Lösungsraum besitzt folglich die Dimension $k \geq n - ms$. □

Bemerkungen Keine der beiden Anschätzungen von Satz (2.6) ist scharf.

1. Für $q = 2$ und $G(t)$ irreduzibel folgt $w_C \geq 2s + 1$. Es sind alle $y_{j_i} = 1$, also gilt $p(t) = q'(t) = h(t)^2$, letzteres wegen

$$q'(t) = \sum_{i=1}^{r} a_i i t^{i-1} = \sum_{\substack{i=1 \\ i \equiv 1 \bmod 2}}^{r} a_i t^{i-1} = \left(\sum_{i=0}^{\lfloor \frac{r-1}{2} \rfloor} b_i t^i \right)^2 .$$

   Es folgt $G \mid h^2$ und wegen G irreduzibel $G \mid h$, also $s \leq \lfloor \frac{r-1}{2} \rfloor$ sowie $2s + 1 \leq r$. Man beachte dazu $p(t) \neq 0$ wegen $p(\beta_i) \neq 0$.

2. Für BCH-Codes, d.h. $G(t) = t^{2\tau}$, gilt $k \geq n - m\frac{s}{2}$.

Decodierung: Es werde $\underline{x} \in \mathbb{F}_q^n$ gesendet und $\underline{y}$ empfangen. Dann ist $\underline{e} := \underline{y} - \underline{x}$ der Fehlervektor. Als Syndrom definieren wie dann das Polynom

$$\begin{aligned} s(t) := \sum_{i=1}^{n} e_i G_i(t) &\equiv \sum_{i=1}^{n} e_i \tfrac{1}{t-\alpha_i} \mod G(t) \\ &\equiv \sum_{i=1}^{n} \tfrac{y_i}{t-\alpha_i} \mod G(t) \end{aligned}$$

vom Grad $< s$.

Falls $e_i \neq 0$ ist, ist ein Fehler in Position i bzw. α_i aufgetreten. Folglich heißt $B := \{\alpha_i \in \mathbb{F}_q^m \mid e_i \neq 0\}$ Fehlerstellenmenge, $\sharp B = wt(\underline{e}) =: e$. Für $\beta \in B$ heißt $e_\beta = e_i$ (für passendes i) der Fehlerwert an der Fehlerstelle β. (Für $q = 2$ folgt $e_\beta = 1 \quad \forall \beta \in B$). Die Aufgabe ist also, alle Fehlerstellen und Fehlerwerte zu berechnen. Es gilt

$$s(t) \equiv \sum_{\beta \in B} \frac{e_\beta}{t - \beta} \mod G(t)$$

und wie im Beweis zu Satz (2.6) erhalten wir die Polynome
$\tau(t) := \prod_{\beta \in B} (t - \beta)$ Fehlerstellenbestimmungspolynom (error-locator-polynomial),
$\rho(t) := \sum_{\beta \in B} e_\beta \prod_{\substack{\gamma \in B \\ \gamma \neq \beta}} (t - \gamma)$ Fehlerwertbestimmungspolynom, (error-evaluator-polynomial).

2.13 Satz. *Fehlerstellen- und Fehlerwertbestimmungspolynom τ bzw. ρ genügen:*

1. $\deg(\tau) = e$,

2. $\deg(\rho) < e$,

3. $\mathrm{ggT}(\tau, \rho) = 1$,

4. $e_\beta = \frac{\rho(\beta)}{\tau'(\beta)}$,
5. $\tau(t)s(t) \equiv \rho(t) \mod G(t)$,
6. $\tau(t)\rho(t) \neq 0$.

Beweis. (1), (2) klar gemäß Definition;
(3) klar, da $\tau(t) = \prod_{\beta\in B}(t-\beta)$ und $\rho(\beta) = e_\beta \prod_{\substack{\gamma\in B\\ \gamma\neq\beta}}(\beta-\gamma) \neq 0$ ist, also $(t-\beta) \not| \rho(t)$, gilt;
(4) es ist $\tau'(t) = \sum_{\beta\in B}\prod_{\substack{\gamma\in B\\ \gamma\neq\beta}}(t-\gamma)$, also $\tau'(\beta) = \prod_{\substack{\gamma\in B\\ \gamma\neq\beta}}(\beta-\gamma)$ und damit $\rho(\beta)/\tau'(\beta) = e_\beta$;
(5) $s(t)\tau(t) \equiv (\sum_{\beta\in B}\frac{e_\beta}{t-\beta})\prod_{\beta\in B}(t-\beta) \equiv \rho(t) \mod G(t)$;
(6) Konsequenz von (3). □

2.14 Satz. *Es seien $\tau(t), \rho(t)$ Fehlerstellen- bzw. Fehlerwertbestimmungspolynom. Hat dann der Fehlervektor $\underline{e}$ ein Gewicht $wt(\underline{e}) \leq \lfloor \frac{s}{2} \rfloor$, so gilt $\tau(t) = \lambda t_j(t), \rho(t) = \lambda r_j(t)$, wobei r_j, t_j die Polynome sind, die man beim Euklidischen Algorithmus für $r_0(t) = G(t), \quad r_1(t) = s(t) \neq 0$ erhält, und j ist der kleinste Index mit $\deg(r_j) < \lfloor \frac{s}{2} \rfloor$. Die Konstante $\lambda \in \mathbb{F}_q$ bestimmt sich dabei, so dass $\tau(t)$ normiert wird.*

Beweis. Wegen $wt(\underline{e}) \leq \lfloor \frac{s}{2} \rfloor$ folgen aus (2.13) $\deg(\tau) + \deg(\rho) < \deg(G) = s, \tau\rho \neq 0$ sowie $\tau s \equiv \rho \mod G$. Also lässt sich der Haupthilfssatz anwenden. Er liefert in dieser Situation $\tau(t) = \lambda(t)t_j(t)$, $\rho(t) = \lambda(t)r_j(t)$ mit eindeutig bestimmtem Index j. Wegen (2.13)(3) muss hier $\lambda(t)$ konstant sein. Da $\tau(t)$ normiert ist, berechnet sich die Konstante λ wie angegeben. Schließlich erhalten wir die behauptete Minimaleigenschaft von j:

$$\begin{aligned} j \text{ nicht minimal } \Longrightarrow \exists k > j : s &= \deg(t_k) + \deg(r_{k-1}) \leq \deg(t_k) + \deg(r_j) \\ &< \deg(t_k) + \lfloor \tfrac{s}{2} \rfloor \Longrightarrow \deg(t_k) > \lfloor \tfrac{s}{2} \rfloor \end{aligned}$$

im Widerspruch dazu, dass die Fehleranzahl $= \deg(t_k) \leq \lfloor \frac{s}{2} \rfloor$ sein sollte. □

Das ergibt unmittelbar einen
Decodierungsalgorithmus für Goppa-Codes:
Input: Empfangener Vektor $\underline{y} \in \mathbb{F}_q^n, \alpha_1, \ldots, \alpha_m \in \mathbb{F}_q^m$ mit $G(\alpha_i) \neq 0$ für $G(t) \in \mathbb{F}_q[t]$.

1. Berechne Syndrom $s(t) \equiv \sum_{i=1}^{n} y_i \frac{1}{t-\alpha_i} \mod G(t)$.
2. Wende Euklidischen Algorithmus auf $G(t), s(t)$ an, bis erstmals $\deg(r_j) < \lfloor s/2 \rfloor$ wird.
3. Bestimme $B := \{\beta \in \mathbb{F}_q^m \mid t_j(\beta) = 0\}$.
4. Für alle $\beta \in B$ setze $e_\beta := r_j(\beta)/t_j'(\beta)$.
5. Setze $e_i := \begin{cases} 0 \text{ für } \alpha_i \notin B \\ e_\beta \text{ für } \alpha_i = \beta \in B \end{cases}$.

6. Output $\underline{x} := \underline{y} - \underline{e}$.

Bemerkungen

1. Die Bestimmung der Konstanten λ kann entfallen wegen
   $\tau(\beta) = 0 \iff \lambda\tau(\beta) = 0$ und $e_\beta = \rho(\beta)/\tau'(\beta) = \lambda^{-1}\rho(\beta)/(\lambda^{-1}\tau)'(\beta)$.

2. Im Fall $q = 2$: In Schritt 4 setze $e_\beta = 1 \quad \forall \beta \in B$.

Spezialfall: BCH-Codes mit Parametern $(n = 2^m - 1, t)$ primitive Wurzel von $\mathbb{F}_2^m$ und $g(t) = t^{2\tau}$.

Decodierungsalgorithmus für BCH-Codes:
Input: Empfangener Vektor $\underline{y} \in \mathbb{F}_2^n, n = 2^m - 1, \alpha$ primitives Element von $\mathbb{F}_2^m$.

1. Berechne Syndrome $s_j = \sum_{i=1}^{n} y_i \alpha^{(i-1)j} \quad (j = 1, \ldots, 2\tau)$.

2. Wende Euklidischen Algorithmus auf $t^{2\tau}$ und $s(t) = \sum_{i=1}^{2\tau} s_i t^{i-1}$ an bis $\deg(r_j) < \tau$ wird.

3. Bestimme $B := \{\beta \in \mathbb{F}_2^m \mid t_j(\beta) = 0\}$.

4. Berechne Fehlervektor $\underline{e}$ mittels $e_i := \begin{cases} 0 \text{ für } \alpha^{-(i-1)} \notin B \\ 1 \text{ für } \alpha^{-(i-1)} \in B \end{cases}$.

5. Output $\underline{x} = \underline{y} + \underline{e}$.

Beispiel BCH-(15,3)-Code, $\alpha^4 = \alpha + 1$

i	0	1	2	3	4	5	6	7	8
α^i	(0001)	(0010)	(0100)	(1000)	(0011)	(0110)	(1100)	(1011)	(0101)
i	9	10	11	12	13	14			
α^i	(1010)	(0111)	(1110)	(1111)	(1101)	(1001)			

Annahme: $\underline{y} = (111\ 000\ 11\ 00\ 11\ 11\ 0)$ wurde empfangen. Berechnung des Syndroms:

$$s_j = \sum_{i=1}^{15} y_i \alpha^{(i-1)j} \quad (j = 1, \ldots, 6).$$

$$\begin{aligned}
s_1 &= \alpha^0+\alpha^1+\alpha^2+(\alpha^3+\alpha^2)+(\alpha^3+\alpha+1)+(\alpha^2+\alpha+1)+(\alpha^3+\alpha^2+\alpha)+\\
&\quad (\alpha^3+\alpha^2+\alpha+1)+\alpha^3+\alpha^2+1\\
&= 1+\alpha+\alpha^3=\alpha^7\\
s_2 &= 1+\alpha^2+\alpha^4+\alpha^{12}+\alpha^{14}+\alpha^5+\alpha^7+\alpha^9+\alpha^{11}\\
&= 1\cdot(1+1+1+1+1)+\alpha(1+1+1+1+1+1)+\alpha^2(1+1+1+1)+\alpha^3\\
&\quad (1+1+1+1+1)\\
&= 1+\alpha^3=\alpha^{14}\\
s_4 &= \alpha^{13}\\
s_3 &= 1+\alpha^3+\alpha^6+\alpha^3+\alpha^6+1+\alpha^3+\alpha^6+\alpha^9\\
&= \alpha^3+\alpha^3+\alpha^2+\alpha^3+\alpha=\alpha^3+\alpha^2+\alpha=\alpha^{11}\\
s_6 &= \alpha^7\\
s_5 &= 1+\alpha^5+\alpha^{10}+1+\alpha^5+\alpha^5+\alpha^{10}+1+\alpha^5=1
\end{aligned}$$

Also erhalten wir das Syndrom

$$s(t)=\alpha^7+\alpha^{14}t+\alpha^{11}t^2+\alpha^{13}t^3+t^4+\alpha^7t^5.$$

Wir wenden den Euklidischen Algorithmus auf $G(t)=t^6$ und $s(t)$ an:
Dabei stellen wir die Polynome durch die Exponenten ihrer Koeffizienten dar ($0=\alpha^*$) : $G'(t)\hat{=}(0\ *\ *\ *\ *\ *\ *)$, $s(t)\hat{=}(7\ 0\ 13\ 11\ 14\ 7)$

i	$t_i(t)$	$r_i(t)$	$q_i(t)$
0	$(*)$	$(0,*,*,*,*,*,*)$	$-$
1	(0)	$(7,0,13,11,14,7)$	$(8,1)$
2	$(8,1)$	$(11,9,2,*,8)$	$(11,14)$
3	$(4,2,*)$	$(8,6,9,*)$	$(3,*)$
4	$(7,5,8,1)$	$(7,*,8)$	

$t^6:(\alpha^7t^5+t^4+\alpha^{13}t^3+\alpha^{11}t^2+\alpha^{14}t+\alpha^7)=\alpha^8t+\alpha$,
$\underline{\alpha^8t^5+\alpha^6t^4+\alpha^4t^3+\alpha^7t^2+t}$
$\alpha^{11}t^4+\alpha^9t^3+\alpha^2t^2+\alpha^8$

$\underline{(\alpha^7t^5+t^4+\alpha^{13}t^3+\alpha^{11}t^2+\alpha^{14}t+\alpha^7)}:(\alpha^{11}t^4+\alpha^9t^3+\alpha^2t^2+\alpha^8)=\alpha^{11}t+\alpha^4$,
$\underline{\alpha^{10}t^4+\alpha^{11}t^2+\alpha^9t+\alpha^7}$
$\alpha^8t^3+\alpha^6t^2+\alpha^9t$

$(\alpha^8t+\alpha)\cdot(\alpha^{11}t+\alpha^{14})+1=\alpha^4t^2+\alpha^2t+0.$

$\underline{(\alpha^{11}t^4+\alpha^9t^3+\alpha^2t^2+\alpha^8)}:(\alpha^8t^3+\alpha^6t^2+\alpha^9t)=\alpha^3t$,
$\alpha^7t^2+\alpha^8$

$(\alpha^4t^2+\alpha^2t)(\alpha^3t)+\alpha^8t+\alpha=\alpha^7t^3+\alpha^5t^2+\alpha^8t+\alpha.$

Hiernach sind die Nullstellen von $\tau(t) = \alpha^7 t^3 + \alpha^5 t^2 + \alpha^8 t + \alpha$ zu bestimmen. $\tau(\alpha^0) = \begin{matrix}1011\\0110\\0101\\0010\end{matrix} \neq 0,$

$\tau(\alpha^1) = \begin{matrix}0111\\1011\\1010\\0010\end{matrix} \neq 0, \tau(\alpha^{-1}) = \begin{matrix}0011\\1000\\1011\\0010\end{matrix} \neq 0,$

$\tau(\alpha^2) = \begin{matrix}1101\\1010\\0111\\0010\end{matrix} \neq 0, \tau(\alpha^{-2}) = \begin{matrix}0010\\0010\\1100\\0010\end{matrix} \neq 0, \tau(\alpha^3) = \begin{matrix}0010\\1110\\1110\\0010\end{matrix} = 0,$

$\tau(\alpha^{-3}) = \begin{matrix}1101\\1001\\0110\\0010\end{matrix} = 0.$

Durch Division erhält man $\alpha^9 = \alpha^{-6}$ als dritte Nullstelle, also existieren Fehler in den Positionen $4, 10, 13$, d.h. $B = \{\alpha^3, \alpha^9, \alpha^{12}\}$, der Output besteht aus $(1\,1\,1\,1\,0\,0\,1\,1\,0\,1\,1\,1\,0\,1\,0)$.

2.15 Definition. Es sei $\mathbb{F} = \mathbb{F}_q$ ein endlicher Körper und $n = q^m - 1 \quad (m \in \mathbb{N})$. Ferner sei α eine Primitivwurzel von $\mathbb{F}_q^m/\mathbb{F}_q$. Für festes $\tau \in \mathbb{N}$ bilden die Vektoren $\underline{x} \in (\mathbb{F}_q^m)^n$ mit $\sum_{i=1}^{n} x_i \alpha^{(i-1)j} = 0 \quad (j = 1, \ldots, 2\tau)$ einen linearen Code, den sogenannten Reed-Solomon-Code RS(n, τ).

2.16 Satz. *RS(n, τ) besteht aus allen Vektoren $\underline{c} \in \mathbb{F}_{q^m}^n$, für die das zugehörige Polynom $C(t) := \sum_{i=1}^{n} x_i t^{i-1}$ die Gestalt $C(t) = I(t) \prod_{j=1}^{2\tau} (t - \alpha^j)$ besitzt und $I(t) \in \mathbb{F}_{q^m}[t]$ einen Grad $\leq n - 1 - 2\tau$ besitzt. RS(n, τ) besitzt die Parameter $n = q^m - 1, \quad k = n - 2\tau$, $d_{\min} = 2\tau + 1$.*

Beweis. Es ist $C(\alpha^j) = 0 \quad (j = 1, \ldots, 2\tau)$ nach Definition. Für jedes Codewort $\underline{c}$ wird $C(t)$ daher durch $\prod_{j=1}^{2\tau} (t - \alpha^j) =: g(t)$ geteilt. Die Koordinaten von $\underline{c}$ liegen jetzt in $\mathbb{F}_{q^m}$ - im Gegensatz zu den BCH-Codes - so dass $g(t)$ gerade das angegebene Produkt ist, nicht mehr der ggT der Minimalpolynome der α^j. Die Dimension $k = n - 2\tau$ ergibt sich dann wie früher in (2.3). $d_{\min} \geq 2\tau + 1$ folgt wie in (2.1). Schließlich besitzt $1 \cdot g(t) \neq 0$ - als Codewort hingeschrieben - das Gewicht $\leq 2\tau + 1$, so dass $d_{\min} = 2\tau + 1$ folgt. Dass der Code zyklisch ist, folgt ebenfalls wie früher. □

Damit lassen sich RS-Codes wie BCH-Codes mittels Shift-Registern codieren. Die Arithmetik in $\mathbb{F}_{q^m}$ ist allerdings schwieriger zu realisieren.

2.17 Satz. *$\underline{c} \in \mathbb{F}_{q^m}^n$ ist Codewort des RS-Codes aus Definition (2.15) dann und nur dann, wenn $\sum_{i=1}^{n} \frac{c_i}{t - \alpha^{-(i-1)}} \equiv 0 \mod t^{2\tau}$ gilt. RS(n, τ) ist zyklisch.*

Beweis. vgl. S. 2.23, Übungen.
Damit lässt sich aber das Decodierungsverfahren für Goppa-Codes - geeignet modifiziert - anwenden. □

Decodierungs-Algorithmus für Reed-Solomon-Codes RS (n, τ)
Input: Empfangener Vektor $\underline{y} \in \mathbb{F}_{q^m}^n$.

1. Berechne Syndrome $s_j := \sum_{i=1}^{n} y_i \alpha^{(i-1)j} \quad (j = 1, \ldots, 2\tau)$.
2. Wende Euklidischen Algorithmus auf $t^{2\tau}$ und $s(t) = s_1 + s_2 t + \ldots + s_{2\tau} t^{2\tau-1}$ an, bis erstmals $\deg(r_j) < \tau$ wird. Setze $\tau(t) = t_j(t), \rho(t) = r_j(t)$.
3. Bestimme $B := \{\beta \in \mathbb{F}_{q^m} \mid \tau(\beta) = 0\}$.
4. Für jedes $\beta \in B$ setze $e_\beta := \rho(\beta)/\tau'(\beta)$.
5. Für $i = 1, \ldots, n$ setze $e_i := \begin{cases} 0 \text{ für } \alpha^{-i} \notin B \\ e_\beta \text{ für } \alpha^{-i} = \beta \in B \end{cases}$.
6. Output $\underline{x} = \underline{y} - \underline{e}$.

Beispiel: RS$(7, 2)$ mit $q^m = 2^3$.
$\mathbb{F}_8 = \{0, 1, \alpha, \ldots, \alpha^6\}$, $\alpha^3 = \alpha + 1$.

i	0	1	2	3	4	5	6
α^i	1	α	α^2	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2+1

Erzeugendes Polynom:

$$\begin{aligned} g(t) &= (t-\alpha)(t-\alpha^2)(t-\alpha^3)(t-\alpha^4) \\ &= (t^2+\alpha^4 t+\alpha^3)(t^2+\alpha^6 t+1) = t^4+\alpha^3 t^3+t^2+\alpha t+\alpha^3 \end{aligned}$$

Annahme der empfangene Vektor ist $\underline{y} = (\alpha^3, \alpha, 1, \alpha^2, 0, \alpha^3, 1)$.
Syndrome:

$$\begin{aligned} s_1 &= \alpha^3+\alpha^2+\alpha^2+\alpha^5+\alpha^8+\alpha^6 = \alpha^3 \\ s_2 &= \alpha^3+\alpha^3+\alpha^4+\alpha^8+\alpha^{13}+\alpha^{12} = \alpha^4 \\ s_3 &= \alpha^3+\alpha^4+\alpha^6+\alpha^{11}+\alpha^{18}+\alpha^{18} = \alpha^4 \\ s_4 &= \alpha^3+\alpha^5+\alpha^8+\alpha^{14}+\alpha^{23}+\alpha^{24} = \alpha^3+\alpha^5+\alpha+1+\alpha^2+\alpha^3 = 0 \end{aligned}$$

Euklidischer Algorithmus für t^4 und $s(t) = \alpha^3 + \alpha^4 t + \alpha^4 t^2$

i	t_i	r_i	q_i
0	$(*)$	$(0, *, *.*, *)$	$-$
1	(0)	$(4.4.3)$	$(3, 3, 5)$
2	$(3, 3, 5)$	$(0, 1)$	

$t^4 : (\alpha^4 t^2 + \alpha^4 t + \alpha^3) = \alpha^3 t^2 + \alpha^3 t + \alpha^5$
$\underline{t^4 + t^3 + \alpha^6 t^2}$
$\quad \underline{t^3 + t^2 + \alpha^6 t}$
$\quad\quad \underline{\alpha^2 t^2 + \alpha^2 t + \alpha}$
$\quad\quad\quad t + \alpha$

Also:
$\tau(t) = \alpha^3 t^2 + \alpha^3 t + \alpha^5$ hat Nullstellen α^4, α^5.
$\rho(t) = t + \alpha$.
Es folgt $e_{\alpha^4} = \frac{\alpha^4 + \alpha}{\alpha^3} = \alpha^6$, $e_{\alpha^5} = \frac{\alpha^5 + \alpha}{\alpha^3} = \alpha^3$ und gemäß Schritt 5. des Algorithmus
Output:

$$\begin{aligned} \underline{x} &= \underline{y} - \underline{e} \\ &= (\alpha^3, \alpha, 1, \alpha^2, 0, \alpha^3, 1) + (0, 0, \alpha^3, \alpha^6, 0, 0, 0) \\ &= (\alpha^3, \alpha, \alpha, 1, 0, \alpha^3, 1). \end{aligned}$$

Anwendung bei Fehlerexplosionen, d.h. gehäuftem Auftreten von Fehlern.
Im obigen Beispiel haben wir RS $(7, 2)$ als einen linearen $(7, 3)$ - Code über $\mathbb{F}_8$ behandelt, der dann 2 - Fehler korrigierend war. Aber genauso lässt sich jedes Codewort als Vektor aus $\mathbb{F}_2^{21}$ schreiben, indem man jede α - Potenz als Linearkombination von $1, \alpha, \alpha^2$ (mittels $\alpha^3 = 1 + \alpha$) schreibt.
Beispiel:
$\underline{x} = (\alpha^3, \alpha, \alpha, 1, 0, \alpha^3, 1) \longrightarrow (011\ 010\ 010\ 001\ 000\ 011\ 001)$. Wurde nun die Binärversion gesendet und trat etwa der Fehler

$$\underline{e} = (000\ 000 \quad \underbrace{011\ 101}_{\text{Fehler-Explosion}} \quad 000\ 000\ 000)$$

auf, so ist das Ergebnis an 4 Positionen falsch. Nun ist es nahezu unmöglich, in einem Codewort der Länge 21 (bei einem ausreichenden Informationsgehalt) 4 Fehler zu korrigieren. Zur Erinnerung: Singleton besagte $k + d \leq n + 1$.

Können wir jedoch davon ausgehen, dass die Fehler gehäuft auftreten, so lässt sich Abhilfe schaffen, indem man die Vektoren als Elemente von $\mathbb{F}_{2^3}^7$ auffasst: Es wird $\underline{e} = (0, 0, \alpha^3, \alpha^6, 0, 0, 0)$ vom Gewicht 2, also korrigierbar! Auf diese Art wird RS$(7, 2)$ ein $(21, 9)$ linearer Code über $\mathbb{F}_2$, der sehr viele gehäuft auftretende Fehler zu korrigieren vermag.

Verallgemeinerung:
Der Reed-Solomon-Code RS(n, τ) über $\mathbb{F}_{q^m}$ lässt sich auch als $(m(q^m - 1),$
$m(q^m - 1 - 2\tau))$ linearer Code über $\mathbb{F}_q$ implementieren, der dann alle gehäuft auftretenden Fehler korrigiert, die in nicht mehr als τ der ursprünglichen Koordinaten des Codeswortes über $\mathbb{F}_{q^m}$ auftreten.

2.1 Golay - Code

In $\mathbb{F}_2^{23}$ $(\mathbb{F}_3^{11})$ enthält eine Kugel vom Radius 3 (2) gerade

$$\binom{23}{0}+\binom{23}{1}+\binom{23}{2}+\binom{23}{3}=1+23+253+1771=2048=2^{11}$$

$$\left(\binom{11}{0}+2\binom{11}{1}+4\binom{11}{2}=1+22+220=243=3^5\right)$$

Vektoren. Demnach könnte es möglich sein, dass man $\mathbb{F}_2^{23}$ $(\mathbb{F}_3^{11})$ mit $k=\frac{2^{23}}{2^{11}}=2^{12}$ (3^6) Kugeln vom Radius 3 (2) vollpackt. Die Kugelmittelpunkte bilden dann einen Code der Länge 23 (11) mit dem Verhältnis

$$k/n=\frac{12}{23}=0,52 \quad \left(\frac{6}{11}=0,55\right),$$

der 3-Fehler korrogierend (2-Fehler-korrigierend) ist. Erstaunlicherweise ist ein solcher Code sogar linear!

Die Konstruktion erfolgt wie bei zyklischen Codes.

Wegen $2^{11}-1=23\cdot 89$ $(3^5-1=11\cdot 22)$ enthält $\mathbb{F}_2^{11}$ $(\mathbb{F}_3^5)$ eine primitive 23 - ste (11 - te) Einheitswurzel ζ. Dann sieht das Minimalpolynom für ζ über $\mathbb{F}_2$ folgendermaßen aus:

$$m_{\zeta/\mathbb{F}_2}(t)=\prod_{\gamma\in B}(t-\gamma) \text{ mit } B:=\{\zeta^j \mid j\in\{1,2,4,8,16,9,18,13,3,6,12\}\}.$$

Entsprechend gilt

$$m_{\zeta^{-1}/\mathbb{F}_2}(t)=\prod_{\gamma\in \tilde{B}}(t-\gamma) \text{ mit } \tilde{B}:=\{\zeta^j \mid j\in\{22,21,19,15,7,14,5,10,20,17,11\}\},$$

also auch $t^{23}-1=(t-1)m_\zeta(t)m_{\zeta^{-1}}(t)$.

Faktorisieren nach dem Berlekamp-Algorithmus liefert
$m_\zeta(t)=t^{11}+t^9+t^7+t^6+t^5+t+1$,
$m_{\zeta^{-1}}(t)=t^{11}+t^{10}+t^6+t^5+t^4+t^2+1$.
(Entsprechend für den ternären Golay-Code:
Aus $B:=\{\zeta^j \mid j\in\{1,3,9,5,4\}\}$ und $\tilde{B}:=\{\zeta^j \mid j\in\{10,8,2,6,7\}\}$ folgt $t^{11}-1=(t-1)m_\zeta(t)m_{\zeta^{-1}}(t)$. Es ist $m_{\zeta/\mathbb{F}_3}(t)=t^5+t^4-t^3+t^2-1$,
$m_{\zeta^{-1}/\mathbb{F}_3}(t)=t^5-t^3+t^2-t-1$.)

2.18 Definition. Der $(23,12)$ - Golay - Code $((11,6)$ - ternäre Golay - Code) besteht aus allen Vektoren $\mathbf{x}=(x_1,\ldots,x_{22})\in\mathbb{F}_2^{23}$ $(\mathbf{x}=(x_1,\ldots,x_{11})\in\mathbb{F}_3^{11})$, für die $x(t):=x_1+x_2t+\ldots,+x_nt^{n-1}$ durch $m_\zeta(t)$ teilbar ist $(n=23$ bzw. $11)$.

Der Golay-Code besteht daher aus allen Polynomen $I(t)m_\zeta(t)$ mit $\deg(I(t)) \leq 11 \quad (\leq 5)$, so dass der Code die Dimension $12 \quad (6)$ besitzt. Es bleibt zu zeigen, dass der so definierte Code die behaupteten Fehlerkorrekturfähigkeiten besitzt.

2.19 Lemma. *Jedes Codewort* $\neq \mathbf{0}$ *hat ein Gewicht* $\geq 5 \quad (\geq 4)$.

Beweis. Jedes Codewort $\mathbf{x}$ erfüllt $x(\zeta) = x(\zeta^2) = x(\zeta^3) = x(\zeta^4) = 0$ (betrachte B) $\quad (x(\zeta^3) = x(\zeta^4) = x(\zeta^5) = 0)$, und die Behauptung folgt mittels (2.2). (Übungen) □

2.20 Lemma. *Für* $n = 23$ *gilt* $A_i = A_{23-i} \quad (i = 0, \ldots, 11)$.

Beweis. Wegen $m_\zeta(t)m_{\zeta^{-1}}(t) = \frac{t^{23}-1}{t-1} = \sum_{i=0}^{22} t^i$ ist der Vektor $\mathbf{1} \in C$. Mit $\mathbf{x}$ ist dann auch $\mathbf{1} + \mathbf{x}$ Codewort vom Gewicht $23 - wt(\mathbf{x})$ und umgekehrt. □

2.21 Lemma. *Es sei* $n = 23$ *und* $\mathbf{x} \in C$ *Codewort des Golay-Codes von geradem Gewicht* w. *Dann gilt* $w \equiv 0 \pmod 4$.

Beweis. Es sei $x(t) = t^{e_1} + \ldots + t^{e_w}$ mit $0 \leq e_1 < e_2 < \ldots < e_w \leq 22$. Hierfür gilt $x(t) \equiv 0 \mod m_\zeta(t)$. Da $\mathbf{x}$ gerades Gewicht hat, gilt auch $x(1) = 0$, d.h. $x(t) \equiv 0 \mod (t-1)$. Für $\tilde{e}_i := -e_i + 23$ sei $\tilde{x}(t) := t^{\tilde{e}_1} + \ldots + t^{\tilde{e}_w}$. Dann ist $0 = x(\zeta) = \tilde{x}(\zeta^{-1})$, d.h. $\tilde{x}(t) \equiv 0 \mod m_{\zeta^{-1}}(t)$. Insgesamt folgt also $x(t)\tilde{x}(t) \equiv 0 \mod (t^{23}-1)$. Ausrechnen ergibt:

$$\begin{aligned} x(t)\tilde{x}(t) &= \sum_{i,j=1}^{w} t^{e_1+\tilde{e}_j} = wt^{23} + \sum_{\substack{i,j=1 \\ i\neq j}}^{w} t^{e_i+\tilde{e}_j} \\ &= \sum_{\substack{i,j=1 \\ i\neq j}}^{w} t^{e_i+\tilde{e}_j} \text{ in } \mathbb{F}_2[t], \text{ da } w \text{ gerade ist.} \end{aligned}$$

Es folgt $x(t)\tilde{x}(t) \equiv \sum_{\nu=1}^{22} \alpha_\nu t^\nu \mod (t^{23}-1)$, da für $i \neq j$ stets $e_i + \tilde{e}_j = e_i - e_j + 23 \not\equiv 0 \mod 23$ ist.

Wegen $\underline{x}(t)\underline{\tilde{x}}(t) \equiv 0 \mod (t^{23}-1)$ folgt daher, dass

$$\alpha_\nu = \sharp\{(i,j) \mid e_i + \tilde{e}_j \equiv \nu \mod 23; \quad i,j \in \{1,\ldots,w\}; i \neq j\}$$

gerade ist $(\nu = 1, \ldots, 22)$.
Wegen $e_i + \tilde{e}_j = e_i - e_j + 23, \quad e_j + \tilde{e}_i = e_j - e_i + 23$ folgt $\alpha_\nu = \alpha_{23-\nu}$ $(\nu = 1, \ldots, 11)$. Damit erhält man $w(w-1) =$ Anzahl d. Summanden in

$$\begin{aligned} \sum_{\substack{i,j=1 \\ i\neq j}}^{w} t^{e_i+\tilde{e}_j} &\stackrel{!}{=} \sum_{\nu=1}^{22} \alpha_\nu \\ &= 2\sum_{\nu=1}^{11} \alpha_\nu \equiv 0 \mod 4. \end{aligned}$$

Da w gerade ist, muss folglich $w \equiv 0 \mod 4$ gelten. □

2.22 Satz. *Die Anzahl A_i der Codeworte vom Gewicht i im $(23, 12)$ - Golay - Code ist 0 mit Ausnahme von $i = 0, 7, 8, 11, 12, 15, 16$. Folglich ist dieser Code perfekt und 3 - Fehler - korrigierend.*

Beweis. $A_1 = A_2 = A_3 = A_4 = 0$ gemäß (2.19).
$\Longrightarrow A_{22} = A_{21} = A_{20} = A_{19} = 0$ gemäß (2.20).
Nach (3.13) folgt: $A_6 = A_{10} = A_{14} = A_{18} = 0$ und somit
nach (2.20) auch $A_{17} = A_{13} = A_9 = A_5 = 0$. □

Bemerkung Codieren als zyklischer Code einfach. Decodieren i.a. mittels Syndrom-Tabelle.

2.23 Lemma. *Sei $\mathbf{x} = (x_1, \ldots, x_n)$ Codewort des ternären $(11, 6)$ Golay - Codes. Ist $\sum_{i=1}^{11} x_i = 0$ (in $\mathbb{F}_3$), so ist $wt(\mathbf{x}) \equiv 0 \pmod 3$. Ist $\sum_{i=1}^{11} x_i = \alpha \in \mathbb{F}_3 \Longrightarrow (x_1 + \alpha, \ldots, x_{11} + \alpha)$ ist Codewort $\tilde{\mathbf{x}}$ mit $wt(\tilde{\mathbf{x}}) \equiv 0 \pmod 3$. Der Code enthält daher keine Codeworte vom Gewicht $4, 7$ oder 10.*

Beweis.

1. $\sum_{i=1}^{n} x_i = 0 \Longrightarrow wt(\mathbf{x}) \equiv 0 \pmod 3$ folgt wie im ersten Teil des Beweises von (3.13):
$$0 \equiv x(t)\tilde{x}(t) \equiv wt^{11} + \sum_{\nu=1}^{10} \alpha_\nu t^\nu \mod (t^{11} - 1)\mathbb{F}_3[t].$$

2. $\tilde{x}(t) = x(t) + \alpha\frac{t^{11}-1}{t-1}$ mit $m_\zeta(t) \mid \tilde{x}(t)$. Also ist $\tilde{\mathbf{x}}$ Codewort mit $\sum_{i=1}^{11} \tilde{x}_i = \sum_{i=1}^{11} x_i + 11\alpha = 12\alpha = 0$ in $\mathbb{F}_3$.

3. Sei $\mathbf{x} \in C$ mit $wt(\mathbf{x}) = 4$. Dann lassen sich die Komponenten $\neq 0$ in der Gestalt $(1, 1, 1, 1)$ oder $(1, 1, 1, 2)$ annehmen. (Keine zwei, eine zwei: zyklischer Shift, vier zweien Mult. mit 2, drei zweien Mult. mit $2+$ Shift, 2 zweien $\Longrightarrow wt(\mathbf{x}) \equiv 0 \pmod 3$ Widerspruch.)
Im ersten Fall ist $\tilde{\mathbf{x}} = \mathbf{x} + \mathbf{1}$ mit $\sum \tilde{x}_i = 7 \cdot 1 + 4 \cdot 2 = 0$
$\Longrightarrow wt(\tilde{\mathbf{x}}) = 11 \equiv 0 \pmod 3$ Widerspruch.
Im zweiten Fall ist $\tilde{\mathbf{x}} = \mathbf{x} + 2 \cdot \mathbf{1}$ mit $\sum \tilde{x}_i = 3 \cdot 0 + 1 + 7 \cdot 2 \equiv 0 \pmod 3$
$\Longrightarrow wt(\tilde{\mathbf{x}}) = 8 \equiv 0 \pmod 3$ Widerspruch.
Sei $\mathbf{x} \in C$ mit $wt(\mathbf{x}) = 7$. OBdA sind hierzu mindestens 4 Koordinaten
Eins (sonst $\mathbf{x} \longrightarrow 2 \cdot \mathbf{x}$).

$$\begin{array}{lcl}
(4 * 1, 3 * 2) + \mathbf{1} & = & (4 * 1 + 4 * 2), \quad wt(8) \not\equiv 0 \pmod 3 \text{ Widerspruch;} \\
(5 * 1, 2 + 2) & & \text{Widerspruch;} \\
(6 * 1, 1 * 2) + 2 * \mathbf{1} & = & (1 * 1, 4 * 2), \quad wt(5) \not\equiv 0 \pmod 3 \text{ Widerspruch;} \\
(2 * 1) + \mathbf{1} & = & (4 * 1 + 7 * 2), \quad wt(11) \not\equiv 0 \pmod 3 \text{ Widerspruch.}
\end{array}$$

□

Schließlich sei $\mathbf{x} \in C$ mit $wt(\mathbf{x}) = 10$. OBdA sind mindestens fünf $\mathbf{x}$ - Koordinaten Eins, sonst Übergang von $\mathbf{x}$ zu $2\mathbf{x}$.
$(5 * 1, 5 * 2)$ Widerspruch; $(6 * 1, 4 * 2) + 2 * \mathbf{1} = (4 * 1 + 1 * 2), \quad wt(5) \not\equiv 0 \pmod 3$;

$(7*1, 3*2) + \mathbf{1} = (1*1 + 7*2), \quad wt(8) \not\equiv 0 \pmod 3$;
$(8*1, 2*2)$ Widerspruch; $(9*1, 1*2) + 2*\mathbf{1} = (1*1 + 1*2), \quad wt(2) \not\equiv 0 \pmod 3$;
$(10*1) + \mathbf{1}$ Widerspruch.

Gewichtsverteilungen:
Golay-Code $(23, 12)$

i	0	7	8	11	12	15	16	23
A_i	1	253	506	1288	1288	506	253	1

Golay-Code $(24, 12)$ erweitert (parity-check)

i	0	8	12	16	24
A_i	1	759	2576	759	1

ternärer Golay-Code $(11, 6)$

i	0	5	6	8	9	11
A_i	1	132	132	330	110	24.

Ausblick

1. Wir haben Block-Codes betrachtet, d.h. Codes, bei denen die Nachricht in Teile gleicher Länge gegliedert und diese Teile dann in Codeworte gleicher Länge decodiert werden. Man erhält hierfür eine besser entwickelte Strukturtheorie (nicht notwendig besser für Praxis).

Wie gut sind die besten Codes?
1950 waren die folgenden perfekten Codes bereits bekannt:

Nr.	n	q	Fehlerkorrekturf. e	Art
1	$2e+1$	2	bel.	Wiederholungscodes $[n, 1]$
2	$(q^m-1)/(q-1)$	$q = p^r$	1	Hamming-Codes
3	23	2	3	Binärer Golay-Code
4	11	3	2	Ternärer Golay-Code.

Dies sind bereits alle! D.h. es gibt keine weiteren perfekten Codes in dem Sinn, dass alle zu $1, 2, 3$ oder 4 äquivalent sind oder die gleichen Parameter wie Hamming-Codes besitzen.
Im Fall $q \neq p^r$ ist die Frage noch nicht gänzlich beantwortet, eine negative Antwort ist jedoch wahrscheinlich.

Da es keine weiteren perfekten Codes gibt, galt und gilt die weitere Untersuchung dem Problem, zu gegebenen n und $d_{\min}$ Codes mit möglichst vielen Codeworten zu konstruieren.
$A(n, d) := \max\{\sharp C \mid C \text{ ist Code der Länge } n \text{ mit Minimalabstand } d\}$.
Untere Schranken durch explizite Konstruktion von Codes, obere Schranken i.a. durch Optimierungsproblem.

Wie konstruiert man nun gute Codes?
Codefolge, die Shannon-Satz entspricht, wurde bisher nicht gefunden!
BCH-Codes sind gut, da Decodierungsalgorithmus existiert.
Cyclic Codes: BCH, Reed-Solomon, Golay, Minimale Codes $\tilde{M}_j =$ irreduzible Codes.
Die besten Codes zu gegebenem n und d sind jedoch i.a. nicht linear und ad hoc Konstruktionen.

Decodierung:

- Goppa-Codes
- lineare, die nicht zu groß sind, mit Hilfe einer Syndrom-Tabelle
- Threshold Decoding (Reed-Muller-Codes) für lineare Codes.

(**Generelle Voraussetzung:** q - ärer symmetrischer Kanal ohne Gedächtnis.)

2.2 Zusammenhang von Idealen und zyklischen Codes

Wir betrachten

$$R_n := \mathbb{F}_q[t]/(t^n - 1)\mathbb{F}_q[t]$$

als Algebra über $\mathbb{F}_q$ mit Basis $1, t, \ldots, t^{n-1}$. Lineare Codes als Teilräume von $\mathbb{F}_q^n$ entsprechen jetzt Polynomen vom Grad $< n$.

2.24 Satz. *$C \subseteq \mathbb{F}_q^n$ zyklischer Code $\Longleftrightarrow$ C Ideal in R_n.*

Beweis. 1. C zyklischer Code, $c(t) \in C$; sei $R_n \ni f(t) = \sum_{i=1}^{m} f_i t^{i-1}$ beliebig; dann gilt $f(t)c(t) = \sum_{i=1}^{m} f_i(t^{i-1}c(t)) \quad \in C$, da Multiplikation mit t einen Shift bewirkt ($t^n = 1$!) und C Unterraum ist, d.h. es gilt $C + C \subseteq C$.

2. C Ideal, $c(t) \in C \Longrightarrow tc(t) \quad \in C$ also ist C zyklisch.

□

Beispiel: $C = \{(000), (011), (101), (110)\} \subseteq \mathbb{F}_2^3$
$\longleftrightarrow \{0, 1+t, 1+t^2, t+t^2\}$ ist Teilraum von $\mathbb{F}_2[t]/(t^3+1)\mathbb{F}_2[t]$ und sogar Ideal!

2.25 Satz. *Es sei $C \neq 0$ ein Ideal in R_n. Dann gilt:*

1. *Es existiert ein eindeutig bestimmtes normiertes Polynom g kleinsten Grades in C;*
2. *$C = R_n g$;*
3. *$g(t) \mid (t^n - 1)$;*
4. *$\forall h \in C \quad \dot{\exists}\, f \in R_n, \deg(f) < n - \deg(g) : h = f \cdot g$; $\dim C = n - \deg(g)$. **Die Botschaft f wird in das Codewort $f \cdot g$ codiert.***

5. *Für* $g(t) = \sum_{i=0}^{r} g_i t^i$ *besitzt* C *die erzeugende Matrix*

$$G_C = \begin{pmatrix} g(t) & & & \\ & tg(t) & & 0 \\ 0 & \cdot & & \\ & & \cdot & \\ & & & \cdot \\ & & & t^{n-r-1}\ g(t) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 \cdots g_r & & \\ & g_0 g_1 \cdots & g_r & 0 \\ & 0 & \cdot & \\ & & & \cdot \\ & & & \cdot \\ & & & g_0 g_1 \ \cdots \ g_r \end{pmatrix}.$$

Beweis. 1. Haben $g_1, g_2 \in C$ beide die gewünschten Eigenschaften, so ist $g_1 - g_2 = 0$ wegen der Gradminimalität.

2. Für $f \in C$ mit $f = qg + r$ folgt $r = 0$ wegen der Gradminimalität von g.

3. In $\mathbb{F}_q[t]$ gilt $(t^n - 1) = q(t)g(t) + r(t)$; in R_n wird daraus: $0 = q(t)g(t) + r(t)$. Hiernach gilt $r(x) \in C$ mit $\deg(r) < \deg(g)$, d.h. $r(t) = 0$ in R_n; wegen $\deg(r) < \deg(g) < n$ muss $r(x) = 0$ bereits in $\mathbb{F}_q[t]$ gelten.

4. Direkte Folge von 2., denn $t^n - 1 = g(t)\tilde{g}(t)$ impliziert $C \ni h = f \cdot g = (f - k\tilde{g})g$.

5. $g(t), tg(t), \ldots, t^{n-r-1}g(t)$ bilden eine Basis von C.

□

Bemerkung $g(t)$ heißt erzeugendes Polynom des Codes C. (vgl. (2.4), (2.5))

Beispiel: Hamming-Code: $g(t) = m_\alpha(t)$, α primitives Element von $\mathbb{F}_2^m$;
τ - Fehler korrigierender BCH-Code: $g(t) = kgV(m_\alpha, (t), \ldots, m_{\alpha^{2\tau-1}}(t))$.

Zusammenhang zwischen n, m **und** q**:** Die erzeugenden Polynome zyklischer Codes sind nach (2.14)(3) Faktoren von $t^n - 1$ für $n =$ Codewortlänge; die Dimension des Codes ergibt sich dann zu $n - \deg(g)$.

Für die weitere Untersuchung ist nun die Einschränkung $(n, q) = 1$ erforderlich. Sie garantiert zunächst, dass $t^n - 1$ lauter einfache Nullstellen besitzt. Bei einer Faktorisierung von $t^n - 1$ sind die auftretenden Faktoren folglich paarweise teiler-fremd. (Im Fall $q = 2$ genügt also n ungerade.)

Ist nun q teilerfremd zu n, so liegt q in der primen Restklassengruppe modulo n. (Die zu n teilerfremden Zahlen bilden eine multiplikative Gruppe der Ordnung $\varphi(n)$.) Also gilt: $\exists m \in \mathbb{N}$ minimal: $q^m \equiv 1$ modulo n, bzw. $\exists m \in \mathbb{N}$ minimal: $n \mid (q^m - 1)$. Es folgt $(t^n - 1) \mid (t^{q^m - 1} - 1)$ sowie $(t^n - 1) \not| (t^{q^s - 1} - 1)$ für $0 < s < m$.

Also liegen alle n - ten Einheitswurzeln in $\mathbb{F}_q^m$ und in keinem kleineren Körper. $\mathbb{F}_q^m$ ist also der Zerfällungskörper von $t^n - 1$, es ist $t^n - 1 = \prod_{i=1}^{n}(t - \alpha_i)$ mit $\alpha_i \in \mathbb{F}_q^m$ paarweise verschieden.

Die α_i bilden dann eine Untergruppe U von $(\mathbb{F}_q^m)^\times$, die dann natürlich ihrerseits zyklisch ist. Folglich existiert $\alpha \in (\mathbb{F}_q^m)^\times$ (primitive n - te Einheitswurzel) mit $t^n - 1 = \prod_{i=1}^{n}(t - \alpha^i)$.

D.h. in der Praxis sind n, q gegeben, und m bestimmt sich dann entweder als kleinste Zahl aus $\mathbb{N}$ mit $n \mid (q^m - 1)$; oder man gibt m vor und wählt $n = q^m - 1$, wie es bei den gängigen Codes geschieht.

2.26 Satz. *Es sei C ein zyklischer Code mit erzeugendem Polynom $g(t)$, α eine primitive n - te Einheitswurzel. Ist dann $g(\alpha^s) = \ldots = g(\alpha^{s+\tau-2}) = 0 \quad (s, \tau \in \mathbb{N})$, so ist das Minimalgewicht des Codes mindestens τ.*

Der Beweis verläuft analog zu dem von Satz (2.2).

Beweis. Die Prüfmatrix zum Code enthält die Teilmatrix (höchstens weniger Zeilen):

$$\begin{pmatrix} 1 & \alpha^s & \ldots & \alpha^{s(n-1)} \\ 1 & \alpha^{s+1} & \ldots & \alpha^{(s+1)(n-1)} \\ \vdots & & & \\ 1 & \alpha^{s+\kappa} & \ldots & \alpha^{(s+\kappa)(n-1)} \end{pmatrix} \text{ mit } \kappa = \tau - 2 \text{ bzw. } \kappa + 1 = \tau - 1.$$

Es genügt also zu zeigen, dass je $r = \kappa + 1$ Spalten linear unabhängig sind. Wir wählen Spalten mit den Indizes $1 \le i_1 < i_2 < \ldots < i_r \le n$.
Wir bilden hiermit die Teilmatrix:

$$A := \begin{bmatrix} \alpha^{si_1} & \alpha^{si_2} & \ldots & \alpha^{si_r} \\ \alpha^{(s+1)i_1} & \alpha^{(s+1)i_2} & & \\ \vdots & \vdots & & \vdots \\ \alpha^{(s+\kappa)i_1} & \alpha^{(s+\kappa)i_2} & \ldots & \alpha^{(s+\kappa)i_r} \end{bmatrix}$$

$$\text{mit } \det A = \alpha^{si_1} \cdot \ldots \cdot \alpha^{si_r} \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \ldots & \alpha^{i_r} \\ \vdots & \vdots & & \vdots \\ \alpha^{\kappa i_1} & \alpha^{\kappa i_2} & \ldots & \alpha^{\kappa i_r} \end{vmatrix}$$

$$= \alpha^{si_1} \cdot \ldots \cdot \alpha^{si_r} \prod_{1 \le \mu < \nu \le r} (\alpha^{i_\mu} - \alpha^{i_\nu}) \neq 0. \qquad \square$$

2.27 Korollar. *Ein zyklischer Code der Länge n mit Nullstellen (des erzeugenden Polynoms $g(t)$) $\alpha^s, \alpha^{s+r}, \ldots, \alpha^{s+(\tau-2)r}$ und $(r, n) = 1$ besitzt einen Minimalabstand $\ge \tau$.*

Beweis. Wir setzen $\beta = \alpha^r$. Da $(r, n) = 1$ gilt, ist β ebenfalls primitive n - te Einheitswurzel. Es folgt $\alpha^s = \beta^u$ für passendes $u \in \mathbb{Z}^{\ge 0}$, und der Code besitzt die Nullstellen $\beta^u, \beta^{u+1}, \ldots, \beta^{u+(\tau-2)}$. Nun folgt das Ergebnis aus (2.26). $\square$

Beispiel: Alle BCH-Codes der Länge 15 mit $s = 1$ über $\mathbb{F}_2$. Es ist $t^{15} + 1 = (t+1)(t^2+t+1)(t^4+t+1)(t^4+t^3+1)(t^4+t^3+t^2+t+1)$ sowie $m = 4$.

Als primitives Element wählen wir α mit $\alpha^4 = 1 + \alpha$, $\alpha^{15} = 1$.

Die Minimalpolynome:	Ihre Nullstellen:
t	0
$t+1$	α^0
t^4+t+1	$\alpha, \alpha^2, \alpha^4, \alpha^8$
t^4+t^3+1	$\alpha^{14}, \alpha^{13}, \alpha^{11}, \alpha^7$
$t^4+t^3+t^2+t+1$	$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$
t^2+t+1	α^5, α^{10}

BCH-Codes:

τ	BCH - Distanz $\geq$ (nach Satz (2.2))	Erz. Polynom $g(t)$	Exponenten d. Wurzeln von g	Dimension $n - \deg(g)$	$d_{\min}$
0	1	1	$-$	15	1
1	3	m_α	$1, 2, 4, 8$	11	3
2	5	$m_\alpha m_{\alpha^3}$	$1-4, 6, 8, 9, 12$	7	5
3	7	$m_\alpha m_{\alpha^3} m_{\alpha^5}$	$1-6, 8-10, 12$	5	7
$4, 5, 6$ oder 7	$9, 11, 13$ oder 15	$(t^{15}+1)/(t+1)$ $= m_\alpha m_{\alpha^3} m_{\alpha^5} m_{\alpha^7}$	$1-14$	1	15

Neben der Beschreibung zyklischer Codes durch ihre erzeugenden Polynome als Teiler von $t^n - 1$ gibt es einen weiteren Zugang, nämlich den über sogenannte **Idempotente**.

2.28 Satz. *Es sei C ein Ideal in R_n sowie $(n, q) = 1$. Dann existiert in C ein Polynom $e(t) \neq 0$ mit den Eigenschaften*

1. $e(t) = e(t)^2$;
2. $C = R_n e(t)$;
3. $\forall f \in R_n : f(t)e(t) = f(t) \iff f(t) \in C$.

Das Polynom $e(t)$ ist durch (1) + (2) bzw. (1) + (3) jeweils eindeutig bestimmt. Es heißt Idempotente von R_n.

Beweis. 1. Es sei $C = R_n g$; dann ist $t^n - 1 = g(t)h(t)$ mit $\mathrm{ggT}(g, h) = 1$. Also existieren $u, v \in \mathbb{F}_q[t]$ mit $1 = u(t)g(t) + v(t)h(t)$. Wir setzen $e(t) := u(t)g(t) \mod (t^n - 1)\mathbb{F}_q[t]$. Dafür gilt in R_n:

$$e(t) = e(t) \cdot 1 = (u(t)g(t))^2 + u(t)v(t)g(t)h(t) = e(t)^2.$$

2. Offenbar gilt $\tilde{C} := R_n e(t) \subseteq C$; andererseits ist das normierte Polynom kleinsten Grades in $\tilde{C}$ gerade $\mathrm{ggT}(e(t), t^n - 1) = g(t)$. (Die Polynome in $\tilde{C}$ sind ja gerade von der Gestalt $we + \tilde{w}(t^n - 1)$, und es ist $\mathrm{ggT}(u, h) = 1$.)

3. Für $f \in C$ gilt $f \stackrel{(2)}{=} w \cdot e = we^2 = f \cdot e$. Ferner ist für $f \in R_n$ stets $f \cdot e \in C$ nach (2), d.h. im Fall $f = fe$ gilt auch $f \in C$.
   Zur Eindeutigkeit: Da (1) + (2) auch (3) implizieren, genügt der Nachweis für (1) + (3). Also mögen e_1, e_2 die Bedingungen (1) + (3) erfüllen. Dann ist aber $e_1 = e_1 e_2 = e_2$ wegen (3).

□

Der Vorteil, zyklische Codes durch Idempotente zu beschreiben, liegt darin, dass man **nicht** erst $t^n - 1$ faktorisieren muss, um ein erzeugendes Element zu erhalten.

Bemerkung ist $e(t) \neq 1$ Idempotente, dann ist es auch $1 - e(t)$. Wegen $e(t)(1 - e(t)) = 0$ enthält R_n dann notwendig Nullteiler.

2.29 Definition. Ein Ideal C in R_n heißt **minimal** (bzw. der zugehörige Code minimal), falls es in R_n kein Ideal $\tilde{C}$ mit $0 \neq \tilde{C} \subset C$ gibt. Eine Idempotente zu einem minimalen Code heißt **primitive Idempotente**. (Entsprechend: **maximale** Ideale).

2.30 Satz. *Es sei $t^n - 1 = f_1(t) \cdot \ldots \cdot f_r(t)$ die Faktorisierung von $t^n - 1$ in irreduzible Polynome. Dann sind $M_i := R_n f_i$ maximale Ideale in R_n. Entsprechend sind $\tilde{M}_i := R_n \prod_{\substack{j=1 \\ j \neq i}}^{n} f_i = R_n \tilde{f}_i$ minimale Ideale. $\tilde{M}_i$ ist zu M_i orthogonal.*
$\tilde{M}_i$ ist isomorph zu einem Körper. Jedes Ideal ist Summe minimaler Ideale.

Beweis. 1. M_i maximal klar wegen f_i irreduzibel.

2. $\tilde{M}_i$ minimal: Es sei $0 \neq C \subseteq \tilde{M}_i$ ein Ideal. Dann existiert ein erzeugendes Element g von C mit $g \mid (t^n - 1)$. Wegen $C \subseteq \tilde{M}_i$ folgt dann $\tilde{f}_i := \prod_{\substack{j=1 \\ j \neq i}}^{n} f_i \mid g$, was wegen $C \neq 0$ dann $C = \tilde{M}_i$ impliziert.

3. Es sei f aus $\tilde{M}_i$, d.h. $f = u\tilde{f}_i$. Wegen $(t^n - 1) \mid f \cdot f_i$ gilt $f f_i = 0$ in R_n, d.h. f steht senkrecht auf M_i.

4. Es genügt zu zeigen, dass $\tilde{M}_i$ Integritätsbereich ist (denn da $\tilde{M}_i$ nur endlich viele Elemente hat, muss es sodann Körper sein). Wähle $f \neq 0$ aus $\tilde{M}_i$ und $C := \{g \in \tilde{M}_i \mid f \cdot g = 0\} \subseteq \tilde{M}_i$. C ist ein Ideal. Wegen der Minimalität von $\tilde{M}_i$ genügt es, $C \neq \tilde{M}_i$ zu zeigen, denn dann folgt sofort $C = 0$.
   Es ist aber $f \notin C$, denn wegen $f \neq 0$ gilt mit $(t^n - 1) \not| f$ auch $(t^n - 1) \not| f^2$, da $t^n - 1$ mach Voraussetzung nur einfache Nullstellen besitzt.

5. Induktiv! Wegen der endlichen Elementzahl von R_n muss der Prozess abbrechen!

Es sei C ein Ideal von R_n mit einer Idempotenten e. Es gilt also $C = R_n e$. Ferner enthält C ein minimales Ideal $M = R_n ef$ mit $ef = (ef)^2 \neq 0$. Wir bemerken noch $fe = ef = ee\tilde{f} = e\tilde{f} = f$. Wir schreiben $e = ef + (e - ef)$ und erhalten

$$\begin{array}{lll} ef \quad (e - ef) & = & ef - (ef)^2 = 0, \\ (e - ef)^2 & = & e(e - ef) - ef(e - ef) = e - ef. \end{array}$$

Ist also $M \subset C$, so gilt $ef \neq e$ und wir erhalten eine Aufspaltung

$$\begin{aligned} C = R_n e &= R_n(ef + (e - ef)) = R_n ef \dotplus R_n(e - ef) \\ &= M \dotplus \tilde{M} \end{aligned}$$

mit einem minimalen Ideal $0 \neq \tilde{M} \subset C$. (Man beachte zum 3. Gleichheitszeichen:

$$\begin{aligned} xef + y(e - ef) &= (x - y)ef + ye \\ &= ((x - y)f + y)e \in R_n e\ .) \end{aligned}$$

□

Bemerkung Eine primitive Idempotente von $\tilde{M}_i$ wird mit $\theta_i(t)$ oder θ_i bezeichnet.

Beispiel Wir übernehmen die Bezeichnung vom letzten Beispiel. Es sei

$$g(t) = m_\alpha(t) m_{\alpha^3}(t) m_{\alpha^5}(t)$$

vom Grad 10 und $C = R_n g$. Dann ist $(t^{15} - 1)/g(t) = h(t)$, also

$$\begin{aligned} h(t) &= (t + 1)(t^4 + t^3 + 1) \\ &= t^5 + t^3 + t + 1 \end{aligned}$$

Gemäß (2.28) bestimmen wir die zugehörige Idempotente mittels Division mit Rest abgewandt auf $g(t) = t^{10} + t^8 + t^5 + t^4 + t^2 + t + 1$ und $h(t) = t^5 + t^3 + t + 1$.

$$\begin{array}{l} (t^{10} + t^8 + t^5 + t^4 + t^2 + t + 1) : (t^5 + t^3 + t + 1) = t^5 + t \\ \underline{t^{10} + t^8 + t^6 + t^5} \\ \qquad\quad t^6 + t^4 + t^2 + t \\ \qquad\quad \underline{t^6 + t^4 + t^2 + t} \\ \qquad\qquad\qquad\quad 1 \end{array}$$

Es ergibt sich also $1 \cdot g(t) + (t^5 + t)h(t) = 1$, d.h. $g(t)$ ist selbst Idempotente. Man rechnet leicht $g^2 = g$ in R_{15} nach.
Demnach ist auch

$$1 - e = 1 + e = t^{10} + t^8 + t^5 + t^4 + t^2 + t$$

Idempotente, es ist offenbar

$$(1 - e)^2 = t^5 + t + t^{10} + t^8 + t^4 + t^2 = (1 - e).$$

Also gilt

$$R_{15} = R_{15} e \dotplus R_{15}(1 - e).$$

Für $f = (t^{15} - 1)/(t - 1) = 1 + t + \ldots + t^{14}$ ist

$$\begin{aligned} f^2 &= (t^{30} - 1)/(t^2 - 1) \\ &= t^{28} + t^{26} + \ldots + 1. \end{aligned}$$

Es ist $f = (t+1) = (t^{13}+t^{11}+t^9+t^7+t^5+t^3+t)+1$ also $1 = 1 \cdot f + (t^{13}+t^{11}+t^9+t^7+t^5+t^3+t)(t+1)$ und f nach Satz (2.28) Idempotente.

2.31 Satz. *Es seien C_1, C_2 Ideale in R_n mit Idempotenten e_1, e_2. Dann bestitzt*

1. *$C_1 \cap C_2$ die Idempotente e_1e_2 (für $C_1 \cap C_2 \neq 0$);*
2. *$C_1 + C_2$ die Idempotente $e_1e_2 + e_1e_2$ (nur für char $\mathbb{F}_q = 2$).*

Beweis. 1. Es ist $e_1e_2 \in C_1 \cap C_2$; $(e_1e_2)^2 = e_1e_2$ und für $f \in C_1 \cap C_2$, d.h. $f = u_1e_1 = u_2e_2$, folgt $e_1e_2f = e_1e_2u_2e_2 = e_1u_2e_2 = e_1u_1e_1 = u_1e_1 = f$; also ist e_1e_2 Idempotente für $C_1 \cap C_2$ nach (2.28).

2. Es ist $e_1 + e_2 + e_1e_2 \in C_1 + C_2$, ferner gilt

$$\begin{aligned}(e_1 + e_2 + e_1e_2)^2 &= e_1^2 + e_1e_2 + e_1^2e_2 + e_2e_1 + e_2^2 + e_1e_2^2 \\ &\quad + e_1^2e_2 + e_1e_2^2 + e_1^2e_2^2 = e_1 + e_2 + 7e_1e_2.\end{aligned}$$

Ist $f = f_1 + f_2$ mit $f_1 \in C_1$ und $f_2 \in C_2$, so wird

$$(e_1 + e_2 + e_1e_2)f = e_1f_1 + e_2f_1 + e_1e_2f_1 + e_1f_2 + e_2f_2 + e_1e_2f_2 =$$

$$f_1 + e_2f_1 + e_2f_1 + e_1f_2 + f_2 + e_1f_2 = f_1 + f_2 = f.$$

Die Behauptung folgt wieder mit (2.28).

□

2.32 Satz. *Für die primitiven Idempotenten $\theta_1, \ldots, \theta_r$ in R_n gilt:*

1. *$\theta_i\theta_j = 0 \quad (i \neq j)$;*
2. *$\sum_{i=1}^{r} \theta_i = 1$;*
3. *$1 + \theta_{i_1} + \ldots + \theta_{i_s}$ ist Idempotente von R_n $f_i, \cdot \ldots \cdot f_{i_s}$. (Char $\mathbb{F}_q = 2$)*

Beweis. 1. Klar nach Definition wegen $(t^n - 1) \mid (\theta_i\theta_j)$.

2. $R_n = \sum_{i=1}^{r} \tilde{M}_i$; wende (2.31)(2) und (2.32)(1) iteriert an. Wir wissen nach (2.31), dass R_n direkte Summe von minimalen Idealen ist. Nach (2.30) sind $\tilde{M}_1, \ldots, \tilde{M}_r$ mit $\tilde{M}_i = R_n\tilde{f}_i$ gerade die minimalen Ideale von R_n. Da der Durchschnitt verschiedener minimaler Ideale 0 ist, ist $\tilde{M}_1 + \ldots + \tilde{M}_r$ direkt; und für die Idempotenten $\tilde{e}_i$ von $\tilde{M}_i$ gilt $\tilde{e}_i\tilde{e}_j = 0$.
(Beachte: R_n selbst Körper $\Longrightarrow$ R_n minimales Ideal.) Also ist $1 = \tilde{e}_1 + \ldots + \tilde{e}_r$, wie es sich auch aus der Zerlegung in (2.31)(5) ergibt.

3.

$$R_nf_{i_1} \cdot \ldots \cdot f_{i_s} = \sum_{\substack{j=1 \\ j \notin \{i_1, \ldots, i_s\}}}^{r} \tilde{M}_j$$

hat Idempotente $\sum_{\substack{j=1 \\ j \notin \{i_1, \ldots, i_s\}}}^{r} \theta_j \overset{(2)}{=} 1 + \theta_{i_1} + \ldots + \theta_{i_s}$.

□

Damit lässt sich nun ein Algorithmus zur Bestimmung aller primitiven Idempotenten herleiten. Zunächst berechnen wir die Anzahl r der primitiven Idempotenten. Sie ist gleich der Anzahl der normierten irreduziblen Teiler von $t^n - 1$ in $\mathbb{F}_q[t]$. Wir haben $n = 2^m - 1$, und es ist $t^{2^m} - t$ das Produkt aller normierten irre-duziblen Polynome vom Grad d mit $d \mid m$ (Algebra). Deren Anzahl A_d beträgt $A_d = \frac{1}{d}\sum_{\kappa|d} \mu(\kappa) 2^{d/\kappa}$. Aus diesen Angaben lässt sich r leicht bestimmen.

Algorithmus zur Berechnung der primitiven Idempotenten eines zyklischen binären Codes ungerader Länge $\mathbf{n = 2^m - 1}$.

Es seien zunächst $\eta_1, \ldots, \eta_r$ die Idempotenten, die zu den Zyklentypen von $n \mod 2$ gehören. Für $j \in \{1, \ldots, n\}$ erhalten wir als Zykel gerade $\{kj \mid 1 \leq k \leq n\} =: \{j_1, \ldots, j_\mu\}$ mit der Idempotenten $t^{j_1} + \ldots + t^{j_\mu}$.

Beispiel $m_\alpha(t) = t^4 + t + 1$ hat die Nullstellen $\alpha, \alpha^2, \alpha^4, \alpha^8$, also ist $\eta_2 = t + t^2 + t^4 + t^8$ Idempotente in $\mathbb{F}_2[t]/(t^{15} - 1)\mathbb{F}_2[t]$. Dann ist $1 = \eta_2 + (1 + \eta_2)$ eine Zerlegung der 1 in orthogonale Idempotente. Wir nehmen an, dass wir bereits die 1 in $s < r$ orthogonale Idempotente zerlegt haben:

$$1 = \sum_{j=1}^{s} \xi_j, \quad \xi_i \xi_j = 0 \quad (i \neq j).$$

ξ sei irgendeine (weitere) Idempotente.

1. Fall:
$\exists j \in \{1, \ldots, s\} : \xi_j \xi \neq 0 \wedge \xi_j(1 + \xi) \neq 0$. Dann ist
$\xi_i(\xi_j \xi) = 0, \xi_i \xi_j (1 + \xi) = 0 \quad \forall i \neq j$;
$\xi_j \xi, \quad \xi_j(1 + \xi)$ sind Idempotente mit

$$\xi_j = \xi_j \xi + \xi_j(1 + \xi) \text{ und } \xi_j \xi \xi_j (1 + \xi) = 0;$$

d.h. wir erhalten $s + 1$ orthogonale Idempotente, indem wir für ξ_j die Elemente $\xi\xi_j$ und $\xi_j(1 + \xi)$ in unsere Menge aufnehmen.

2. Fall:
Es gelten $\xi_j \xi = 0 \vee \xi_j(1 + \xi) = 0$ für $j = 1, \ldots, s$ und alle $\xi \in \{\eta_1, \ldots, \eta_r\}$. Wir setzen $s = \{j \in \{1, \ldots, s\} \mid \xi_j \xi = 0\}$, $T = \{1, \ldots, s\} \backslash S$ und erhalten $0 = \sum_{j \in S} \xi_j \xi + \sum_{j \in T} \xi_j (1 + \xi) =$

$$\left(\sum_{j \in S \cup T} \xi_j \right) \xi + \sum_{j \in T} \xi_j = \xi + \sum_{j \in T} \xi_j \Longrightarrow \xi = \sum_{j \in T} \xi_j.$$

Aber $\eta_1, \ldots, \eta_r$ sind über $\mathbb{F}_2$ - linear unabhängig, da sie verschiedene Grade besitzen. Falls der Algorithmus abbricht, sind $\eta_1, \ldots, \eta_r$ Linearkomb. von $\xi_1, \ldots, \xi_s$ mit $1 = \xi_1 + \ldots + \xi_s$, $\xi_i \xi_j = \delta_{ij} \xi_i$. Da $\eta_1, \ldots, \eta_r \quad \mathbb{F}_2$ - linear unabhängig sind, folgt $s \geq r$. Aus der Theorie (Min. Ideale $\Longleftrightarrow \frac{x^n - 1}{\pi(x)}$) folgt $s \leq r$, also sind wir gemäß der folgenden Bemerkung fertig.

Bemerkung Sind zunächst $\emptyset \neq S, T \subseteq \{1, \ldots, r\}$, so gilt:

$$(\sum_{j \in S} \theta_j)(\sum_{j \in T} \theta_j) = \sum_{j \in S \cap T} \theta_j \quad (= 0 \Longleftrightarrow S \cap T = \emptyset).$$

Sind andererseits $\xi_1, \ldots, \xi_r$ Idempotente mit $\xi_i \xi_j = 0 \quad (i \neq j)$, so ist jedes ξ_j Summe von gewissen ξ_{j_ν} und kein θ_k kann in der Darstellung von ξ_i **und** $\xi_j \quad (j \neq i)$ auftreten! Folglich ist $\{\xi_1, \ldots, \xi_r\}$ eine Umordnung von $\{\theta_1, \ldots, \theta_r\}$.

Beispiel: Für $n = 15$ gilt: $\eta_1 \stackrel{\wedge}{=} (0), \quad \eta_2 \stackrel{\wedge}{=} (1, 2, 4, 8), \quad \eta_3 \stackrel{\wedge}{=} (3, 6, 9, 12), \quad \eta_4 \stackrel{\wedge}{=} (5, 10), \quad \eta_5 \stackrel{\wedge}{=} 7, 11, 13, 14$ (also $\eta_2 = t + t^2 + t^4 + t^8$ usw.). Wir starten mit $1 = \eta_2 + (1 + \eta_2)$.
Anwendung des Algorithmus mit $\xi = \eta_3$ auf $(1 + \eta_2)$ liefert $1 = \eta_2 + (\eta_2 + \eta_3) + (1 + \eta_3)$ (beachte $\eta_2 \eta_3 = \eta_2$).
Anwendung mit $\xi = \eta_4$ (beachte $\eta_2 \eta_4 = \eta_3 + \eta_5$) auf η_2 und η_4 auf $(1 + \eta_3)$ (beachte $\eta_3 \eta_4 = \eta_2 + \eta_5$) liefert

$$1 = (\eta_3 + \eta_5) + (\eta_2 + \eta_3 + \eta_5) + (\eta_2 + \eta_3) + (\eta_2 + \eta_4 + \eta_5) + (\eta_1 + \eta_2 + \eta_3 + \eta_4 + \eta_5).$$

Damit sind wir fertig. Im übrigen war der letzte Summand zu erwarten, denn für den Faktor $1 + t$ von $t^n - 1$ erhalten wir

$$1 = (1 + t)(t^{n-2} + t^{n-4} + \ldots + t) + 1 \cdot (1 + t + \ldots + t^{n-1})$$

und damit $\eta_1 + \eta_2 + \eta_3 + \eta_4 + \eta_5$ als primitve Idempotente für $\tilde{M}_{1+t}$.

Kapitel 3

Algebraisch-geometrische Codes

3.1 Hilfsmittel algebraischer Funktionenkörper

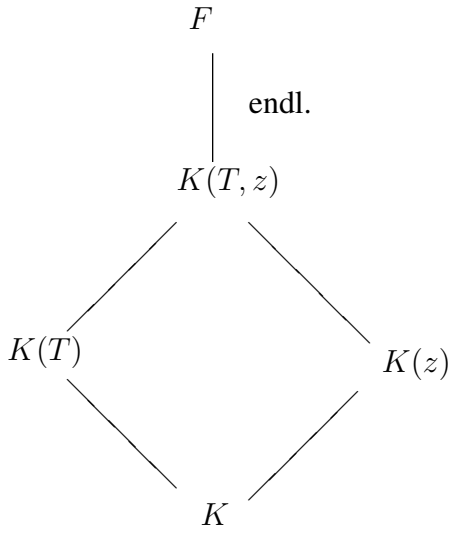
3.1 Definition. Ein **algebraischer Funktionenkörper** F **in einer Variablen** über einem Körper K ist ein Oberkörper von K, zu dem ein über K transzendentes Element $T \in F$ existiert, so dass $F/K(T)$ endlich ist.

Im folgenden schreiben wir nur "Funktionenkörperßtatt "algebraischer Funktionenkörper". Die Elemente von K heißen Konstanten.

3.2 Lemma. *Es sei F/K ein Funktionenkörper.*

1. $\tilde{K} := \{z \in F \mid \quad z/K$ *algebraisch* $\}$ *heißt* **Konstantenkörper** *zu F/K. K heißt im Fall $K = \tilde{K}$* **algebraisch abgeschlossen** *in F, bzw.* **voller Konstantenkörper** *zu F/K.*

2. *Für $z \in F$ gilt: z/K transzendent $\iff [F : K(z)] < \infty$.*



Beweis. 1. Offenbar ist $\tilde{K}$ ein Körper.

2. Wir werten das obenstehende Diagramm aus:
   Es ist $[F : K] = \infty$. Für z/K algebraisch ist $K(z)/K$ endlich, also $[F : K(z)] = \infty$. Für z/K transzendent ist wegen $\infty > [F : K(T)] \geq [K(T, z) : K(T)]$ dann $z/K(T)$ algebraisch. Dies impliziert aber auch $T/K(z)$ algebraisch (!). Folglich ist $[K(T, z) : K(z)]$ und damit auch $F/K(z)$ endlich.

□

3.3 Definition. Ein **Bewertungsring** eines Funktionenkörpers F/K ist ein Teilring R von F mit den Eigenschaften:

1. $K \subset R \subset F$,
2. $\forall z \in F : \quad z \in R \vee z^{-1} \in R$.

3.4 Lemma. *Ein Bewertungsring R von F/K ist ein lokaler Ring (mit maximalem Ideal $\mathfrak{p}$). Es gilt $\tilde{K} \subseteq R$ und $\tilde{K} \cap \mathfrak{p} = \{0\}$.*

Beweis. 1. Wir zeigen, dass $\mathfrak{p} := R \backslash U(R)$ ein Ideal ist. Zu $x, y \in \mathfrak{p}$ und $z \in R$ ist $xz \in R\backslash U(R) = \mathfrak{p}$; wegen $x + y = x(1 + \frac{y}{x}) = y(1 + \frac{y}{x})$ gilt auch $x + y \in \mathfrak{p}$.

2. Es sei $z \in \tilde{K}$. Im Fall $z \notin R$ ist $\frac{1}{z} \in R$. Da aber z/K algebraisch ist, ist es auch $\frac{1}{z}$, und es besteht eine Gleichung $z^{-1}(a_r z^{-r+1} + \ldots + a_1) = -1$ mit $a_i \in K$. Hiernach ist $z \in K[z^{-1}] \subseteq R$. Widerspruch.
   Also gilt für alle $z \in \tilde{K}\backslash\{0\}$ sowohl $z \in R$ als auch $z^{-1} \in R$, also $z \in U(R)$.

□

3.5 Lemma. (ohne Beweis) *Ein Bewertungsring R von F/K ist Hauptidealring. Jedes Ideal $I \neq 0$ von R ist von der Form $(\pi R)^m$ für $\mathfrak{p} = \pi R$ und $m \in \mathbb{Z}^{\geq 0}$ geeignet.*

3.6 Definition. Eine **Stelle** $\mathfrak{p}$ eines Funktionenkörpers ist das maximale Ideal eines Bewertungsrings R. $\pi \in \mathfrak{p}$ mit $\mathfrak{p} = \pi R$ heißt **Primelement** von $\mathfrak{p}$, **lokaler Parameter** oder **uniformisierendes Element**. Mit $\mathbb{P}_F$ bezeichnen wir die Menge aller Stellen von F/K.

Bemerkung Eine Stelle $\mathfrak{p}$ legt den zugehörigen Bewertungsring R mittels $R = \{z \in F \mid z^{-1} \notin \mathfrak{p}\}$ eindeutig fest.

3.7 Definition. Eine **diskrete Bewertung** von F/K ist eine Funktion $\nu : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ mit den Eigenschaften:

1. $\nu(x) = \infty \Longleftrightarrow x = 0$;
2. $\nu(xy) = \nu(x) + \nu(y) \quad \forall x, y \in F$;
3. $\nu(x + y) \geq \min\{\nu(x), \nu(y)\} \quad \forall x, y \in F$;
4. $\exists z \in F \quad : \nu(z) = 1$;

5. $\nu(x) = 0 \quad \forall x \in K^\times$.

Bemerkung Es gelten $\nu(1) = 0, \quad \nu(\frac{1}{x}) = -\nu(x), \quad \nu(-x) = \nu(x)$. Gilt $\nu(x) \neq \nu(y)$, so ist $\nu(x+y) = \min\{\nu(x), \nu(y)\}$.

(*Beweis.* Es sei $\nu(x) < \nu(y)$. Dann folgt $\nu(x) = \nu(x+y+(-y)) \geq \min\{\nu(x+y), \nu(+y)\} = \nu(x+y) \geq \nu(x)$.) □

Bemerkung Es sei $\mathfrak{p}$ eine Stelle von F/K mit Primelement π. Dann lässt sich $z \in F^\times$ eindeutig in der Form $z = \pi^n u$ mit $n \in \mathbb{Z}$ und $u \in U(R)$ schreiben.

3.8 Satz. *Die Funktion* $\nu_\mathfrak{p} : F \longrightarrow \mathbb{Z} \cup \{\infty\} : \left\{ {}^{0}_{z=\pi^n u} \right\} \mapsto \left\{ {}^{\infty}_{n} \right\}$ *ist eine diskrete Bewertung von* F. *Für sie gilt*

$$R = R_\mathfrak{p} = \{z \in F \mid \nu_\mathfrak{p}(z) \geq 0\}, \quad \mathfrak{p} = \{z \in F \mid \nu_\mathfrak{p}(z) > 0\}.$$

Für jede diskrete Bewertung ist $\mathfrak{p} := \{z \in F \mid \nu(z) > 0\}$ *eine Stelle von* F/K *mit zugehörigem Bewertungsring* $R = \{z \in F \mid \nu(z) \geq 0\}$.

3.9 Definition. Für $\mathfrak{p} \in \mathbb{P}_F$ heißt die Abbildung $\bar{} : F \longrightarrow R/\mathfrak{p} \cup \{\infty\} : \left\{ {}^{x \in R}_{x \notin R} \right\} \mapsto \left\{ {}^{x+\mathfrak{p}}_{\infty} \right\}$ **Restklassenabbildung**. $[R/\mathfrak{p} : K]$ heißt **Grad** $\deg \mathfrak{p}$ von $\mathfrak{p}$.

Bemerkung (ohne Beweis)

1. $\deg \mathfrak{p} \leq [F : K(T)]$.
2. Für $z \in F$ und $\mathfrak{p} \in \mathbb{P}_F$ heißt $\mathfrak{p}$ **Nullstelle, Polstelle** von z, falls $\nu_\mathfrak{p}(z) \left\{ {}^{>0}_{<0} \right\}$ gilt.
3. Für $z \in F$ transzendent über K besitzt z wenigstens eine Nullstelle und einen Pol. Die Anzahl von Null- bzw. Polstellen ist endlich. $\sharp \mathbb{P}_F = \infty$.

Beispiel: Rationaler Funktionenkörper und seine Bewertungen.

Im folgenden sei K der volle Konstantenkörper zu F/K.

3.10 Definition. Die additive freie Gruppe

$$D_F := \left\{ D = \sum_{\mathfrak{p} \in \mathbb{P}_F} n_\mathfrak{p} \mathfrak{p} \mid n_\mathfrak{p} \in \mathbb{Z}, \quad n_\mathfrak{p} = 0 \text{ für fast alle } \mathfrak{p} \right\}$$

heißt **Divisorengruppe** zu F/K, ihre Elemente **Divisoren**. Unter dem **Support** $\mathrm{supp} D$ eines Divisors D verstehen wir $\mathrm{supp} D := \{\mathfrak{p} \in \mathbb{P}_F \mid n_\mathfrak{p} \neq 0\}$. $D = \mathfrak{p}$ für ein $\mathfrak{p} \in \mathbb{P}_F$ heißt **Primdivisor**.

Auf D_F erhalten wir eine partielle Ordnung "$\leq$mittels

$$D_1 = \sum_{\mathfrak{p} \in \mathbb{P}_F} n_\mathfrak{p} \mathfrak{p} \leq D_2 = \sum_{\mathfrak{p} \in \mathbb{P}_F} m_\mathfrak{p} \mathfrak{p} \Longleftrightarrow \forall \mathfrak{p} \in \mathbb{P}_F : n_\mathfrak{p} \leq m_\mathfrak{p}.$$

Wir schreiben zudem $\nu_{\mathfrak{p}}(D_1) = n_{\mathfrak{p}}$. Ein Divisor $D \geq 0$ heißt **positiv** bzw. **effektiv**.
Die Abbildung

$$\deg : D_F \longrightarrow \mathbb{Z} : \sum_{\mathfrak{p}\in\mathbb{P}_F} n_{\mathfrak{p}}\mathfrak{p} \mapsto \sum_{\mathfrak{p}\in\mathbb{P}_F} n_{\mathfrak{p}} \deg \mathfrak{p}$$

heißt **Grad** und ist ein Homomorphismus.

3.11 Definition. Für $x \in F^\times$ heißt $(x) := \sum_{\mathfrak{p}\in\mathbb{P}_F} \nu_{\mathfrak{p}}(x)\mathfrak{p}$ **Hauptdivisor**. Die Gruppe P_F der Haupdivisoren von F/K ist eine Untergruppe von D_F. Die Faktorgruppe $C_F := D_F/P_F$ heißt **Divisorklassengruppe** von F/K.

Bemerkung Zwei Divisoren $D_1, D_2 \in D_F$ heißen **äquivalent**, falls $D_1P_F = D_2P_F$ gilt, d.h. falls $x \in F^\times$ mit $D_1 = D_2 + (x)$ existiert.

3.12 Definition. Unter dem **Riemann-Roch-Raum** $\mathcal{L}(A)$ eines Divisors $A \in D_F$ verstehen wir den K - Vektorraum

$$\mathcal{L}(A) := \{x \in F \mid (x) + A \geq 0\} \cup \{0\}.$$

$\dim A := \dim \mathcal{L}(A)$ heißt **Dimension** des Divisors A.

Bemerkungen

1. Für $x \in F$ gilt: $x \in \mathcal{L}(A) \iff \nu_{\mathfrak{p}}(x) \geq -\nu_{\mathfrak{p}}(A) \quad \forall \mathfrak{p} \in \mathbb{P}_F$.
2. $\mathcal{L}(A)$ ist genau dann nicht trivial, wenn $\tilde{A} \in AP_F$ mit $\tilde{A} \geq 0$ existiert.
3. $\forall \hat{A} \in AP_F : \mathcal{L}(\hat{A}) \cong \mathcal{L}(A)$.
4. $\mathcal{L}(0) = K$.
5. $A < 0 \Longrightarrow \mathcal{L}(A) = \{0\}$.

3.13 Satz. (ohne Beweis) *Für $x \in F^\times \setminus K$ gilt $\deg(x) = 0$. (Dies folgt etwa aus der Produktformel für die Bewertungen von F.)*

3.14 Korollar. *1. $\tilde{A} \in AP_F$ impliziert $\dim A = \dim \tilde{A}$ und $\deg A = \deg \tilde{A}$.*

2. $\deg A < 0$ impliziert $\dim A = 0$.

3. Für $\deg A = 0$ sind äquivalent:

$$(\alpha) A \in P_F, \quad (\beta) \dim A \geq 1, \quad (\gamma) \dim A = 1.$$

Beweis. 1. Klar nach obiger Bemerkung (3) und (3.13).

2. Im Fall $\dim A > 0$ existiert nach obiger Bemerkung (2) ein $\tilde{A} \in AP_F$ mit $\deg \tilde{A} \geq 0$. Nach (1) folgt $\deg A = \deg \tilde{A} \geq 0$ im Widerspruch zur Voraussetzung.

3. $(\alpha) \Longrightarrow (\beta)$: Für $A = (a)$ mit $a \in F^\times$ ist $a^{-1} \in \mathcal{L}(A)$.
   $(\beta) \Longrightarrow (\gamma)$: Es existiert $\tilde{A} \in AP_F$ mit $\tilde{A} \geq 0$. Wegen $\deg A = 0$ ist nach (1) auch $\deg \tilde{A} = 0$, also notwendig $\tilde{A} = 0$.
   Nach obiger Bemerkung (4) $\wedge$ (3) ist $\mathcal{L}(A) \cong K$, also $\dim A = 1$.
   $(\gamma) \Longrightarrow (\alpha)$: Wegen $\dim A = 1$ existiert $0 \neq z \in \mathcal{L}(A)$, also gilt $(z) + A \geq 0$. Jedoch ist $\deg((z) + A) = 0$ nach Voraussetzung und (3.13). Dies bedingt $(z) + A = 0$, also ist $A = -(z) = (z^{-1}) \in P_F$.

□

Bemerkung Für den Nulldivisor 0 gilt $\deg(0) - \dim(0) + 1 = 0$.

3.15 Satz. (ohne Beweis) $g := \max\{\deg A - \dim A + 1 \mid A \in D_F\}$ *existiert in* $\mathbb{Z}^{\geq 0}$. g *heißt* **Geschlecht** *von* F/K. *Es existiert* $c = c(F/K) \in \mathbb{Z}^{\geq 0}$ *mit* $\dim A = \deg A + 1 - g$ *für alle* $A \in D_F$ *mit* $\deg A \geq c$.

Beispiel $F = K(T)$ hat das Geschlecht $g = 0$. Dazu sei $\mathfrak{p}_\infty$ der Poldivisor zu T. Für $r \in \mathbb{Z}^{\geq 0}$ betrachten wir $\mathcal{L}(r\mathfrak{p}_\infty)$. Offenbar gilt $1, T, \ldots, T^r \in \mathcal{L}(r\mathfrak{p}_\infty)$, was $r + 1 \leq \dim(r\mathfrak{p}_\infty) = \deg(r\mathfrak{p}_\infty) + 1 - g = r + 1 - g$ für hinreichend großes r impliziert. Wegen $g \geq 0$ muss also $g = 0$ gelten.

3.16 Definition. Zu $A \in D_F$ heißt $i(A) := \dim A - \deg A - 1 + g$ **Spezialitätsindex** von A. Im Fall $i(A) = 0$ heißt A **nicht-speziell**, für $i(A) > 0$ **speziell**.
Wir werden später sehen: Für $A \in D_F$ mit $\deg(A) \geq 2g - 1$ gilt $i(A) = 0$ (vgl. 3.30 (2)).

3.17 Bemerkung.
1. *Für* $\tilde{A} \in AP_F$ *gilt* $i(\tilde{A}) = i(A)$.
2. *Für* $A \in D_F$ *mit* $\dim A > 0$ *und* $\deg A < g$ *ist* $i(A) > 0$.
3. $i(0) = g$.

3.2 Geometrische Codes

Geometrische Goppa Codes lassen sich als Verallgemeinerungen von Reed-Solomon-Codes deuten. Zur Erinnerung: Wir hatten $n = q - 1, \quad \mathbb{F}_q^\times =< \beta >$, zu $k \in \{1, \ldots, n\}$ betrachteten wir $k - \dim$ Vektorräume $L_k := \{f(x) \in \mathbb{F}_q[x] \mid \deg f \leq k - 1\}$ nebst Spezialisierungen $\sigma : L_k \longrightarrow \mathbb{F}_q^n : f \mapsto (f(\beta), \ldots, f(\beta^n))$. σ ist $\mathbb{F}_q$ - lineare Abbildung; σ ist zudem injektiv, da ein Polynom vom Grad $< n$ keine n Nullstellen besitzt (mit Ausnahme des 0 - Polynoms). Es ist $C_k := \sigma(L_k)$ Unterraum von $\mathbb{F}_q^n$ der Dimension k, also ist C_k ein $[n, k]$ - Code. Zur Bestimmung des minimalen Abstands d_C sei $\mathbf{x} \in C_k$ mit $\mathbf{x} = \sigma(f)$. $\mathbf{x}$ genügt

$$\begin{aligned} wt(\mathbf{x}) &= n - \sharp\{i \in \{1, \ldots, n\} \mid f(\beta^i) = 0\} \\ &\geq n - \deg f \geq n - (k - 1). \end{aligned}$$

Also gilt $d_C \geq n + 1 - k$, andererseits haben wir $d_C \leq n + 1 - k$ nach Singleton, so dass C_k ein

maximum distance separable Code ist.

Bemerkung Die Codelänge n ist klein im Vergleich zur Alphabetgröße q.

Wir kommen nun zur Verallgemeinerung auf globale Funktionenkörper. Notation: $F/\mathbb{F}_q$ algebraischer Funktionenkörper vom Geschlecht g; $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ paarweise verschiedene Stellen von $F/\mathbb{F}_q$ vom Grad 1; $D = \mathfrak{p}_1 + \ldots + \mathfrak{p}_n$; G Divisior von $F/\mathbb{F}_q$ mit supp$G \cap$ supp$D = \emptyset$.
Damit können wir nun einen Geometrischen Goppa Code $C_{\mathcal{L}}(D, G)$ - assoziiert zu den Divisoren D, G - wie folgt erklären:

$$C_{\mathcal{L}}(D, G) := \{(x + \mathfrak{p}_1, \ldots, x + \mathfrak{p}_n) \mid x \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n$$

mittels der Restklassenabbildung

$$\sigma : \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n : x \mapsto (x + \mathfrak{p}_1, \ldots, x + \mathfrak{p}_n).$$

Man beachte, dass $\nu_{\mathfrak{p}_i}(x) \geq 0$ wegen $x \in \mathcal{L}(G)$ und supp$(G) \neq \mathfrak{p}_i$ für $1 \leq i \leq n$ gilt.

3.18 Satz. *$C_L(D, G)$ ist ein $[n, k, d]$ Code mit $k = \dim G - \dim(G - D), d \geq n - \deg G$.*

Beweis. Nach Definition ist σ linear mit $\sigma(\mathcal{L}(G)) = C_{\mathcal{L}}(D, G)$. Es ist zudem

$$\begin{aligned} \ker \sigma &= \{x \in \mathcal{L}(G) \mid \nu_{\mathfrak{p}_i}(x) > 0, \quad 1 \leq i \leq n\} \\ &= \mathcal{L}(G - D). \end{aligned}$$

Als Konsequenz erhalten wir $k = \dim C_{\mathcal{L}}(D, G) = \dim \mathcal{L}(G) - \dim \mathcal{L}(G - D)$ (Homomorphiesatz für Vektorräume). Die Aussage über den Minimalabstand macht nur im Fall $C_{\mathcal{L}}(D, G) \neq \{0\}$ Sinn. Wir setzen dies im folgenden voraus. Dann sei $x \in \mathcal{L}(G)$ mit $w(\sigma(x)) = d$. Hierfür sind dann gerade $n - d$ Stellen $\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_{n-d}} \in$ supp(D) Nullstellen von x, folglich gilt: $0 \neq x \in \mathcal{L}(G - (\mathfrak{p}_{i_1} + \ldots + \mathfrak{p}_{i_{n-d}}))$. Gemäß 3.14(2) erhalten wir so $0 \leq \deg(G - (\mathfrak{p}_{i_1} + \ldots + \mathfrak{p}_{i_{n-d}})) = \deg G - (n - d)$ und damit $d \geq n - \deg G$. □

3.19 Korollar. *Für $\deg(G) < n$ ist die Restklassenabbildung $\sigma : \mathcal{L}(G) \longrightarrow C_{\mathcal{L}}(D, G)$ injektiv; es gelten:*

1. *$C_{\mathcal{L}}(D, G)$ ist ein $[n, k, d]$ - Code mit $d \geq n - \deg(G)$, $k = \dim G \geq \deg(G) + 1 - g$. Also folgt $k + d \geq n + 1 - g$.*
2. *Ist zusätzlich $2g - 2 < \deg(G) < n$ erfüllt, so ist $k = \deg(G) + 1 - g$.*
3. *Ist $\{x_1, \ldots, x_k\}$ eine Basis von $\mathcal{L}(G)$, so ist*

$$M = \begin{pmatrix} x_1 + \mathfrak{p}_1 & x_1 + \mathfrak{p}_2 & \ldots & x_1 + \mathfrak{p}_n \\ \vdots & \vdots & & \vdots \\ x_k + \mathfrak{p}_1 & x_k + \mathfrak{p}_2 & \ldots & x_k + \mathfrak{p}_n \end{pmatrix}$$

eine Erzeugermatrix von $C_{\mathcal{L}}(D, G)$.

Beweis. Wegen $\deg(G-D) = \deg(G) - n < 0$ ist $\mathcal{L}(G-D) = \{0\}$. Wegen $\mathcal{L}(G-D) = \ker\sigma$ ist σ injektiv. Der Rest folgt unmittelbar aus 3.18 und 3.30 (2). □

Bemerkung Für $\deg(G) < n$ haben wir $n+1-g \leq k+d$ (Singleton) $\leq n+1$. Im Fall $g=0$ (rationale Funktionenkörper) sind die konstruierten geometrischen Goppa Codes also MDS-Codes (maximum distance separable).

3.20 Definition. $d^* := n - \deg(G)$ heißt **designierter Abstand** von $C_{\mathcal{L}}(D,G)$.

3.21 Bemerkung. *Es seien* $\dim(G) > 0$ *und* $d^* = n - \deg(G) > 0$. *Dann ist genau dann* $d^* = d$, *falls* $D' \in D_F$ *mit* $0 \leq D' \leq D, \quad \deg(D') = \deg(G)$ *und* $\dim(G-D') > 0$ *existiert.*

Beweis. "$\Longrightarrow$" Es existiert $0 \neq x \in \mathcal{L}(G)$, so dass das Codewort $(x+\mathfrak{p}_1, \ldots, x+\mathfrak{p}_n) \in C_{\mathcal{L}}(D,G)$ genau $n-d = n-d^* = \deg(G)$ Nullkoordinaten besitzt, etwa $x + \mathfrak{p}_{i_j} = \mathfrak{p}_{i_j} \quad (1 \leq j \leq \deg(G))$. Setzen wir $D' := \sum_{j=1}^{\deg(G)} \mathfrak{p}_{i_j}$, so gelten: $0 \leq D' \leq D, \quad \deg(D') = \deg(G)$ sowie $\dim(G-D') > 0$ (wegen $x \in \mathcal{L}(G-D')$).
"$\Longleftarrow$" Besitzt D' die angeführten Eigenschaften, so wählen wir $0 \neq y \in \mathcal{L}(G-D')$. Das Gewicht des entsprechenden Codewortes $(y+\mathfrak{p}_1, \ldots, y+\mathfrak{p}_n)$ ist dann $n - \deg G = d^*$, also gilt $d = d^*$.
□

3.22 Definition. Ein **Adel** von F/K ist eine Abbildung $\underline{\alpha} : \mathbb{P}_F \longrightarrow F : \mathfrak{p} \mapsto \alpha_{\mathfrak{p}}$ mit $\alpha_{\mathfrak{p}} \in R_{\mathfrak{p}}$ für fast alle $\mathfrak{p}$. (Schreibweise: $\underline{\alpha} = (\alpha_{\mathfrak{p}}) = (\alpha_{\mathfrak{p}})_{\mathfrak{p}\in\mathbb{P}_F}$)

Die Adele bilden bzgl. komponentenweiser Verknüpfung eine K - Algebra $\mathcal{A}_F$. F lässt sich hierin diagonal einbetten. Bewertungen von F lassen sich auf $\mathcal{A}_F$ fortsetzen mittels $\nu_{\mathfrak{p}}(\underline{\alpha}) := \nu_{\mathfrak{p}}(\alpha_{\mathfrak{p}})$.

3.23 Definition. Für $A \in D_F$ definieren wir einen Teilraum $\mathcal{A}_F(A)$:
$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F \mid \nu_{\mathfrak{p}}(\alpha) \geq -\nu_{\mathfrak{p}}(A) \quad \forall \mathfrak{p} \in \mathbb{P}_F\}$.

Beispiel: Für $A \in D_F$ ist $\mathcal{A}_F \cap \iota(F) = \iota(\mathcal{L}(A))$, wenn $\iota : F \longrightarrow \mathcal{A}_F : x \longrightarrow (x)_{\mathfrak{p}}$ die Einbettung von F in $\mathcal{A}_F$ ist.

3.24 Satz. (ohne Beweis) *Für den Spezialitätsindex* $i(A)$ *von* $A \in D_F$ *gilt:* $i(A) = \dim(\mathcal{A}_F/(\mathcal{A}_F(A)+F))$.

Bemerkung Hiernach ist

$$\dim(\mathcal{A}_F/(\mathcal{A}_F(0)+F)) = i(0) = \dim(0) - \deg(0) + g - 1 = 1 - 0 + g - 1 = g.$$

3.25 Definition. Ein **Weil Differential** von F/K ist eine K - lineare Abbildung $\omega : \mathcal{A}_F \longrightarrow K$, die für einen geeigneten Divisor $A \in D_F$ auf $\mathcal{A}_F(A) + F$ verschwindet.
$\Omega_F := \{\omega \mid \omega$ Weil Differential von $F/K\}$ heißt **Modul der Weil Differentiale.** Wir setzen noch

$$\Omega_F(A) := \{\omega \in \Omega_F \mid \omega \mid_{\mathcal{A}_F(A)+F} = 0\}.$$

3.26 Bemerkungen. *1.* Ω_F *ist ein* K *- Vektorraum,* $\Omega_F(A)$ *Unterraum von* Ω_F*.*

2. *Für* $A \in D_F$ *gilt* $\dim\ \Omega_F(A) = i(A)$.
($\Omega_F(A)$ *ist isomorph zu* $\mathrm{Hom}(\mathcal{A}_F/(\mathcal{A}_F(A)+F), K)$*, und die Aussage folgt somit aus (3.24).)*

3. $\Omega_F \neq 0$.
(Für $A \in D_F$ *mit* $\deg(A) \leq -2$ *erhalten wir* $\dim\ \Omega_F(A) = i(A) = \dim\ A - \deg A + g - 1 \geq 1$.*)*

4. *Mittels* $F \times \Omega_F \longrightarrow \Omega_F : (x, \omega) \mapsto x\omega := (x\cdot\ \ )$ *wird* Ω_F *zu einem* F *- Vektorraum.*
(Falls ω *auf* $\mathcal{A}_F(A)+F$ *verschwindet, so verschwindet* $x\omega$ *auf* $\mathcal{A}_F(A+(x))+F$*.)*

5. $\dim_F\ \Omega_F = 1$ *(ohne Beweis).*

3.27 Definition. 1. **Divisor** (ω) eines Weil Differentials $\omega \neq 0$ ist das $A \in D_F$ mit

- ω verschwindet auf $\mathcal{A}_F(A)+F$,
- falls ω auf $\mathcal{A}_F(B)+F$ für $B \in D_F$ verschwindet, gilt $B \leq (A)$.

2. Für $0 \neq \omega \in \Omega_F$ und $\mathfrak{p} \in \mathbb{P}_F$ setzen wir $\nu_{\mathfrak{p}}(\omega) := \nu_{\mathfrak{p}}((\omega))$.

3. $\mathfrak{p} \in \mathbb{P}_F$ heißt **Nullstelle (Pol)** von ω im Fall $\nu_{\mathfrak{p}}(\omega) > 0 \quad (\nu_{\mathfrak{p}}(\omega) < 0)$. Im Fall $\nu_{\mathfrak{p}}(\omega) \geq 0$ heißt ω **regulär** in $\mathfrak{p} \in \mathbb{P}_F$. ω heißt **regulär**, falls es an allen $\mathfrak{p} \in \mathbb{P}_F$ regulär ist.

4. $W \in D_F$ heißt **kanonischer Divisor**, falls $W = (\omega)$ für ein $\omega \in \Omega_F$ gilt.

3.28 Bemerkungen. *1.* $\Omega_F(A) = \{\omega \in \Omega_F \mid \omega = 0 \vee (\omega) \geq A\}$,
$\Omega_F(0) = \{\omega \in \Omega_F \mid \omega$ *regulär* $\}$.

2. $\dim\ \Omega_F(0) = g$ *gemäß Bemerkung (3.26)(2).*

3. $x \in F^\times$, $0 \neq \omega \in \Omega_F : (x\omega) = (x) + (\omega)$.
(Denn $\omega\,|_{\mathcal{A}_F(A)+F} = 0$ *impliziert* $x\omega\,|_{A_F(A+(x))+F} = 0$*, also gilt* $(\omega)+(x) \leq (x\omega)$*. Analog folgt* $(x\omega)+(x^{-1}) \leq (x^{-1}x\omega) = (\omega)$ *und insgesamt* $(\omega)+(x) \leq (x\omega) \leq -(x^{-1})+(\omega) = (x)+(\omega)$*.)*

4. *Je zwei kanonische Divisoren sind äquivalent.*
(Konsequenz von 3.26(5) und 3.28(3).)

3.29 Satz. (Riemann-Roch) (ohne Beweis) *Es seien* $A, W \in D_F$ *und* W *kanonisch. Dann gilt* $\dim A = \deg(A) + 1 - g + \dim(W - A)$.

3.30 Korollar. *1. Für* $W \in D_F$ *kanonisch gilt* $\deg W = 2g-2$, $\dim W = g$*, also* $i(W) = \dim(W) - \deg(W) + g - 1 = 1$.

2. *Für* $A \in D_F$ *mit* $\deg(A) \geq 2g-1$ *gilt* $i(A) = 0$.

Beweis. Riemann-Roch liefert für $A = 0$: $1 = \dim(0) = \deg(0) + 1 - g + \dim(W - 0)$ bzw. $\dim(W) = g$. Für $A = W$ folgt $g = \dim(W) = \deg(W)+1-g+\dim(W-W)$ bzw. $\deg W = 2g-2$. Wegen $\deg(A) \geq 2g - 1, \deg(W) = 2g - 2$ ist $\deg(W - A) < 0$, also $\dim(W - A) = 0$ nach 3.14(2). □

Bemerkung Die Abschätzung in (2) ist nach (1) bestmöglich.

3.31 Definition. Es sei $\mathfrak{p} \in \mathbb{P}_F$. Wir setzen

$$\iota_{\mathfrak{p}} : F \longrightarrow \mathcal{A}_F : \alpha \mapsto \underline{\alpha} \text{ mit } \alpha_{\mathfrak{p}} = \alpha \text{ und } \alpha_{\mathfrak{q}} = 0 \quad \forall \mathfrak{q} \neq \mathfrak{p}.$$

Dann heißt $\omega_{\mathfrak{p}} : F \longrightarrow K : x \mapsto \omega(\iota_{\mathfrak{p}}(x))$ **lokale Komponente** von $\omega \in \Omega_F$.

3.32 Hilfssatz. (ohne Beweis) *Es seien $\omega \in \Omega_F$ und $\underline{\alpha} = (\alpha_{\mathfrak{p}}) \in \mathcal{A}_F$. Dann ist $\omega_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) \neq 0$ höchstens für endlich viele $\mathfrak{p}$, und es gelten:*

$$\omega(\alpha) = \sum_{\mathfrak{p} \in \mathbb{P}_F} \omega_{\mathfrak{p}}(\alpha_{\mathfrak{p}}), \quad \sum_{\mathfrak{p} \in \mathbb{P}_F} \omega_{\mathfrak{p}}(1) = 0.$$

Ein Weil Differential ist durch jede seiner lokalen Komponenten bereits eindeutig bestimmt.

3.33 Definition. Es seien G und $D = \mathfrak{p}_1 + \ldots + \mathfrak{p}_n$ Divisoren aus D_F wie zuvor. Dann erhalten wir einen Code $C_\Omega(D, G) \subseteq \mathbb{F}_q^n$ mittels

$$C_\Omega(D, G) := \{(\omega_{\mathfrak{p}_1}(1), \ldots, \omega_{\mathfrak{p}_m}(1)) \mid \omega \in \Omega_F(G - D)\}.$$

3.34 Satz. (ohne Beweis) *$C_\Omega(D, G)$ ist ein $[n, k', d']$ - Code mit den Parametern $k' = i(G-D)-i(G)$, $d' \geq \deg(G) - (2g - 2)$.*
Gilt zusätzlich $\deg(G) > 2g-2$, so erhalten wir $k' = i(G - D) \geq n+g-1-\deg(G)$. Ist außerdem $\deg(G) < n$, so wird $k' = n + g - 1 - \deg(G)$.

3.35 Satz. (ohne Beweis) *Es ist $C_{\mathcal{L}}(D, G)^\perp = C_\Omega(D, G)$.*

Goppa Codes über dem rationalen Funktionskörper $\mathbb{F}_q(x)$

3.36 Bemerkung. *1. Es existieren $q+1$ Stellen vom Grad 1, nämlich $P_\alpha \stackrel{\wedge}{=} x-\alpha \quad (\alpha \in \mathbb{F}_q), P_\infty$.*

2. *Es sei $C = C_{\mathcal{L}}(D, G)$ Goppa-Code mit Parametern $[n, k, d]$. Für $0 \leq \deg G \leq n - 2$ gilt $k \stackrel{(3.19)}{=} 1 + \deg G, \quad d = n - \deg G$, C ist ein Maximum Distance Separable Code . (Letzteres folgt aus 3.21 mittels $D' = \mathfrak{p}_1+\ldots+\mathfrak{p}_{k-1}$, da dann $\dim(G-D') = \deg(G-D')+1-g = 1 > 0$ gilt.)*

3.37 Satz. *Für $n \leq q$ existieren paarweise verschiedene Elemente $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ sowie $v_1, \ldots, v_n \in \mathbb{F}_q^\times$ mit*
$C = \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) \mid f(T) \in \mathbb{F}_q[T], \deg f \leq k - 1\}$,
$G_C = (v_j \alpha_j^{i-1})_{1 \leq i \leq k,\ 1 \leq j \leq n}$.

Beweis. Es sei $D = \mathfrak{p}_1 + \ldots + \mathfrak{p}_n$ und $\mathfrak{p} \neq \mathfrak{p}_i \quad (1 \leq i \leq n)$ eine weitere Stelle vom Grad 1. Wähle $\mathfrak{q} \neq \mathfrak{p}$ vom Grad 1, etwa $\mathfrak{q} = \mathfrak{p}_1$. Riemann-Roch: $\dim(\mathfrak{q} - \mathfrak{p}) = 1, \quad \mathfrak{q} - \mathfrak{p}$ ist nach 3.14 (3) Hauptdivisor, etwa (z). Dann erzeugt z den Funktionenkörper $\mathbb{F}_q(T), \mathfrak{p}$ ist Poldivisor zu z. Schreibe $\mathfrak{p} = \mathfrak{p}_\infty$. Nach der Vorbemerkung ist $\deg G = k - 1 \geq 0$, also ist $\deg((k-1)P_\infty - G) = 0$, wegen Riemann-Roch und 3.14 (3) demnach Hauptdivisor (u) mit $0 \neq u \in \mathbb{F}_q(T)$. Die Elemente $u, zu, \ldots, z^{k-1}u$ liegen in $\mathcal{L}(G)$ und sind $\mathbb{F}_q$ - linear unabhängig. Wegen $\dim G = k$ bilden sie eine Basis von $\mathcal{L}(G)$. Dies liefert $\mathcal{L}(G) = \{uf(z) \mid f \in \mathbb{F}_q[z] \text{ mit } \deg f \leq k-1\}$. Mittels $\alpha_i := z + \mathfrak{p}_i, \quad v_i := u + \mathfrak{p}_i$ wird $(uf(z)) + \mathfrak{p}_i = (u + \mathfrak{p}_i)(f(z) + \mathfrak{p}_i) = v_i f(\alpha_i)$. Das Codewort von C, welches zu uz^j korrespondiert, ist $(v_1\alpha_1^j, \ldots, v_n\alpha_n^j)$, woraus die Gestalt von G_C folgt. □

3.38 Definition. Es seien $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ paarweise verschieden, $v_1, \ldots, v_n \in \mathbb{F}_q^\times$. Dann heißt $GRS_k(\mathfrak{a}, \mathfrak{v}) = \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) \mid f(x) \in \mathbb{F}_q[x], \deg f \leq k-1\}$ **verallgemeinerter Reed Solomon Code**.

Bemerkung

1. $GRS_k(\mathfrak{a}, \mathfrak{v})$ wird ebenso durch G_C aus Satz 3.37 festgelegt.
2. Für $n = q - 1, \mathbb{F}_q^\times =< \beta >, \mathfrak{a} = (\beta, \beta^2, \ldots, \beta^n), \mathfrak{v} = (1, \ldots, 1)$ wird GRS_k zu einem gewöhlichen Reed-Solomon-Code.

3.39 Satz. *Jeder verallgemeinerte Reed Solomon Code ist geometrischer Goppa Code (und vice versa gemäß Satz 3.37).*

Beweis. Betrachte $F = \mathbb{F}_q(T), \quad \mathfrak{p}_i \stackrel{\triangle}{=} T - \alpha_i \quad (1 \leq i \leq n), \mathfrak{p} = \mathfrak{p}_\infty$. Wähle $u \in F$ mit $u + \mathfrak{p}_i = v_i \quad (1 \leq i \leq n)$ (Approximationssatz). Setze $D := \mathfrak{p}_1 + \ldots + \mathfrak{p}_n$, $G := (k-1)\mathfrak{p}_\infty - (u)$. Dann liefert der Beweis des vorangehenden Satzes die Aussage $GRS_k(\mathfrak{a}, \mathfrak{v}) = C_{\mathcal{L}}(D, G)$. □

3.40 Definition. Es sei C ein Code der Länge n über dem Erweiterungskörper $\mathbb{F}_{q^m}$ von $\mathbb{F}_q$. Dann heißt $C\,|_{\mathbb{F}_q} := C \cap \mathbb{F}_q^n$ **Teilkörpercode** zu C.

Bemerkung Der Minimalabstand von $C\,|_{\mathbb{F}_q}$ ist mindestens so groß wie der von C, die Dimension dagegen im allgemeinen kleiner.

3.41 Definition. Es sei $n \mid (q^m - 1)$ und $\beta \in \mathbb{F}_{q^m}$ eine primitive n-te Einheitswurzel. Für $l \in \mathbb{Z}$ und $\delta \geq 2$ definieren wir einen Code $C(n, l, \delta)$ über $\mathbb{F}_{q^m}$ mittels Erzeugermatrix

$$H_1 := \left(\beta^{(j-1)(l+i-1)}\right)_{1 \leq i \leq \delta-1,\ 1 \leq j \leq n}.$$

Der Code $C := C(n, l, \delta)^\perp\,|_{\mathbb{F}_q}$ heißt BCH-Code mit designiertem Abstand δ.

Bemerkung Es ist $C = \{\mathfrak{c} \in \mathbb{F}_q^n \mid H_1\mathfrak{c} = \mathbf{0}\}$.

3.42 Satz. *Es seien n, m, β wie in 3.41. Wir betrachten den rationalen Funktionenkörper $F = \mathbb{F}_{q^m}(T)$ über $\mathbb{F}_{q^m}$. $\mathfrak{p}_0$ bzw. $\mathfrak{p}_\infty$ seien Nullstelle bzw. Pol von T. Für $i = 1, \ldots, n$ sei $\mathfrak{p}_i$ Nullstelle von $T - \beta^{i-1}$. Wir setzen $D_\beta := \mathfrak{p}_1 + \ldots + \mathfrak{p}_n$. Ferner seien $a, b, \in \mathbb{Z}$ mit $0 \leq a + b \leq n - 2$. Dann gilt:*

1. $C_{\mathcal{L}}(D_\beta, a\mathfrak{p}_0 + b\mathfrak{p}_\infty) = C(n, l, \delta)$ *mit* $l = -a, \delta = a + b + 2$.

2. *(ohne Beweis)* $C_{\mathcal{L}}(D_\beta, a\mathfrak{p}_0 + b\mathfrak{p}_\infty)^\perp = C_{\mathcal{L}}(D_\beta, r\mathfrak{p}_0 + s\mathfrak{p}_\infty)$ *mit* $r = -(a+1)$ *und* $s = n - b - 1$.

Beweis. 1. Die Elemente $T^{-a}T^j$ mit $0 \leq j \leq a + b$ bilden eine Basis von $\mathcal{L}(a\mathfrak{p}_0 + b\mathfrak{p}_\infty)$. Folglich ist die Matrix

$$\left(\beta^{(j-1)(i-1-a)}\right)_{1\leq j\leq a+b+1,\ 1\leq j\leq n}$$

eine Erzeugermatrix von $C_{\mathcal{L}}(D_\beta, a\mathfrak{p}_0 + b\mathfrak{p}_\infty)$. Mit $l := -a$ und $\delta := a + b + 2$ erhalten wir die Matrix aus (3.41).

□

3.43 Definition. Es sei $L = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_{q^m}$ mit $\sharp L = n$ sowie $g(T) \in \mathbb{F}_{q^m}[T]$ mit $\deg(g) = \tau \in \{1, \ldots, n-1\}$ und $g(\alpha_i) \neq 0 \quad \forall \alpha_i \in L$.
Wir definieren einen Code $C(L, g) \subseteq (\mathbb{F}_{q^m})^n$ mittels Erzeugermatrix
$H_2 = (\alpha_j^{i-1} g(\alpha_j)^{-1})_{1\leq i\leq \tau,\quad 1\leq j\leq n}$.
Hierzu heißt $\Gamma(L, g) : C(L, g)^\perp \mid_{\mathbb{F}_q}$ **klassischer Goppa Code** zum Polynom $g : \Gamma(L, g) = \{\mathfrak{c} \in \mathbb{F}_q \mid H_2\mathfrak{c} = \mathbf{0}\}$.

Bemerkung H_2 ist ein Spezialfall von G_C aus 3.37 für $v_i = g(\alpha_i)^{-1}$.

3.44 Satz. *Zusätzlich zu den Voraussetzungen in 3.43 seien* $\mathfrak{p}_i$ *die Nullstellen von* $T - \alpha_i \quad \forall \alpha_i \in L$, $\mathfrak{p}_\infty$ *Pol zu* T, $D_L = \mathfrak{p}_1 + \ldots + \mathfrak{p}_n$. *Ferner sei* G_0 *der Nulldivisor von* $g(T) : G_0 = \sum_{\substack{\mathfrak{p}\in\mathbb{P}_F \\ \nu_\mathfrak{p}(g)>0}} \nu_\mathfrak{p}(g)\mathfrak{p}$.

Dann gelten:

1. $C(L, g) = C_{\mathcal{L}}(D_L, G_0 - \mathfrak{p}_\infty)$,

2. $\Gamma(L, g) = C_{\mathcal{L}}(D_L, G_0 - \mathfrak{p}_\infty)^\perp \mid_{\mathbb{F}_q}$.

Beweis. Wegen 3.43 genügt der Nachweis von (1). Für $0 \leq j \leq t - 1$ ist $T^j g(T)^{-1}$ in $\mathcal{L}(G_0 - \mathfrak{p}_\infty)$ wegen $(T^j g(T)^{-1}) = j(\mathfrak{p}_0 - \mathfrak{p}_\infty) - (G_0 - t\mathfrak{p}_\infty) \geq -G_0 + \mathfrak{p}_\infty$. Wegen $\dim \mathcal{L}(G_0 - \mathfrak{p}_\infty) = t$ bilden die Elemente $T^j g(T)^{-1}$ eine Basis von $\mathcal{L}(G_0 - \mathfrak{p}_\infty)$. Folglich ist H_2 Erzeugermatrix von $C_{\mathcal{L}}(D_L, G_0 - \mathfrak{p}_\infty)$. Es gilt $C(L, g) = C_{\mathcal{L}}(D_L, G_0 - \mathfrak{p}_\infty)$. □

3.45 Korollar. *(1) (BCH Schranke) Der Minimalabstand eines BCH-Codes mit designiertem Abstand* δ *ist mindestens* δ.
(2) (Goppa Schranke, ohne Beweis) Der Minimalabstand eines klassischen Goppa Codes $\Gamma(L, g)$ *ist mindestens* $1 + \deg(g)$.

Beweis. (1) Gemäß 3.42(2) betrachten wir den Code $C_{\mathcal{L}}(D_\beta, r\mathfrak{p}_0 + s\mathfrak{p}_\infty) \mid_{\mathbb{F}_q}$. Der Minimalabstand von $C_{\mathcal{L}}(D_\beta, r\mathfrak{p}_0 + s\mathfrak{p}_\infty)$ ist nach 3.36 und 3.42(2)

$$d = n - \deg(r\mathfrak{p}_0 + s\mathfrak{p}_\infty) = n - r - s = n + a + 1 - n + b + 1 = a + b + 2 = \delta.$$

Dies gilt dann mindestens auch für den Teilkörpercode. □

Bemerkungen

1. Mittels der Teilkörpercodekonstruktion lassen sich Codes über $\mathbb{F}_q$ von beliebiger Länge realisieren.

2. Übergang vom rationalen Funktionenkörper auf beliebige Funktionenkörper bringt eine Reihe von Problemen mit sich.

Probleme: Es sei $F = \mathbb{F}_q(x, y)$, $\varphi(x, y) \in \mathbb{F}_q[x, y]$ mit $\varphi(x, y) = 0$.

1. Ist $\mathbb{F}_q$ voller Konstantenkörper zu F?

2. Geschlecht g ist zu berechnen.

3. Beschreibe Stellen von F (vom Grad 1) explizit!

4. Konstruiere Basis von $\mathcal{L}(G)$!

5. Beschreibung der Weil Differentiale.

6. Wie viele Stellen vom Grad 1 kann es geben?

3.3 Lange Codes

3.46 Definition. Für einen $[n, k, d]$ Code C über $\mathbb{F}_q$ setzen wir fest: $R = R(C) := k/n$ (Informationsrate), $\delta = \delta(C) := d/n$ (relativer Minimalabstand). Ferner seien $V_q := \{(\delta(C), R(C)) \in [0, 1]^2 \mid C$ Code über $\mathbb{F}_q\}$ sowie $U_q :\subseteq [0, 1]^2$ Menge der Häufungspunkte von V_q.

3.47 Satz. (Manin, ohne Beweis) *Es gibt eine stetige Funktion* $\alpha_q : [0, 1] \longrightarrow [0, 1]$ *mit* $U_q = \{(\delta, R) \mid 0 \leq \delta \leq 1, \quad 0 \leq R \leq \alpha_q(\delta)\}$. *Hierfür gelten:* $\alpha_q(0) = 1, \quad \alpha_q(\delta) = 0$ *für* $1-q^{-1} \leq \delta \leq 1$, α_q *ist monoton fallend für* $0 \leq \delta \leq 1 - q^{-1}$.

Die exakten Werte für $\alpha_q(\delta)$ sind nicht bekannt. Wir zitieren einige Schranken. Dazu benötigen wir noch die q - äre Entropie Funktion $H_q : [0, 1 - q^{-1}] \longrightarrow \mathbb{R}$ definiert durch $H_q(0) := 0, \quad H_q(x) := x \log_q(q - 1) - x \log_q(x) - (1 - x) \log_q(1 - x)$ für $0 < x \leq 1 - q^{-1}$.

3.48 Satz. *E gelten für* $0 \leq \delta \leq 1 - q^{-1}$*:*

1. **Plotkin Schranke** $\alpha_q(\delta) \leq 1 - \frac{q}{q-1}\delta$*;*

2. **Hamming Schranke** $\alpha_q(\delta) \leq 1 - H_q(\delta/2)$*;*

3. **Bassalygo-Elias Schranke** $\alpha_q(\delta) \leq 1 - H_q(\theta - \sqrt{\theta(\theta - \delta)})$ *mit* $\theta := 1 - q^{-1}$.

4. **Gilbert-Varshamov Schranke** $\alpha_q \geq 1 - H_q(\delta)$.

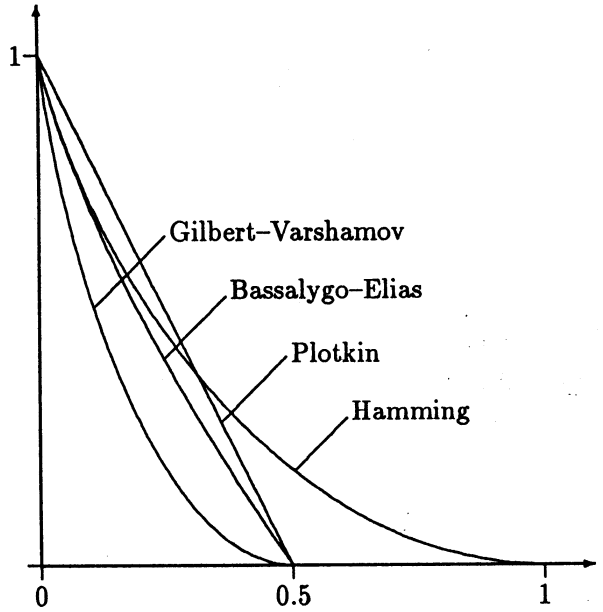


Fig. 1. Bounds for $q = 2$

Zeichnung aus Stichtenoth

Wir betrachten nun lange geometrische Goppa Codes. Dazu sei $F/\mathbb{F}_q$ ein algebraischer Funktionenkörper mit $N = N(F)$ Stellen vom Grad 1. Die Länge von $C_{\mathcal{L}}(D, G)$ ist offensichtlich durch N beschränkt.

3.49 Lemma. *Es seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ paarweise veschiedene Stellen vom Grad 1 in F. Dann existiert für jedes $r \geq 0$ ein Divisor G mit $\deg(G) = r$ und $\mathfrak{p}_i \notin \mathrm{supp}(G)$ für $1 \leq i \leq n$.*

Beweis. Falls eine weitere Stelle $\mathfrak{q}$ vom Grad 1 existiert, setzen wir $G = r\mathfrak{q}$. Ansonsten wählen wir einen Divisor $G \sim r\mathfrak{p}_1$ mit $v_{\mathfrak{p}_i}(G) = 0 \quad (1 \leq i \leq n)$, was nach dem Approximationssatz möglich ist. □

Es seien $N_q(g) := \max\{N(F) \mid F/\mathbb{F}_q \text{ Funktionenkörper vom Geschlecht } g\}$, $A(q) := \limsup_{g \longrightarrow \infty} N_q(g)/g$.
Es ist bekannt:
$A(q) \leq \lfloor 2q^{1/2} \rfloor$ (Serre-Schranke), abgeleitet aus $\mid N(F) - (q+1) \mid \leq g\lfloor 2q^{1/2} \rfloor$;
$A(q) \leq q^{1/2} - 1$ (Drinfeld-Vladut-Zink).

Bemerkung Ist q ein Quadrat, so gilt $A(q) = q^{1/2} - 1$. Stets gilt $A(q) > 0$.

3.50 Satz. *Für $A(q) > 1$ gilt $\alpha_q(\delta) \geq (1 - A(q)^{-1}) - \delta$ im Intervall $0 \leq \delta \leq 1 - A(q)^{-1}$.*

Beweis. Wir wählen eine Folge von Funktionenkörpern $F_i/\mathbb{F}_q$ mit Geschlecht g_i, so dass für $n_i := N(F_i)$ gilt: $g_i \longrightarrow \infty$, $n_i/g_i \longrightarrow A(q)$. Hierzu wählen wir eine Folge $r_i > 0$ mit $r_i/n_i \longrightarrow 1 - \delta$. Es sei D_i Summe aller Stellen vom Grad 1 in F_i, also gilt $\deg(D_i) = n_i$. Nach (3.49) existiert ein Divisor $G_i \in D_{F_i}$ mit $\deg(G_i) = r_i$ und $\mathrm{supp}(G_i) \cap \mathrm{supp}(D_i) = \emptyset$. Wir betrachten dazu den Code $C_i := C_{\mathcal{L}}(D_i, G_i)$. Dessen Parameter $[n_i, k_i, d_i]$ erfüllen dann die Abschätzungen: $n_i > k_i \geq$

$\deg(G_i) + 1 - g_i = r_i + 1 - g_i$ sowie $d_i \geq n_i - \deg(G_i) = n_i - r_i$. Wir erhalten $R_i := R(G_i) \geq \frac{r_i+1-g_i}{n_i}$, $\delta_i := \delta(C_i) \geq 1 - \frac{r_i}{n_i}$.
OBdA (sonst geeignete Auswahl von Teilfolgen) können wir annehmen, dass die Folgen (R_i) und (δ_i) konvergieren, etwa $R_i \longrightarrow R$, $\delta_i \longrightarrow \tilde{\delta}$. Zusammenfassend ergibt dies für i genügend groß $R \geq \frac{r_i}{n} + \frac{1}{n_i} - \frac{g_i}{n_i}$, also auch $R \geq 1 - \delta - A(q)^{-1}$ sowie $\tilde{\delta} \geq \delta$. Es folgt wegen $\alpha_q(\tilde{\delta}) \geq R$ und α_q monoton fallend $\alpha_q(\delta) \geq \alpha_q(\tilde{\delta}) \geq 1 - \delta - A(q)^{-1}$. □

Um 3.50 anwenden zu können, bedarf es unterer Schranken für $A(q)$. Tsfasman-Vladut-Zink bewiesen $A(q) = q^{1/2} - 1$, falls q eine Quadratzahl ist. In diesem Fall erhalten wir dann

$$\alpha_q(\delta) \geq (1 - (q^{1/2} - 1)^{-1}) - \delta \text{ für } 0 \leq \delta \leq 1 - (q^{1/2} - 1)^{-1}$$

(**Tsfasman-Vladut-Zink-Schranke**). Letztere ist für Quadratzahlen $q \geq 49$ in einem geeigneten Intervall größer als die Gilbert-Varshamov-Schranke.

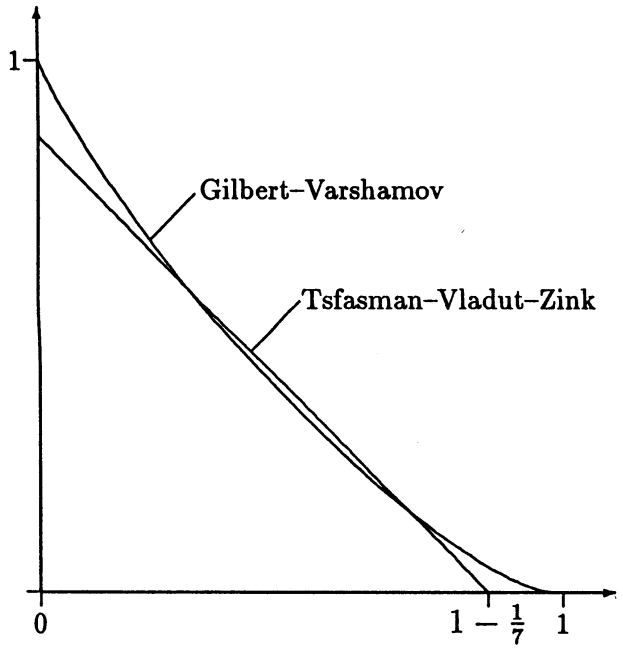


Fig. 2. Bounds for $q = 64$

Zeichnung aus Stichtenoth

Hermitesche Funktionenkörper und Codes

Es seien $K = \mathbb{F}_{q^2}$ und $K[u, v]$ der Polynomring in 2 Variablen. Dann wird durch die Gleichung $u^{q+1} + v^{q+1} + 1 = 0$ ein hermitescher Funktionenkörper $F = K(v)(u)$ definiert, der über dem rationalen Funktionenkörper $K(v)$ den Grad $q+1$ besitzt (Eisenstein-Kriterium). F ist ein **maximaler Funktionenkörper**, da - wie wir zeigen werden - in ihm die Serre Schranke $q^2+1+2gq$ für die Anzahl $N(F)$ der Stellen vom Grad 1 angenommen wird.

3.51 Hilfssatz. *Ist $E/\mathbb{F}_{q^2}$ ein maximaler Funktionenkörper, so gilt für sein Geschlecht g:*

$$g \leq q(q-1)/2.$$

Wir werden zeigen, dass das Geschlecht des hermiteschen Funktionenkörpers F gerade $q(q-1)/2$ ist.

Statt $u^{q+1}+v^{q+1}+1=0$ betrachten wir dazu $u^{q+1}=v^{q+1}-1$. Dies ist möglich, da $\mathbb{F}_{q^2}$ ein Element δ mit $\delta^{q+1}=-1$ enthält. In $\mathbb{F}_{q^2}(v)$ existieren q^2+1 Stellen vom Grad 1. Es sind dies $v-\alpha \quad (\alpha \in \mathbb{F}_{q^2})$ sowie $\frac{1}{v}$.
Wir untersuchen deren Fortsetzungen nach F mittels Kummers Satz aus der Zahlentheorie. Der besagt, dass unter bestimmten Voraussetzungen, die hier vorliegen, die Zerlegung der Stellen $v-\alpha$ aus der Faktorisierung von $u^{q+1}-(v^{q+1}-1) \mod (v-\alpha)$ abgelesen werden kann. (Die Grade der Stellen in F entsprechen dabei genau den Graden der Faktoren.)

1. Fall $\alpha \in K \wedge \alpha^{q+1}=1$.
Dann ist α einfache Nullstelle von $v^{q+1}-1 \in K[v]$, also ist $u^{q+1}-(v^{q+1}-1) \equiv u^{q+1} \mod (v-\alpha)$, $v-\alpha$ ist voll verzweigt in $F/K(v)$, und $v-\alpha$ hat eindeutige Fortsetzung $\mathfrak{P} \in \mathbb{P}_F$ vom Grad 1.

2. Fall $\alpha \in K \wedge \ \alpha^{q+1} \neq 1$.
Es gilt $\mathrm{ord}(\alpha^{q+1}) \mid (q-1)$, also ist α^{q+1} und damit $\alpha^{q+1}-1 \in \mathbb{F}_q$. Für $\mathbb{F}_{q^2}^{\times} =< \lambda >$ gilt $\mathrm{ord}(\lambda)=q^2-1$ nebst $\mathrm{ord}(\lambda^{q+1})=q-1$, folglich hat $y^{q+1}-(\alpha^{q+1}-1)$ in $\mathbb{F}_{q^2}$ eine und damit dann $q+1$ paarweise verschiedene Nullstellen. Die Stelle $v-\alpha$ besitzt also $q+1$ verschiedene Fortsetzungen vom Grad 1.

3. Fall $\frac{1}{v}$.
Hier ist Kummers Satz nicht direkt anwendbar, da $u^{q+1}-(v^{q+1}-1)$ nicht im zugehörigen Bewertungsring liegt. Wir substituieren $z=\frac{u}{v}$ und erhalten
$z^{q+1}=\frac{u^{q+1}}{v^{q+1}}=\frac{v^{q+1}-1}{v^{q+1}}=1-(v^{-1})^{q+1}$, also $z^{q+1}-1+(v-1)^{q+1} \equiv z^{q+1}-1 \mod v^{-1}$.
Nun hat $z^{q+1}-1$ genau $q+1$ Nullstellen in $\mathbb{F}_{q^2}$, also hat auch $\frac{1}{v}$ genau $q+1$ verschiedene Fortsetzungen $\mathfrak{P}_\infty \in \mathbb{P}_F$, die alle vom Grad 1 sind.

Insgesamt bekommen wir
$(q+1)$ Stellen vom Grad 1 im Fall 1,
$(q^2-(q+1))(q+1)$ Stellen vom Grad 1 im Fall 2,
$(q+1)$ Stellen vom Grad 1 im Fall 3,
was bedingt

$$\begin{aligned} N(F) &= (q+1)+(q+1)(q^2-q-1)+(q+1) \\ &= (q+1)(1+q^2-q-1+1) \\ &= q^3-q^2+q+q^2-q+1 \\ &= q^3+1. \end{aligned}$$

F ist also maximal.

Für das Geschlecht von F erhalten wir mit der Hurwitzschen Geschlechterformel: $g = 1+(q+1)(0-1) + \frac{1}{2}\sum_{\mathfrak{p}\in\mathbb{P}_F}(q+1-r_{\mathfrak{p}})\deg\mathfrak{p}$.

Dabei bezeichnet die Null das Geschlecht des rationalen Funktionenkörpers $K(v)$ sowie $r_{\mathfrak{p}} := \gcd(q+1, \nu_{\mathfrak{p}}(v^{q+1}-1)) \quad \forall\mathfrak{p}\in\mathbb{P}_F$. Es gilt

$$\nu_{\mathfrak{p}}(v^{q+1}-1) = \begin{cases} 0 \text{ für } \mathfrak{p} \text{ aus den Fällen } 2,3 \\ 1 \text{ für } \mathfrak{p} \text{ aus Fall } 1 \end{cases}.$$

Es folgt $g = 1-(q+1)+\frac{1}{2}\sum_{i=1}^{q+1} q = \frac{q(q+1)}{2} - q = \frac{q(q-1)}{2}$.

Hermitesche Funktionenkörper lassen sich in der folgenden Form: $y^q + y = x^{q+1}, F = K(x)(y)$ leichter behandeln. Wir zeigen zunächst, das beide Formen äquivalent sind.

Umrechnung verschiedener Darstellungen Hermitescher Funktionenkörper:

1. $u^{q+1} + v^{q+1} + 1 = 0$;

2. $y^q + y = x^{q+1}$.

(1) $\Longrightarrow$ (2) Wir wählen $\gamma, \delta \in \mathbb{F}_{q^2}$ mit $\gamma^q + \gamma = \delta^{q+1} = -1$. Setzen wir dann $x := \frac{\delta}{v-\delta u}, y := \frac{\delta(1+\gamma)u-\gamma v}{v-\delta u}$, so erhalten wir

$$\begin{aligned}
&(v-\delta u)^{q+1}(y^q + y - x^{q+1}) \\
&\quad = (v-\delta u)(\delta(1+\gamma)u-\gamma v)^q + (v-\delta u)^q(\delta(1+\gamma)u-\gamma v) - \delta^{q+1} \\
&\quad = (v-\delta u)(\tfrac{-1}{\delta}(1+(-1-\gamma))u^q - (-1-\gamma)v^q) + (v^q - \tfrac{-1}{\delta}u^q)(\delta(1+\gamma)u-\gamma v) + 1 \\
&\quad = \tfrac{\gamma}{\delta}(v-\delta u)u^q + (\gamma+1)(v-\delta u)v^q + v^q\delta(1+\gamma)u - v^{q+1}\gamma + u^{q+1}(1+\gamma) - \tfrac{\gamma}{\delta}vu^q + 1 \\
&\quad = -\gamma u^{q+1} + (\gamma+1)v^{q+1} - (\gamma+1)\delta uv^q + v^q u\delta(1+\gamma) - v^{q+1}\gamma + u^{q+1}(1+\gamma) - 1 \\
&\quad = v^{q+1} + u^{q+1} + 1 = 0,
\end{aligned}$$

also muss

$$y^q + y = x^{q+1}$$

gelten.

(2) $\Longrightarrow$ (1) Aus $y = \frac{\delta(1+\gamma)u-\gamma v}{v-\delta u} = ux - \gamma, x = \frac{\delta}{v-\delta u}$ folgen $u = \frac{y+\gamma}{x}$ und $v = \frac{\delta}{x} + \delta\frac{y+\gamma}{x} = \frac{\delta}{x}(y+(\gamma+1))$. Wir erhalten dann

$$
\begin{aligned}
u^{q+1} + v^{q+1} + 1 & \\
&= \tfrac{1}{x^{q+1}}((y^q+\gamma^q)(y+\gamma) + \delta^{q+1}(y^q+(\gamma+1)^q)(y+(\gamma+1)) + x^{q+1}) \\
&= \tfrac{1}{x^{q+1}}(y^{q+1} + \gamma^q y + \gamma y^q + \gamma^{q+1} - y^{q+1} - (\gamma+1)y^q - (\gamma^q+1)y \\
&\quad -(\gamma^q+1)(\gamma+1) + x^{q+1}) \\
&= \tfrac{1}{x^{q+1}}(-y^q - y - \gamma^q - \gamma - 1 + x^{q+1}) \\
&= \tfrac{-1}{x^{q+1}}(y^q + y - x^{q+1}),
\end{aligned}
$$

also notwendig $y^q + y = x^{q+1}$.

Zur Analysierung der neuen Darstellung von F benötigen wir einige Eigenschaften von $\mathbb{F}_{q2}$. $\mathbb{F}_{q^2}$ ist eine quadratische Erweiterung von $\mathbb{F}_q$ und somit galoissch (Algebra). Die Galoisgruppe ist zyklisch von der Ordnung 2. Sie wird erzeugt vom Frobenius Automorphismus

$$\pi : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_{q^2} : x \mapsto x^q.$$

Für $x \in \mathbb{F}_{q^2}$ ist dann $Tr(x) := Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x) = x + \pi(x) = x + x^q$. Es ist $Tr(x) \in \mathbb{F}_q$. Da Tr ein additiver Homomorphismus ist und $\mathbb{F}_{q^2}$ eine primitive (q^2-1) - te Einheitswurzel enthält, ist $\ker(Tr)$ eine additive Untergruppe von $\mathbb{F}_{q^2}$ der Ordnung q. Folglich ist Tr notwendig surjektiv.
Eine Gleichung $x^q + x = \mu \quad (\mu \in \mathbb{F}_{q^2})$ hat genau dann eine Lösung $x \in \mathbb{F}_{q^2}$, wenn $\mu \in \mathbb{F}_q$ ist. Wegen $(\mu^{q+1})^{q-1} = \mu^{q^2-1} = 1$ ist dies jedoch stets für $\mu = \alpha^{q+1}$ mit $\alpha \in \mathbb{F}_{q^2}$ erfüllt. Besitzt die Gleichung $x^q + x = \mu$ eine Lösung $\beta \in \mathbb{F}_{q^2}$, so hat sie bereits q paarweise verschiedene Lösungen. Denn $x + x^q = 0$ hat q paarweise verschiedene Lösungen $\beta_1, \ldots, \beta_q \in \mathbb{F}_{q^2}$, also sind $\beta + \beta_i \quad (1 \le i \le q)$ Lösungen von $x^q + x = \mu$.

In der Darstellung Hermitescher Funktionenkörper mittels $F = \mathbb{F}_{q^2}(y, x)$ mit $y^q + y = x^{q+1}$ gilt dann:

1. $F/\mathbb{F}_{q^2}(x)$ ist zyklisch vom Grad q. Die Automorphismen werden gegeben durch $\sigma(y) = y + \beta_\nu$ mit $\beta_\nu \in \ker \pi$. $\mathbb{F}_{q^2}$ ist der volle Konstantenkörper zu F.

2. F hat $q^3 + 1$ Stellen vom Grad 1, nämlich je q, die zu $x - \alpha \quad (\alpha \in \mathbb{F}_{q^2})$ korrespondieren sowie den gemeinsamen Pol $\mathfrak{q}_\infty$ von y und x. ($\mathfrak{p}_\infty$ ist hier total verzweigt. Dies wird allerdings nicht explizit gezeigt.)

   (Nach Kummer spaltet jede Stelle $\mathfrak{p}_\alpha \stackrel{\triangle}{=} x - \alpha \quad (\alpha \in \mathbb{F}_{q^2})$ in $F = \mathbb{F}_{q^2}(x)(y)$ mit $y^q + y = x^{q+1}$ in q paarweise verschiedene Stellen $\mathfrak{p}_{\alpha,\beta} \supseteq \mathfrak{p}_\alpha$ auf. Diese sind notwendig vom Grad 1. Es gilt $x + \mathfrak{p}_{\alpha,\beta} = \alpha, y + \mathfrak{p}_{\alpha,\beta} = \beta$.)

3. Das Geschlecht von $F/\mathbb{F}_{q^2}(x)$ ist $q(q-1)/2$. Damit ist $F/\mathbb{F}_{q^2}(x)$ ein maximaler Funktionenkörper.

4. Für $r \ge 0$ bilden die Elemente $x^i y^j$ mit $0 \le i, \quad 0 \le j \le q-1$ und $iq + j(q+1) \le r$ eine Basis von $\mathcal{L}(r\mathfrak{q}_\infty)$.

Begründung: $1, y, \ldots, y^{q-1}$ bilden eine Ganzheitsbasis von $F/K(x)$, da das Minimalpolynom $y^q + y - x^{q+1} \in K[x][y]$ ist, dessen Ableitung an allen endlichen Stellen $\mathfrak{p}$ den $\nu_\mathfrak{p}$ - Wert 0 hat.

Ist nun $z \in \mathcal{L}(r\mathfrak{q}_\infty)$, so ist $\nu_\mathfrak{p}(z) \geq 0 \quad \forall \mathfrak{p} \in \mathbb{P}_{K(x)} \setminus \{\mathfrak{p}_\infty\}$. Also gilt $z = \sum_{j=0}^{q-1} z_j y^j$ mit $z_j \in K[x]$, d.h. $z = \sum_{j=0}^{q-1} \left(\sum_{i \geq 0} a_{ij} x^i \right) y^j \quad (a_{ij} \in K)$.
Die Elemente $x^i y^j$ mit $0 \leq j \leq q-1$ haben paarweise verschiedene Polordnungen wegen $\nu_{\mathfrak{q}_\infty}(x) = -q, \nu_{\mathfrak{q}_\infty}(y) = -q+1$ und
$iq + j(q+1) = \mu q + \nu(q+1)$
$\Longrightarrow (i-\mu)q = (\nu - j)(q+1)$
$\Longrightarrow q \mid (\nu - j)$, aber $\mid \nu - j \mid < q$
$\Longrightarrow \nu = j$ und damit auch $i = \mu$.
Es folgt $\nu_{\mathfrak{q}_\infty}(z) = \min\{-iq - j(q+1) \mid a_{ij} \neq 0\}$.

Hermitesche Codes: $\mathbf{y^q + y = x^{q+1}}$

Für $r \in \mathbb{Z}$ setzen wir $C_r := C_\mathcal{L}(D, r\mathfrak{q}_\infty)$, wobei $D := \sum_{\beta^q + \beta = \alpha^{q+1}} \mathfrak{p}_{\alpha,\beta}$ der Divisor ist, der Summe aller endlichen Stellen vom Grad 1 des Funktionenkörpers ist. Die Länge von C_r ist $n = q^3$, C_r ist Code über $\mathbb{F}_{q^2}$.
Für $r \leq s$ ist offenbar C_r ein Unterraum von C_s. Im Fall $r < 0$ ist $\mathcal{L}(r\mathfrak{q}_\infty) = 0$, also $C_r = \mathbf{0}$.
Für $r > q^3 + q^2 - q - 2 = q^3 + (2g-2)$ gilt wie früher

$$\begin{aligned} \dim C_r &= \dim(r\mathfrak{q}_\infty) - \dim(r\mathfrak{q}_\infty - D) \\ &= (r + 1 - g) - (r - q^3 + 1 - g) \\ &= q^3 = n. \end{aligned}$$

3.52 Proposition. (ohne Beweis) *Setzen wir $I = \{n \in \mathbb{Z}^{\geq 0} \mid \exists z \in F : (z)_\infty = n\mathfrak{q}_\infty\}$, sowie für $s \in \mathbb{Z}^{\geq 0} : I(s) = \{n \in I \mid n \leq s\}$, dann gilt für $0 \leq r \leq q^3 + q^2 - q - 2$:*

1. *Die Dimension von C_r ist*
$$\dim C_r = \begin{cases} \sharp I(r) \text{ für } 0 \leq r < q^3 \\ q^3 - \sharp I(s) \text{ für } q^3 \leq r \text{ und } s := q^3 + q^2 - q - 2 - r. \end{cases}$$

2. *Der Minimalabstand d von C_r genügt $d \geq q^3 - r$. Für $0 \leq r < q^3$ und $r, q^3 - r \in I$ ist $d = q^3 - r$. Speziell ist letzteres stets für $q^2 - q \leq r \leq q^3 - q^2 + q$ erfüllt.*

Unter einem Funktionenkörperturm über $\mathbb{F}_q$ verstehen wir eine Folge von Funktionenkörpern $\mathcal{F} = (F_i)_{i \in \mathbb{N}}$ mit:

1. $F_1 \subseteq F_2 \subseteq F_3 \subseteq \ldots$,

2. $\forall n \in \mathbb{N}$ ist F_{n+1}/F_n separabel mit $[F_{n+1} : F_n] > 1$,

3. das Geschlecht $g(F_j)$ ist größer als Eins für ein $j \in \mathbb{Z}^{\geq 1}$,

4. $\mathbb{F}_q$ ist der volle Konstantenkörper für alle F_i.

Bemerkung Die Hurwitzsche Geschlechterformel liefert $g(F_i) \longrightarrow \infty$ für $i \longrightarrow \infty$.

Es sei $\lambda(\mathcal{F}) := \lim\limits_{i \longrightarrow \infty} N(F_i)/g(F_i)$.

Ein Turm heißt **asymptotisch gut** im Fall $\lambda(\mathcal{F}) > 0$, er heißt **optimal** für $A(q) = \lambda(\mathcal{F})$.

Ein Funktionenkörperturm wird durch ein Polynom $f(x, y) \in \mathbb{F}_q(x, y)$ definiert, falls $F_1 = \mathbb{F}_q(x)$ ist und für $n > 1$ stets $F_n = \mathbb{F}_q(x_1, \ldots, x_n)$ mit $f(x_i, x_{i+1}) = 0 \quad (1 \leq i < n)$ gilt.

3.53 Satz. (Li, Maheraj, Stichtenoth, Elkies) *Jedes der folgenden Polynome definiert einen optimalen Turm:*

1. $2xy^2 + (x^2 + x + 1)y + x^2 + x + 2$ *über* $\mathbb{F}_9$,

2. $(4x + 1)y^2 + (x^2 + x + 2)y + x + 3$ *über* $\mathbb{F}_{25}$,

3. $(x^2 + 6)y^2 + xy + +x^2 + 4$ *über* $\mathbb{F}_{49}$,

4. $x^2y^3 + (x^3 + x^2 + x)y^2 + (x + 1)y + x^3 + x$ *über* $\mathbb{F}_4$.

3.54 Satz. (Bezerra, Garcia) *Es seien* $F_1 = K(x_1)$ *mit* $K = \mathbb{F}_{q^2}$ *sowie* $F_{n+1} = F_n(x_{n+1})$ *mit* $\frac{x_{n+1}-1}{x_{n+1}^q} = \frac{x_n^q-1}{x_n}$. *Dann gilt* $\lambda(\mathcal{F}) = q - 1 \quad (= A(q))$.

Bemerkung Im letzten Körperturm treten Erweiterungen auf, die nicht galoissch sind.

Anhang: Beispiel aus Lütgebohmert

Reed-Solomon-Codes haben hohe (optimale) Informationsrate bei gegebenen relativen Abstand. Die Komplexität nimmt zu, wenn man die Blocklänge vergrößert, weil der zugrunde liegende Körper größer gewählt werden muss.

Wir wollen den RS-Code $[16, 8, 9]$ vergleichen mit einem geometrischen Code über $\mathbb{F}_{16}$. Der RS-Code wird gegeben durch das Erzeugerpolynom

$$g(z) := \prod_{i=0}^{z}(z - \alpha^i) \in \mathbb{F}_{16}[z]$$

wobei $\alpha \in \mathbb{F}_{16}$ primitive 15 - te Einheitswurzel ist. Man kann diesen Code auch als geometrischen Code über die Auswertungsabbildung

$$ev : L(7) := \{f \in F_q[z] \mid \deg f \leq 7\} \longrightarrow \mathbb{F}_{16}^{15} : f \mapsto (f(\alpha^{15}), \ldots, f(\alpha^1))$$

finden.

Andererseits betrachten wir den geometrischen Code zur Hermite-Kurve

$$X := V(T_0^5 + T_1^5 + T_2^5) \subseteq \mathbb{P}^2_{\mathbb{F}_{16}}$$

über $\mathbb{F}_{16}(q = 4)$. Sie hat card $(X(\mathbb{F}_{16})) = 65$ rationale Punkte und Geschlecht $g(X) = 6$.
Zum rationalen Punkt $x_0 := (0, 1, 1) \in x(\mathbb{F}_{16})$ betrachten wir den $\mathbb{F}_{16}$ - Vektorraum $\mathcal{L}(37 \cdot x_0)$ der rationalen Funktionen auf X, die höchstens in x_0 einen Pol bis zur Ordnung 37 haben $r = 37$. Dann gilt $\dim(\mathcal{L}(37 \cdot x_0)) = 37 - 6 + 1 = 32$. Setzt man $D := x_1 + \ldots + x_{64}$, so hat der $\mathbb{F}_{16}$ - Code $C_{\mathcal{L}}(D, 37 \cdot x_0)$ die Länge $n = 64$, Dimension 32 und Minimalabstand $d \geq 64 - 37 = 27$. Eine Basis von $\mathcal{L}(37 \cdot \cdot x_0)$ wird durch

$$f_{i,j} := \frac{T_0^i \cdot T_1^i}{(T_1 + T_2)^{1+j}} \quad (0 \leq i \leq 4, \quad 0 \leq j \quad 5 \cdot (i + j) - i \leq 37)$$

gegeben.

Man beachte, dass auf X die Relation

$$(T_1^4 + T_1^3 T_2 + T_1^2 T_3^2 + T_1 T_2^3 + T_2^4)^{i+j} \cdot (T_1 + T_2)^{i+i} = T_0^{5(i+i)}$$

gilt.

Daher hat $f_{i,j}$ in x_0 einen Pol der Ordnung $4i + 5_j$. Auswertung dieser Funktion an den rationalen Stellen $x_1, \ldots, x_{34}$ liefert eine konkrete Darstellung dieses Codes mit den Parametern $[64, 32, 27]$.

Vergleich der Codes:

	$[16, 8, 9]$ - RS-Code	$[64, 32, 27]$ AG-Code
Informationsrate:	$0,5$	$0,5$
relativer Abstand	$0,5625$	$0,4219$
Fehlerwahrscheinlichkeit im Kanal mit:		
$p = 0,04$	$\sim 3 \cdot 10^{-4}$	$\sim 2 \cdot 10^{-7}$
$p = 0,02$	$\sim 1 \cdot 10^{-5}$	$\sim 3 \cdot 10^{-11}$