

Geometrische Goppa-Codes und verallgemeinerte Produktcodes

Diplomarbeit

von

Joe-Kai Tsay

November 2001

Universität Essen

Vorab möchte ich mich bei einigen Personen bedanken, die am Zustandekommen dieser Arbeit beteiligt waren.

Zunächst bedanke ich mich aufrichtig bei Prof. Dr. Henning Stichtenoth, der mich als Dozent von Anfang an durch mein Studium begleitet und mich nicht nur während dieser Arbeit hervorragend betreut hat. Er gab mir unverzichtbare Tips und Anregungen für diese Arbeit und unterstützte mich stets mit viel Geduld.

Danke auch an Dennis Kreuzer, Sonja Schnitzler und Ali Majidi, die sich für mich auf Fehlersuche begaben.

Und nicht zuletzt möchte ich mich bei meinen Eltern bedanken, die mir mein Studium und damit diese Arbeit ermöglichten.

Hiermit versichere ich, daß ich diese Arbeit selbständig und nur unter Zuhilfenahme der
aufgeführten Quellen angefertigt habe.
Essen, im Juli 2001

Joe-Kai Tsay

Inhaltsverzeichnis

Vorwort	7
I Grundlagen der Codierungstheorie und der Theorie algebraischer Funktionenkörper	9
I.1 Codes	9
I.2 Grundbegriffe der Theorie algebraischer Funktionenkörper	11
I.3 Geometrische Goppa Codes	15
II Eine Konstruktion von Niederreiter und Xing für lineare Codes	17
II.1 Darstellung linearer Codes als algebraisch-geometrische Codes	17
II.2 Eine Konstruktion von Niederreiter und Xing	19
III Bemerkungen zu der NX-Konstruktion von Özbudak und Stichtenoth	25
III.1 Eine Konstruktion von Özbudak und Stichtenoth	25
III.2 Die NX-Konstruktion als Spezialfall der Konstruktion von Özbudak und Stichtenoth	31
III.3 Numerische Resultate	35
A Anhang	37
A.1 Beispiel eines Funktionenkörpers F_n/\mathbb{F}_q mit beliebig vielen rationalen Stellen	37
A.2 Das Geschlecht von F_n/\mathbb{F}_q	41
B Anhang. Das Hutproblem und Hamming-Codes	45
B.1 Für drei Spieler	45
B.2 Für $n = 2^r - 1$ Spieler	45
Literaturverzeichnis	49

Vorwort

Die vorliegende Diplomarbeit beschäftigt sich mit einer Konstruktion von H. Niederreiter und C. Xing für lineare Codes ([4]) und der Verallgemeinerung und Vereinfachung dieser Konstruktion durch F. Özbudak und H. Stichtenoth ([10]).

Wendet man die Konstruktion von Niederreiter und Xing auf einen gegebenen linearen Code an, so erhält man einen neuen längeren Code größerer Dimension. Dabei sind drei Parameter frei wählbar (bzw. ein Parameter im binären Fall), so daß man eine ganze Familie von Codes bekommt. Bei ihrer Konstruktion benutzen Niederreiter und Xing (verallgemeinerte) geometrische Goppa Codes. Diese große Klasse von Codes wird mit Hilfe algebraischer Funktionenkörper über endlichen Körpern konstruiert und enthält Codes, die lang sind und für die man eine gute untere Abschätzung des Minimalabstandes angeben kann. Insbesondere letzteres ist bisher nur für sehr wenige Klassen von Codes möglich (BCH Codes, klassische Goppa Codes und quadratische Reste Codes; siehe [1], [3]).

Auch Niederreiter und Xing geben für ihren Code eine untere Schranke des Minimalabstandes an, welche eine gute Abschätzung liefert, wie man z.B. in Abschnitt III.3 Beispiel 2 sehen kann. Ferner zeigen Niederreiter und Xing, daß man mit ihrer Methode viele optimale Codes konstruieren kann.

Eine einfache Weise, aus gegebenen linearen Codes einen längeren Code größerer Dimension zu konstruieren, ist das direkte Produkt zweier Codes (siehe [1, chapter 18]). Tatsächlich zeigen Özbudak und Stichtenoth in [10], daß die Konstruktion von Niederreiter und Xing ein Spezialfall einer Konstruktion ist, die man als (verallgemeinerten) Produktcode auffassen kann. Sie kommen dabei mit sehr viel einfacheren Hilfsmitteln aus als Niederreiter und Xing. Insbesondere werden in [10] keine algebraischen Funktionenkörper benötigt, sondern lediglich Kenntnisse der linearen Algebra. Ferner existieren bei der Methode von Özbudak und Stichtenoth noch mehr Möglichkeiten bei der Auswahl der drei bei Niederreiter und Xing frei wählbaren Parameter, so daß sich deutlich mehr (optimale) Codes konstruieren lassen.

Die Arbeit ist wie folgt aufgebaut:

Im ersten Kapitel klären wir die in dieser Arbeit verwendeten Begriffe und Definitionen aus der Codierungstheorie und der Theorie algebraischer Funktionenkörper und zeigen am Beispiel der geometrischen Goppa-Codes einen Zusammenhang zwischen Codes und algebraischen Funktionenkörpern auf.

Im zweiten Kapitel betrachten wir die Konstruktion von Niederreiter und Xing. Diese stellen einen linearen $[n, k, d]$ -Code C als verallgemeinerten geometrischen Goppa-Code über einem Funktionenkörper F/\mathbb{F}_q mit mindestens n rationalen Stellen dar. Zu $h, r, s \in \mathbb{Z}$ mit $2 \leq h \leq q$, $1 \leq r < h$, $0 \leq s \leq r$ betrachten sie dann eine algebraische Erweiterung E von F und konstruieren mit Hilfe der Fortsetzungen von den n rationalen Stellen in E einen $[hn, k(s+1) + r - s]$ -Code mit Minimalabstand $\geq \min\{(h-s)d, (h-r)n\}$.

Im dritten Kapitel stellen wir zuerst die Konstruktion von Özbudak und Stichtenoth vor. Diese gehen von einem linearen $[m, k, d]$ -Code C , welcher Untercode $C_1 \subseteq C_2 \subseteq \dots \subseteq C_k = C$ enthält, und von k linearen Codes W_1, \dots, W_k der Länge n aus. Sie betrachten dann $n \times k$ Matrizen, deren j -te Spalte ($1 \leq j \leq k$) ein Element aus W_j ist, und multiplizieren diese Matrizen mit einer gewissen Erzeugermatrix von C . Die Menge der resultierenden Matrizen bilden einen $[mn, \sum_{j=1}^k \dim(W_j)]$ -Code mit Minimalabstand $\geq \min\{d(W_j) \cdot d(C_j) \mid 1 \leq j \leq k\}$. Im dritten Kapitel zeigen wir anschließend, daß die Konstruktion von Niederreiter und Xing wirklich ein Spezialfall dieser Methode ist, und belegen durch Beispiele, daß man mit der Methode von Özbudak und Stichtenoth (bzw. von Niederreiter und Xing) optimale Codes konstruieren kann.

Im Anhang A werden wir zu vorgegebenem q die Existenz eines Funktionenkörpers F/\mathbb{F}_q mit beliebiger Anzahl rationaler Stellen zeigen, welcher für die Konstruktion des verallgemeinerten algebraisch-geometrischen Codes benötigt wird. Niederreiter und Xing verweisen dafür auf die *asymptotic theory* rationaler Stellen eines Funktionenkörpers F/\mathbb{F}_q ([2, V.3]). Diese setzt allerdings großes Wissen über algebraische Funktionenkörper voraus. Wir geben ein Beispiel eines Funktionenkörpers mit beliebig vielen rationalen Stellen an und prüfen seine Eigenschaften mit weitaus einfacheren Mitteln. Anschließend bestimmen wir das Geschlecht des Funktionenkörpers.

Anhang B hat keinen direkten Bezug zu den vorangegangenen Kapitel. Es wird hier aber ein nettes Beispiel für die Verwendung der Codierungstheorie vorgestellt. Es geht dabei um ein Spiel, bei dem n Spieler jeweils entweder einen roten oder einen blauen Hut - die Verteilung ist dabei gleich - auf dem Kopf tragen und versuchen müssen, die Farbe ihres eigenen Hutes richtig zu tippen. Das Spiel ist gewonnen, wenn mindestens einer richtig tippt, und kein Spieler falsch tippt. Benutzen die Spieler Hamming-Codes, so haben sie für den Fall $n = 2^k - 1$ eine Gewinnwahrscheinlichkeit von $\frac{n}{n+1}$.

Kapitel I

Grundlagen der Codierungstheorie und der Theorie algebraischer Funktionenkörper

Dieses Kapitel dient in erster Linie dem Verständnis der nachfolgenden Inhalte. Es wird zuerst eine Einführung in die Codierungstheorie und ihre Begriffe gegeben. Danach werden wir kurz die grundlegenden Definitionen der Theorie algebraischer Funktionenkörper klären, die wir für diese Arbeit benötigen. Wir werden in diesem Kapitel auf Beweise der Ergebnisse weitgehend verzichten, um dieses Kapitel nicht zu umfangreich werden zu lassen. Beweise und genauere Ausführungen zu beiden Themen findet man in [1], [3] bzw. [2].

I.1 Codes

Wir bezeichnen mit \mathbb{F}_q den endlichen Körper mit q Elementen, und mit \mathbb{F}_q^n den n -dimensionalen Vektorraum, dessen Elemente n -Tupel $a = (a_1, \dots, a_n)$ sind.

Definition I.1.1 Eine Teilmenge $\emptyset \neq C \subseteq \mathbb{F}_q^n$ heißt *Code der Länge n (über \mathbb{F}_q)*. Die Elemente $c \in C$ heißen *Codewörter*. Falls $C \leq \mathbb{F}_q^n$ ein Untervektorraum ist, heißt C *linearer Code* der Länge n . Ist $k := \dim_{\mathbb{F}_q}(C)$, so wird C auch als *$[n, k]$ -Code über \mathbb{F}_q* bezeichnet. Wir werden uns im Folgenden ausschließlich mit linearen Codes beschäftigen, die wegen ihrer Struktur große Vorteile gegenüber nichtlinearen Codes besitzen, und deshalb in der Praxis auch die am häufigsten verwendeten sind. Es hat sich gezeigt, daß man ebenso gute lineare wie nichtlineare Codes konstruieren kann.

Definition I.1.2 Für $a, b \in \mathbb{F}_q^n$, etwa $a = (a_1, \dots, a_n)$ und $b = (b_1, \dots, b_n)$, heißt

$$d(a, b) := \#\{i \mid a_i \neq b_i\}$$

der *Abstand* (oder *Hamming-Distanz*) von a und b . Das *Gewicht* von einem Element $a \in \mathbb{F}_q^n$ wird durch

$$wt(a) := d(a, 0) = \#\{i \mid a_i \neq 0\}$$

definiert. Man kann leicht sehen, daß die Hamming-Distanz d eine Metrik auf \mathbb{F}_q^n ist. Insbesondere gilt die Dreiecksungleichung $d(a, c) \leq d(a, b) + d(b, c)$ für alle $a, b, c \in \mathbb{F}_q^n$. Sei $C \subseteq \mathbb{F}_q^n$ ein Code mit $\dim(C) \geq 1$. Dann heißt

$$d(C) := \min\{d(c, c') \mid c, c' \in C, c \neq c'\}$$

der *Minimalabstand* von C . Für $C = \{0\}$ (d.h. $\dim(C) = 0$) setzt man $d(C) := 0$. Wegen $d(a, b) = wt(a - b)$ gilt

$$d(C) = \min\{wt(c) \mid 0 \neq c \in C\}.$$

Ist C ein $[n, k]$ -Code und $d = d(C)$ der Minimalabstand von C , so bezeichnet man C als $[n, k, d]$ -Code. Dabei heißen n, k, d die *Parameter* von C .

Definition I.1.3 Für $q \geq 2$, $r \geq 0$ und $z \in \mathbb{F}_q^n$ sei $B_r(z) \subset \mathbb{F}_q^n$ die Kugel vom Radius r mit Mittelpunkt z (bzgl. der Metrik d). Ein Code C heißt *e-fehlerkorrigierend*, wenn gilt: Sind $c, c' \in C$ und $c \neq c'$, so folgt $B_e(c) \cap B_e(c') = \emptyset$.
Ist C ein $[n, k, d]$ -Code, so kann C bis zu $\lfloor \frac{d-1}{2} \rfloor$ Fehler korrigieren.

Man kann einen linearen Code C auf einfache Weise beschreiben, indem man eine Basis von C (als Vektorraum über \mathbb{F}_q) angibt.

Definition I.1.4 Sei C ein $[n, k, d]$ -Code über \mathbb{F}_q , wobei $k \geq 1$. Eine $k \times n$ -Matrix über \mathbb{F}_q heißt eine *Erzeugermatrix* von C , wenn die Zeilen von G eine Basis von C bilden. Ist G eine Erzeugermatrix von C , dann gilt

$$C = \{(u_1, \dots, u_k) \cdot G \mid u_i \in \mathbb{F}_q\}.$$

Da die Zeilen von G als Basis von C linear unabhängig sind, gilt $\text{rg}(G) = k$.

Eine weitere einfache Beschreibung eines linearen Code C liefert

Definition I.1.5 Ist $k < n$, so heißt eine Matrix $H \in \text{Mat}(n-k, n; \mathbb{F}_q)$ eine *Kontrollmatrix* für C , falls

$$C = \{u \mid u \in \mathbb{F}_q^n, H \cdot u^t = 0\}$$

ist. Dabei gilt stets $\text{rg}(H) = n - \dim(\ker H) = n - \dim(C) = n - k$. Somit sind die Zeilen von H ebenfalls linear unabhängig und H stellt eine Erzeugermatrix eines Codes (i.a. $\neq C$) dar. Dies liefert die folgende

Definition I.1.6 Sei C ein $[n, k]$ -Code über \mathbb{F}_q . Dann heißt

$$C^\perp := \{u \in \mathbb{F}_q^n \mid \langle u, c \rangle = 0\}$$

der *duale Code* zu C (dabei ist $\langle x, y \rangle := \sum_{i=1}^n x_i y_i$ das kanonische Skalarprodukt auf \mathbb{F}_q^n für $x = (x_1, \dots, x_n)$ und $y = (y_1, \dots, y_n)$). Aus der Definition sehen wir, daß $\text{Länge}(C^\perp) = n$ gilt. C heißt *selbstdual*, wenn $C = C^\perp$ ist.

Satz I.1.7 Die Voraussetzungen und Bezeichnungen seien die gleichen wie oben. Dann gilt

- i) $\dim(C^\perp) = n - k$
- ii) $(C^\perp)^\perp = C$
- iii) Eine Matrix $G \in \text{Mat}(k \times n)$ ist genau dann eine Erzeugermatrix von C , wenn G Kontrollmatrix von C^\perp ist.
- iv) Eine Matrix $H \in \text{Mat}(n-k \times n)$ ist genau dann eine Kontrollmatrix von C , wenn H eine Erzeugermatrix von C^\perp ist.

Definition I.1.8 Sei $C \leq \mathbb{F}_q^n$ ein $[n, k, d]$ -Code.

1. Dann nennt man

$$\hat{C} := \{(c_1, \dots, c_n, c_{n+1}) \in \mathbb{F}_q^{n+1} \mid (c_1, \dots, c_n) \in C, \sum_{i=1}^{n+1} c_i = 0\}$$

Erweiterung von C . \hat{C} ist ein linearer Code mit den Parametern $[n+1, k, \delta]$, wobei $d \leq \delta \leq d+1$. Ist $q=2$ und d ungerade, so ist \hat{C} ein $[n+1, k, d+1]$ -Code.

2. Sei $n \geq 2$. Dann heißt

$$\check{C}_i := \{(c_1, \dots, c_{i-1}, c_{i+1}, \dots, c_n) \in \mathbb{F}_q^{n-1} \mid (c_1, \dots, c_{i-1}, 0, c_{i+1}, \dots, c_n) \in C\}$$

Verkürzung von C (an der Stelle i) und ist ein $[n-1, k-1, d']$ -Code mit $d' \geq d$. Verkürzt man den Code C an einer Stelle, an der ein minimalgewichtiges Codewort von C einen Eintrag Null besitzt, dann gilt $d' = d$.

Ziel in der Codierungstheorie ist es, gute Codes C zu finden. C soll viele Fehler korrigieren können (d.h. $d(C)$ soll groß sein). Zudem sollen viele Informationen versendet werden, wobei man gleichzeitig den Aufwand des Codierens klein halten will (d.h. die *Informationsrate* $\frac{k}{n}$ soll groß sein). Diese Aussagen stehen jedoch im Widerspruch zueinander (denn je größer $k = \dim(C)$ ist, desto mehr Elemente enthält C ; dadurch wird aber der Minimalabstand $d(c)$ zwischen diesen Elementen kleiner). Es gilt z.B.

Satz I.1.9 (Singleton-Schranke). Für einen $[n, k, d]$ -Code ist

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

Und es gibt noch viele weitere Schranken, die auch von q abhängen, u.a.

Satz I.1.10 (Griesmer-Schranke). Für einen $[n, k, d]$ -Code über \mathbb{F}_q gilt

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil.$$

I.2 Grundbegriffe der Theorie algebraischer Funktionenkörper

Definition I.2.1 Sei K ein Körper. Ein *algebraischer Funktionenkörper* F/K (einer Variablen) über K ist eine Körpererweiterung $F \supseteq K$ derart, daß F eine endliche algebraische Erweiterung von $K(x)$ für ein transzendentes Element $x \in F$ ist.

Im weiteren meinen wir mit F/K stets einen algebraischen Funktionenkörper.

Definition I.2.2

$$\tilde{K} := \{z \in F \mid z \text{ algebraisch über } K\}$$

heißt der *volle Konstantenkörper* von F/K . Da Summe, Produkt und Inverse algebraischer Elemente wieder algebraisch sind, bildet \tilde{K} wirklich einen Körper. Es gilt $K \subseteq \tilde{K} \subset F$.

Definition I.2.3 Ein *Bewertungsring* von F/K ist ein Teilring $O \subseteq F$ mit:

- i) $K \subset O \subset F$
- ii) $z \in F \wedge z \notin O \Rightarrow z \in O^{-1}$.

Proposition I.2.4 Sei O ein Bewertungsring von F/K . Dann gilt:

- i) O ist ein lokaler Ring, d.h. $P := O \setminus O^*$ ist das einzige maximale Ideal von O .
- ii) Für $0 \neq x \in F$ gilt: $x \in P \Leftrightarrow x^{-1} \notin O$.
- iii) Ist \tilde{K} der Konstantenkörper, dann gilt $\tilde{K} \subseteq O$ und $\tilde{K} \cap P = \{0\}$.

Definition I.2.5 Eine *diskrete Bewertung* von F/K ist eine Abbildung $v : F \rightarrow \mathbb{Z} \cup \{\infty\}$ mit folgenden Eigenschaften:

- i) $v(x) = \infty \Leftrightarrow x = 0$
- ii) $v(x \cdot y) = v(x) + v(y)$
- iii) $v(x + y) \geq \min\{v(x), v(y)\}$ (Dreiecksungleichung)
- iv) $v(a) = 0$ für alle $0 \neq a \in K$
- v) es existiert ein $x \in F$ derart, daß $v(x) = 1$

Bemerkung. Sind $x, y \in F$ mit $v(x) \neq v(y)$, dann gilt die *scharfe Dreiecksungleichung*:

$$v(x + y) = \min\{v(x), v(y)\}.$$

Definition I.2.6 Das maximale Ideal P eines Bewertungsringes O heißt eine *Stelle* von F/K . Eine Stelle bestimmt den zugehörigen Bewertungsring eindeutig (denn $z \notin O \Leftrightarrow z^{-1} \in P$). Daher setzen wir $O =: O_P$. Ferner ist P ein Hauptideal. Falls $P = t \cdot O_P$ ($t \in O_P$), heißt t *Primelement* für P , und jedes Element $0 \neq z \in F$ besitzt eine eindeutig bestimmte Darstellung $z = t^n \cdot u$, wobei $n \in \mathbb{Z}$ und $u \in O_P^*$. Die Menge aller Stellen von F/K bezeichnen wir mit \mathbb{P}_F .

Für $F \setminus \{0\} \ni z = t^m \cdot u$ ($m \in \mathbb{Z}$, $u \in O_P^*$) setzen wir $v_P(z) := m$ und $v_P(0) := \infty$. Man nennt v_P die *zu P gehörige (diskrete) Bewertung von F/K* .

Satz I.2.7 Für jedes $P \in \mathbb{P}_F$ ist v_P eine diskrete Bewertung von F/K . Dabei gilt:

$$O_P = \{z \in F \mid v_P(z) \geq 0\}$$

$$P = \{z \in F \mid v_P(z) > 0\}.$$

Definition I.2.8 Sei $P \in \mathbb{P}_F$ und O_P der zugehörige Bewertungsring. Dann heißt $F_P := O_P/P$ *Restklassenkörper* von P . Für $x \in O_P$ setzen wir $x(P) := x + P \in F_P$. Für $x \in F \setminus O_P$ setzen wir $x(P) := \infty$. Der *Grad von P* ist definiert durch

$$\deg P := [F_P : K].$$

Von jetzt ab sei K algebraisch abgeschlossen in F .

Definition I.2.9

- (a) Ein *Divisor* von F/K ist eine (endliche) formale Summe

$$D = \sum_{P \in \mathbb{P}_F} n_P \cdot P, \quad \text{mit } n_P \in \mathbb{Z}, \text{ fast alle } n_P = 0.$$

- (b) Der *Träger* von D ist $\text{supp}(D) := \{P \mid n_P \neq 0\}$.
- (c) Die abelsche Gruppe $\mathcal{D}_F := \{D \mid D \text{ Divisor von } F/K\}$ heißt *Divisorengruppe* von F/K .
- (d) Für $Q \in \mathbb{P}_F$ und $D = \sum n_P \cdot P$ setzen wir $v_Q(D) := n_Q$. Damit folgt

$$D = \sum_{P \in \mathbb{P}_F} v_P(D) \cdot P.$$

- (e) Der *Grad* eines Divisors $D = \sum n_P \cdot P$ ist definiert durch $\deg(D) := \sum n_P \cdot \deg(P)$.
- (f) Sei $0 \neq x \in F$. Dann heißt $(x) := \sum_{P \in \mathbb{P}_F} v_P(x) \cdot P$ *Hauptdivisor* von x .
- (g) Sei $A \in \mathcal{D}_F$. Wir bezeichnen den K -Vektorraum $\mathcal{L}(A) := \{x \in F \mid (x) \geq -A\} \cup \{0\}$ als *Vielfachenmodul* von A , wobei $(x) \geq -A \Leftrightarrow v_P(x) \geq -v_P(A)$ für alle $P \in \mathbb{P}_F$.
- (h) Die ganze Zahl

$$g := \max_{A \in \mathcal{D}_F} \{\deg(A) - \dim(\mathcal{L}(A)) + 1\}$$

heißt das *Geschlecht* von F/K (man schreibt auch $g = g(F) = g(F/K)$).

Wir betrachten als nächstes Erweiterungen algebraischer Funktionenkörper.

Definition I.2.10

- i) F'/K' heißt *algebraische Erweiterung* von F/K , wenn F' algebraische Erweiterung von F ist und $K' \supseteq K$.
- ii) Eine algebraische Erweiterung F'/K' heißt *Konstantenerweiterung*, wenn $F' = FK'$ ist.
- iii) Eine algebraische Erweiterung F'/K' von F/K heißt *endlich*, wenn $[F' : F] < \infty$ gilt.

Definition I.2.11 Sei F'/K' eine algebraische Erweiterung von F/K . Eine Stelle P' von F' (d.h. $P' \in \mathbb{P}_{F'}$) heißt *Fortsetzung* einer Stelle $P \in \mathbb{P}_F$, wenn $P \subseteq P'$. Man schreibt in diesem Fall auch $P' \mid P$.

Satz I.2.12 F'/K' sei algebraische Erweiterung von F/K . Weiter seien $P' \in \mathbb{P}_{F'}$ und $P \in \mathbb{P}_F$. Dann sind äquivalent:

- (a) $P' \mid P$
- (b) $O_P \subseteq O_{P'}$

- (c) es gibt eine natürliche Zahl $e(P' | P) \geq 1$, so daß $v_{P'}(x) = e(P' | P) \cdot v_P(x)$ für alle $x \in F$.

In dieser Situation gilt auch $P = P' \cap F$ und $O_P = O_{P'} \cap F$. Daher heißt P auch *Einschränkung* von P' auf F .

Man hat zudem eine Einbettung

$$\begin{cases} O_P/P \hookrightarrow O_{P'}/P' \\ x + P \mapsto x + P' \end{cases} .$$

Insbesondere gilt somit $F_P \subseteq F_{P'}$. Man bezeichnet $f(P' | P) := [F_{P'} : F_P]$ als *Relativgrad* von $P' | P$ und $e(P' | P)$ als *Verzweigungsgrad* von $P' | P$.

Die *Conorm* von P ist definiert durch: $Con_{F'/F}(P) := \sum_{P'|P} e(P' | P) \cdot P'$.

Definition I.2.13 Die Situation sei die gleiche wie oben.

- i) P heißt *verzweigt* in F' , wenn ein $P' | P$ existiert mit $e(P' | P) > 1$ (sonst heißt P *unverzweigt* in F').
- ii) P heißt *voll verzweigt* in F' , wenn ein $P' | P$ existiert mit $e(P' | P) = [F' : F]$.

Lemma I.2.14 Sei F''/K'' eine weitere algebraische Erweiterung von F'/K' . Sei $P' | P$ und $P'' | P'$. Dann folgt $P'' | P$ und

- (a) $e(P'' | P) = e(P' | P) \cdot e(P'' | P')$
- (b) $f(P'' | P) = f(P' | P) \cdot f(P'' | P')$

Lemma I.2.15 Sei F'/K' eine algebraische Erweiterung von F/K .

- (a) $P' \in \mathbb{P}_{F'} \Rightarrow$ es existiert $P \in \mathbb{P}_F$ mit $P' | P$, nämlich $P = P' \cap F$.
- (b) $P \in \mathbb{P}_F \Rightarrow$ es gibt mindestens eine, aber höchstens endlich viele $P' \in \mathbb{P}_{F'}$ mit $P' | P$.

Satz I.2.16 Sei F'/K' eine endliche Erweiterung von F/K , P eine Stelle von F/K , und P_1, \dots, P_n seien alle über P liegenden Stellen von F' . Sei $e_i := e(P_i | P)$ und $f_i := f(P_i | P)$ (für $i = 1, \dots, n$). Dann gilt

$$\sum_{i=1}^n e_i f_i = [F' : F].$$

Definition I.2.17 Sei F'/F eine endliche separable Erweiterung des Funktionenkörpers F/K , und $P \in \mathbb{P}_F$ sei eine Stelle von F/K . Dann existiert für den algebraischen Abschluß $O'_P = \bigcap_{P'|P} O_{P'}$ von O_P in F' eine Basis $\{u_1, \dots, u_n\}$ von F'/F derart, daß

$$O'_P = \sum_{i=1}^n O_P \cdot u_i.$$

Man nennt $\{u_1, \dots, u_n\}$ eine *Ganzheitsbasis* von F'/F an der Stelle P .

Beispiel. Ein Beispiel eines Funktionenkörpers F/K ist der Fall des *rationalen Funktionenkörpers* $F = K(x)$, wobei x transzendent über K ist. Für ein normiertes, irreduzibles Polynom $p(x) \in K[x]$ bilden

$$O_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \nmid g(x) \right\}$$

$$\text{und} \quad P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \nmid g(x) \wedge p(x) \mid f(x) \right\}$$

einen diskreten Bewertungsring und das zugehörige maximale Ideal (ist $p(x) = x - \alpha$ für ein $\alpha \in K$, dann setzen wir $P_\alpha := P_{x-\alpha}$). Zusammen mit

$$O_\infty := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], \deg f(x) \leq \deg g(x) \right\}$$

$$\text{und} \quad P_\infty = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], \deg f(x) < \deg g(x) \right\}.$$

hat man dann alle diskreten Bewertungsringe und deren maximalen Idealen von $K(x)/K$. Ist $p(x) \in K[x]$ irreduzibel, dann ist $p(x)$ ein Primelement von $P = P_{p(x)}$, und die zugehörige diskrete Bewertung sieht wie folgt aus: Schreibt man ein Element $z \in K(x) \setminus 0$ in der Form $z = p(x)^n \cdot \frac{f(x)}{g(x)}$, wobei $p(x) \nmid g(x)$ und $p(x) \nmid f(x)$, dann ist $v_P(z) = n \in \mathbb{Z}$. Ist $P = P_\infty$ und $z = \frac{f(x)}{g(x)} \in K(x)$, dann ist $v_P(z) = \deg g(x) - \deg f(x)$. Ferner ist K der volle Konstantenkörper von $K(x)/K$ und P_∞, P_α (für $\alpha \in K$) sind sämtliche Stellen vom Grad 1.

I.3 Geometrische Goppa Codes

Dieser Abschnitt gibt eine Verbindung zwischen der Codierungstheorie und der Theorie der Funktionenkörper an.

Gegeben sei ein algebraischer Funktionenkörper F/\mathbb{F}_q mit vollem Konstantenkörper \mathbb{F}_q und Geschlecht $g = g(F/\mathbb{F}_q)$. Seien $P_1, \dots, P_n \in \mathbb{P}_F$ paarweise verschiedene Stellen vom Grad 1. Sei $G \in \mathcal{D}_F$ ein Divisor mit $\{P_1, \dots, P_n\} \cap \text{supp}(G) = \emptyset$. Wir setzen dann $D := P_1 + \dots + P_n$ und definieren eine \mathbb{F}_q -lineare Abbildung $ev_D : \mathcal{L}(G) \rightarrow \mathbb{F}_q^n$ durch $ev_D(x) := (x(P_1), \dots, x(P_n))$. Man beachte dabei: Für $x \in \mathcal{L}(G)$ und $P_i \notin \text{supp}(G)$ folgt $v_{P_i}(x) \geq 0$. Deshalb ist $x \in O_{P_i}$ und insbesondere $x(P_i) \in \mathbb{F}_q$.

Definition I.3.1

$$C(D, G) := \text{Im}(ev_D)$$

heißt der zu D und G gehörige *geometrische Goppa Code*.

Satz I.3.2 Seien die Bezeichnungen wie oben. Dann ist $C(D, G)$ ein $[n, k, d]$ -Code mit

$$k = \dim(\mathcal{L}(G)) - \dim(\mathcal{L}(G - D)) \quad \text{und} \quad d \geq n - \deg(G).$$

Ist $0 < \deg(G) < n$, dann folgt

$$k = \dim(\mathcal{L}(G)) \geq \deg(G) + 1 - g \quad \text{und} \quad k + d \geq n + 1 - g.$$

Wir haben somit eine untere Schranke für die Parameter, und es gilt zusammen mit der Singleton-Schranke

$$n + 1 \geq k + d \geq n + 1 - g.$$

Man bekommt also einen Code mit guten Parametern, wenn man einen Funktionenkörper F mit kleinem g und vielen rationalen Stellen findet. Das Verhältnis ist dabei unter anderem durch die *Hasse-Weil* Schranke bestimmt:

$$|N - (q + 1)| \leq 2gq^{1/2},$$

wobei N die Anzahl der rationalen Stellen von F ist.

Kapitel II

Die Niederreiter-Xing-Konstruktion für lineare Codes

In diesem Kapitel wird die im Jahr 2000 in AAEECC ([4]) veröffentlichte Konstruktion von Harald Niederreiter und Chaoping Xing beschrieben. Sie selbst haben diese als eine *propagation rule for linear codes* bezeichnet. Gemeint sind Methoden, durch Kombination vergleichsweise kurzer linearer Codes einen langen linearen Code mit neuen Parametern zu konstruieren. Andere Beispiele hierfür findet man in [1, chapter 18]. Niederreiter und Xing gehen von einem einzigen beliebigen linearen Code aus, um daraus einen längeren Code größerer Dimension zu erhalten. Dabei stellen sie den gegebenen linearen Code als (verallgemeinerten) algebraisch-geometrischen Code dar und benutzen dann eine Erweiterung des bei der Darstellung verwendeten Funktionenkörpers, um einen neuen Code zu konstruieren.

II.1 Darstellung linearer Codes als algebraisch-geometrische Codes

In diesem Abschnitt wird zuerst eine verallgemeinerte Form der geometrischen Goppa-Codes ([2, II.2.] oder Kapitel 1) eingeführt und anschließend gezeigt, daß sich jeder lineare Code in dieser verallgemeinerten Form darstellen läßt.

Sei F/\mathbb{F}_q ein Funktionenkörper mit vollem Konstantenkörper \mathbb{F}_q , d.h. F sei ein algebraischer Funktionenkörper über \mathbb{F}_q derart, daß \mathbb{F}_q algebraisch abgeschlossen ist in F . Bekanntermaßen gilt dann

Lemma II.1.1 (schwacher Approximationssatz). *Sei F/\mathbb{F}_q ein Funktionenkörper über dem endlichen Körper \mathbb{F}_q , und seien P_1, \dots, P_n paarweise verschiedene Stellen von F . Dann existiert für beliebige $a_1, \dots, a_n \in F$ und beliebige $e_1, \dots, e_n \in \mathbb{Z}$ ein $x \in F$, so daß*

$$v_{P_l}(x - a_l) = e_l \quad \text{für } 1 \leq l \leq n$$

gilt. (Beweis siehe [2, I.3.1 Theorem])

Eine Stelle P eines Funktionenkörpers F/\mathbb{F}_q heißt *rational*, wenn F_P (d.h. der Restklassenkörper von P) gleich \mathbb{F}_q ist. Für eine rationale Stelle $P \in F/\mathbb{F}_q$ und beliebiges $f \in \mathcal{O}_P$ beachte man, daß $f(P) = f + P \in \mathbb{F}_q$.

Nun zur verallgemeinerten Form geometrischer Goppa-Codes: Sei F/\mathbb{F}_q ein Funktionenkörper, und seien P_1, \dots, P_n paarweise verschiedene rationale Stellen von F . Sei V ein endlich-dimensionaler \mathbb{F}_q -linearer Unterraum von F derart, daß

$$v_{P_l}(f) \geq 0 \quad \text{für } 1 \leq l \leq n \text{ und } f \in V. \quad (2.1)$$

(Die Existenz eines solchen Unterraums V ist offensichtlich, z.B. nehme man sich $f_1, \dots, f_r \in F$ mit $v_{P_l}(f_j) \geq 0$, und setze $V := \text{span}\{f_1, \dots, f_r\}$. Mit den Rechenregeln für die diskreten Bewertungen v_{P_l} hat man sofort, daß V ein \mathbb{F}_q -linearer Unterraum mit der verlangten Eigenschaft ist.)

Betrachte die Abbildung $\theta : V \rightarrow \mathbb{F}_q^n$, definiert durch

$$\theta(f) = (f(P_1), \dots, f(P_n)) \quad \text{für } f \in V. \quad (2.2)$$

Das Bild $\text{Im}(\theta)$ wird mit $C_V(P_1, \dots, P_n)$ bezeichnet und heißt *verallgemeinerter algebraisch-geometrischer Code*. Da θ eine \mathbb{F}_q -lineare Abbildung ist, ist $C_V(P_1, \dots, P_n)$ ein linearer Code über \mathbb{F}_q der Länge n .

Lemma II.1.2 *Sei C ein linearer Code über \mathbb{F}_q der Länge n und der Dimension k . Dann existieren ein Funktionenkörper F/\mathbb{F}_q , n paarweise verschiedene rationale Stellen P_1, \dots, P_n von F/\mathbb{F}_q und ein k -dimensionaler \mathbb{F}_q -linearer Unterraum V von F derart, daß $C = C_V(P_1, \dots, P_n)$ ist.*

Beweis. Wie wir im Anhang A beweisen werden, kann man zu gegebenem q stets einen Funktionenkörper F/\mathbb{F}_q mit beliebig großer Anzahl an rationalen Stellen finden. Insbesondere existiert somit ein Funktionenkörper F/\mathbb{F}_q mit n rationalen Stellen P_1, \dots, P_n . Seien $\mathbf{c}_1, \dots, \mathbf{c}_k$ eine Basis von C . Wir setzen

$$\mathbf{c}_j = (c_{j1}, \dots, c_{jn}) \in \mathbb{F}_q^n \quad \text{für } 1 \leq j \leq k.$$

Nach dem schwachen Approximationssatz II.1.1 existiert für alle $1 \leq j \leq k$ ein f_j derart, daß

$$v_{P_l}(f_j - c_{jl}) \geq 1 \quad \text{für } 1 \leq l \leq n. \quad (2.3)$$

Somit gilt $f_j - c_{jl} \in P_l$, also $f_j(P_l) = c_{jl}$ für alle j, l . Gleichzeitig ist für f_j auch (2.1) erfüllt, denn nach der Dreiecksungleichung gilt

$$v_{P_l}(f_j - c_{jl}) \geq \min\{v_{P_l}(f_j), v_{P_l}(c_{jl})\}.$$

Ist $c_{jl} \in \mathbb{F}_q$, $c_{jl} \neq 0$, dann gilt $v_{P_l}(c_{jl}) = 0$, und es folgt wegen (2.3)

$$v_{P_l}(f_j) \geq 0.$$

Ist $c_{jl} = 0$, dann ist mit (2.3) die Aussage (2.1) trivial.

Sei nun V der \mathbb{F}_q -lineare Unterraum von F , der durch f_1, \dots, f_k aufgespannt wird, und $\theta : V \rightarrow \mathbb{F}_q^n$ definiert wie in (2.2). Dann gilt

$$\theta(f_j) = \mathbf{c}_j \in \mathbb{F}_q^n \quad \text{für } 1 \leq j \leq k. \quad (2.4)$$

Nun folgt sofort, daß $\dim(V) = k$ und $C = C_V(P_1, \dots, P_n)$. Denn angenommen, die f_j seien linear abhängig. Es existieren dann $\gamma_j \in \mathbb{F}_q$ (nicht alle = 0) derart, daß $\sum \gamma_j f_j = 0$. Unter der linearen Abbildung θ hat man $\theta(\sum \gamma_j f_j) = \theta(0) = 0$. Andererseits ist $\theta(\sum \gamma_j f_j) = \sum \gamma_j \theta(f_j) = \sum \gamma_j \mathbf{c}_j \neq 0$, da die \mathbf{c}_j eine Basis von C bilden. Die f_j sind also ebenfalls linear unabhängig, und daher gilt $\dim(V) = k$. Mit (2.4) hat man zudem, daß $\theta(V) = C$, und damit $C_V(P_1, \dots, P_n) = C$ ist.

II.2 Eine Konstruktion von Niederreiter und Xing

In diesem Abschnitt wird die eigentliche Konstruktion von Niederreiter und Xing vorgestellt, welche wir im folgenden auch als NX-Konstruktion bezeichnen werden. Die Konstruktion stützt sich im wesentlichen auf Verzweigungstheorie algebraischer Funktionenkörper.

Satz II.2.1 *Sei C ein linearer $[n, k, d]$ -Code über \mathbb{F}_q . Dann existiert für beliebige $h, r, s \in \mathbb{Z}$ mit $2 \leq h \leq q$, $1 \leq r < h$, $0 \leq s \leq r$ ein linearer $[N, K, D]$ -Code über \mathbb{F}_q mit*

$$N = hn, \quad K = k(s + 1) + r - s, \quad D \geq \min \{(h - s)d, (h - r)n\}.$$

Beweis. Nach Lemma II.1.2 existieren ein Funktionenkörper F/\mathbb{F}_q , n paarweise verschiedene rationale Stellen P_1, \dots, P_n von F/\mathbb{F}_q und ein k -dimensionaler Unterraum $V \leq F$ derart, daß $C = C_V(P_1, \dots, P_n)$. Wähle eine weitere Stelle $Q \neq P_1, \dots, P_n$.

Nach dem schwachen Approximationsatz II.1.1 existiert ein $x \in F$ derart, daß $v_{P_l}(x) \geq 1$ für $1 \leq l \leq n$ und $v_Q(x) = -1$. Wir wählen eine Teilmenge $H \subseteq \mathbb{F}_q$ mit $|H| = h$ und $0 \in H$, und betrachten das Polynom

$$\varphi(T) := \prod_{\alpha \in H} (T - \alpha) - x. \quad (2.5)$$

Nach [2, III.1.14.(2) Proposition] (für $P = Q$) ist $\varphi(T)$ ein in $F[T]$ irreduzibles Polynom. Folglich ist die durch $\varphi(y) = 0$ definierte einfache Erweiterung $E = F(y)$ vom Grad $[E : F] = h$, und $\varphi(T)$ ist das Minimalpolynom von y .

Wir zeigen nun, daß \mathbb{F}_q der volle Konstantenkörper von E ist. Sei R eine Fortsetzung von Q auf E , und $e := e(R | Q)$ sei der Verzweigungsgrad. Dann gilt

$$v_R(x) = e \cdot \underbrace{v_Q(x)}_{=-1} = -e. \quad (2.6)$$

Andererseits gilt mit $\varphi(y) = 0$

$$v_R(x) = v_R\left(\prod_{\alpha \in H} (y - \alpha)\right) = \sum_{\alpha \in H} v_R(y - \alpha).$$

Da nun $v_R(\alpha) \geq 0$ (wegen $\alpha \in \mathbb{F}_q$) und somit $v_R(y) < 0$ (sonst wäre auch $v_R(x) \geq 0$, was im Widerspruch zu (2.6) stände), gilt nach der scharfen Dreiecksungleichung

$$v_R(y - \alpha) = v_R(y).$$

Damit hat man

$$-e = v_R(x) = v_R\left(\prod_{\alpha \in H} (y - \alpha)\right) = h \cdot v_R(y).$$

Folglich ist h ein Teiler von e , und insbesondere $h \leq e$. Wegen $\sum e_i f_i = [E : F] = h$ gilt aber auch $e \leq h$. Also ist $e = h$ und $v_R(y) = -1$.

Es folgt wegen $e = [E : F]$, daß

$$Q \text{ voll verzweigt in } E/F. \quad (2.7)$$

Aus der letzten Aussage erhält man wiederum, daß

$$\mathbb{F}_q \text{ der volle Konstantenkörper von } E \quad (2.8)$$

ist. Denn angenommen, E habe einen Konstantenkörper $K' \neq \mathbb{F}_q$. Da E/K' eine endliche Erweiterung von F/\mathbb{F}_q ist, gilt nach [2, III.1.2], daß $[K' : \mathbb{F}_q] < \infty$. Wir schreiben deshalb $K' = \mathbb{F}_{q^i}$. Sei $F' := F \cdot \mathbb{F}_{q^i}$ die Konstantenerweiterung von F/\mathbb{F}_q mit \mathbb{F}_{q^i} . Da $F \cap \mathbb{F}_{q^i} = \mathbb{F}_q$ (siehe [2, III.1.2.(a)]) aber $\mathbb{F}_q \neq \mathbb{F}_{q^i}$, ist $[F' : F] > 1$. Folglich ist $[E : F'] < h$. Nach [2, III.6.3 Theorem] gilt, daß F'/F unverzweigt ist (d.h. $e(P' | P) = 1$ für alle $P \in \mathbb{P}_F$ und alle $P' \in \mathbb{P}_{F'}$ mit $P' | P$). Insbesondere ist Q in F' unverzweigt. Dies steht aber im Widerspruch zu (2.7). Denn sei $R \supseteq Q' \supseteq Q$ für $Q' \in \mathbb{P}_{F'}$. Nach Satz I.2.16 ist $e(R | Q') \leq [E : F'] < h$. Mit Lemma I.2.14 gilt dann

$$h = e(R | Q) = e(R | Q') \cdot \underbrace{e(Q' | Q)}_{=1} < h.$$

Somit hat man einen Widerspruch und (2.8) ist bewiesen.

Wir zeigen nun, daß jede Stelle P_j (für $1 \leq j \leq n$) in E voll zerlegt ist, d.h. P_j besitzt genau $[E : F]$ Fortsetzungen in E . Dabei werden wir den Satz von Kummer [2, III.3.7] benutzen.

Für eine Stelle P von F setzen wir entsprechend:

$$\overline{F} := F_P = O_P/P \text{ Restklassenkörper von } P$$

$$\overline{a} := a(P) \text{ Restklasse von } a \in O_P$$

$$\phi(T) = \sum c_i T^i \text{ sei Polynom mit } c_i \in O_P, \text{ dann schreiben wir}$$

$$\overline{\phi}(T) := \sum \overline{c}_i T^i \in \overline{F}[T].$$

Satz II.2.2 (Kummer). Sei $F' = F(y)$, wobei y ganz über O_P , und sei $\varphi(T) \in O_P[T]$ das Minimalpolynom von y über F . Ferner bezeichne

$$\overline{\varphi}(T) = \prod_{i=1}^r \gamma_i(T)^{\varepsilon_i}$$

die Zerlegung von $\overline{\varphi}(T)$ in irreduzible Faktoren über \overline{F} (d.h. die Polynome $\gamma_1(T), \dots, \gamma_r(T)$ sind irreduzibel, normiert, paarweise verschieden in $\overline{F}[T]$ und $\varepsilon_i \geq 1$). Wähle normierte Polynome $\varphi_i(T) \in O_P[T]$ derart, daß

$$\overline{\varphi}_i(T) = \gamma_i(T) \quad \text{und} \quad \deg \varphi_i(T) = \deg \gamma_i(T).$$

Dann existiert für $1 \leq i \leq r$ eine Stelle P_i von F' mit

$$P_i | P, \quad \varphi_i(y) \in P_i \quad \text{und} \quad f(P_i | P) \geq \deg \gamma_i(T),$$

wobei $P_i \neq P_j$ für $i \neq j$.

Eine stärkere Aussage erhält man, falls

$$\varepsilon_i = 1 \quad \text{für } i = 1, \dots, r, \text{ oder}$$

$\{1, y, \dots, y^{n-1}\}$ eine Ganzheitsbasis für P ist.

Dann folgt, daß für $1 \leq i \leq r$ genau eine Stelle P_i von F' existiert mit $P_i \mid P$ und $\varphi_i(y) \in P_i$. Die Stellen P_1, \dots, P_r sind alle Stellen von F' , die über P liegen, und es gilt

$$\text{Con}_{F'/F}(P) = \sum_{i=1}^r \varepsilon_i P_i,$$

d.h. $\varepsilon_i = e(P_i \mid P)$. Der Restklassenkörper $F_{P_i} = O_{P_i}/P_i$ ist isomorph zu $\overline{F}[T]/(\gamma_i(T))$, also ist $f(P_i \mid P) = \deg \gamma_i(T)$. (Beweis siehe [2, III.3.7])

Wir betrachten nun $\varphi(T)$ aus (2.5). Wegen $v_P(x) > 0$ (für $P \in \{P_1, \dots, P_n\}$) ist $\varphi(T) \in O_P[T]$. Wie schon oben gesehen, ist $\varphi(T)$ das Minimalpolynom von y über F , d.h. insbesondere, daß y ganz über O_P ist. Als Polynom in O_P/P betrachtet, erhält man

$$\overline{\varphi}(T) = \prod_{\alpha \in H} (T - \alpha) \in \overline{F}[T]$$

(man beachte hierbei, daß $x(P) = 0$ wegen $v_P(x) > 0$ und daß $\alpha(P) = \alpha$ wegen $\alpha \in \mathbb{F}_q$). Dies ist bereits die gewünschte Zerlegung in irreduzible Faktoren über \overline{F} . Dabei ist den obigen Bezeichnungen entsprechend $\gamma_\alpha = (T - \alpha)$ und $\varepsilon_\alpha = 1$. Darüber hinaus hat man so auch schon die zugehörigen normierten Polynome vom selben Grad in $O_P[T]$, da trivialerweise auch $(T - \alpha) \in O_P[T]$ gilt. Nach dem Satz von Kummer folgt schließlich, daß für jedes $\alpha \in H$ genau eine Stelle $R^{(\alpha)}$ von E mit

$$R^{(\alpha)} \mid P \quad \text{und} \quad (y - \alpha) \in R^{(\alpha)} \quad (2.9)$$

existiert. Dies sind alle Fortsetzungen von P auf E . Jedes $P \in \{P_1, \dots, P_n\}$ hat also genau h Fortsetzungen, d.h. P ist voll zerlegt in E .

Wir bezeichnen für $1 \leq l \leq n$ und $\alpha \in H$ mit $R_l^{(\alpha)}$ die eindeutige Fortsetzung von P_l auf E , für welche

$$y(R_l^{(\alpha)}) = \alpha$$

gilt (man beachte: $(y - \alpha) \in R_l^{(\alpha)} \Leftrightarrow y(R_l^{(\alpha)}) = \alpha$).

Wir betrachten als nächstes

$$U := \left\{ \sum_{j=0}^r v_j y^j \in E \mid v_j \in V \text{ für } 0 \leq j \leq s, v_j \in \mathbb{F}_q \text{ für } s+1 \leq j \leq r \right\}. \quad (2.10)$$

U ist ein \mathbb{F}_q -linearer Unterraum von E . Da $\dim V = k$, und weil $1, y, \dots, y^r$ linear unabhängig über F , sieht man leicht, daß

$$\dim(U) = k(s+1) + r - s$$

(denn sei $(\overline{v}_1, \dots, \overline{v}_k)$ eine Basis von V ; dann ist offensichtlich

$$\{\overline{v}_i \cdot y^j \mid 1 \leq i \leq k, 0 \leq j \leq s\} \cup \{y^j \mid s+1 \leq j \leq r\}$$

eine Basis von U).

Aus $y(R_l^{(\alpha)}) = \alpha$ für $1 \leq l \leq n$ und $\alpha \in H$ folgt, daß

$$v_R(y) \geq 0 \quad \text{für alle } R \in \{R_l^{(\alpha)} \mid 1 \leq l \leq n, \alpha \in H\}. \quad (2.11)$$

Denn angenommen, es sei $v_{R_l^{(\alpha)}}(y) < 0$. Dann gilt mit der scharfen Dreiecksungleichung $v_{R_l^{(\alpha)}}(\alpha - y) = v_{R_l^{(\alpha)}}(y) < 0$. Daraus folgt $y(R_l^{(\alpha)}) \neq \alpha$, und man hat einen Widerspruch.

Mit (2.1) (d.h. $v_{P_l}(f) \geq 0$ für alle $1 \leq l \leq n$ und $f \in V$) erhält man die analoge Aussage

$$v_R(u) \geq 0 \quad \text{für alle } R \in \{R_l^{(\alpha)} \mid 1 \leq l \leq n, \alpha \in H\} \text{ und } u \in U.$$

$$\text{Denn: } v_R(u) = v_R(\sum_{j=0}^r v_j y^j) \geq \min\{\underbrace{v_R(v_0)}_{(2.1) \geq 0}, \underbrace{v_R(v_1)}_{(2.1) \geq 0} + \underbrace{v_R(y)}_{(2.11) \geq 0}, \dots, \underbrace{v_R(v_s)}_{(2.1) \geq 0} + \underbrace{v_R(y^s)}_{(2.11) \geq 0}\} \geq 0.$$

Wir setzen $N := h \cdot n$ und betrachten die Abbildung

$$\psi : U \rightarrow \mathbb{F}_q^N$$

$$\text{mit} \quad \psi(u) := \left(u(R_l^{(\alpha)}) \right)_{(1 \leq l \leq n, \alpha \in H)} \quad \text{für alle } u \in U.$$

Wir zeigen zuerst, daß $\psi(u)$ auch tatsächlich in \mathbb{F}_q^N liegt: Zum einen bezeichnet $R_l^{(\alpha)}$ die Fortsetzung von P_l , für welche $y(R_l^{(\alpha)}) = \alpha$ gilt. Mit der natürlichen Einbettung von F_{P_l} in $E_{R_l^{(\alpha)}}$ hat man zum anderen, daß für $z \in F$ $z(R_l^{(\alpha)}) = z(P_l)$ ist. Es gilt somit

$$u(R_l^{(\alpha)}) = \sum_{j=0}^r (v_j y^j)(R_l^{(\alpha)}) = \sum_{j=0}^r v_j (P_l) \alpha^j. \quad (2.12)$$

Da P_l rational ist, liegt $v_j(P_l)$ in \mathbb{F}_q . Also ist die Abbildung vernünftig definiert. Das Bild $\text{Im}(\psi)$ ist ein linearer Code über \mathbb{F}_q der Länge N , denn ψ ist \mathbb{F}_q -linear.

Im letzten Beweisschritt werden wir zeigen, daß der verallgemeinerte algebraisch-geometrischer Code $\text{Im}(\psi)$ die Eigenschaften aus Satz II.2.1 besitzt.

Für ein beliebiges $u \in U \setminus \{0\}$ bestimmen wir das Gewicht $wt(\psi(u))$. Dazu schreiben wir

$$u = \sum_{j=0}^r v_j y^j \quad \text{mit } v_j \in V \text{ für } 0 \leq j \leq s, v_j \in \mathbb{F}_q \text{ für } s+1 \leq j \leq r;$$

dabei sind nicht alle $v_j = 0$. Sei t die größte Indexzahl, für die $v_t \neq 0$ ist, d.h.

$$u = \sum_{j=0}^t v_j y^j \quad \text{mit } v_t \neq 0.$$

Wir betrachten zuerst den Fall $0 \leq t \leq s$. Dann hat man für alle $1 \leq l \leq n$ und $\alpha \in H$

$$u(R_l^{(\alpha)}) = \sum_{j=0}^t v_j (P_l) \alpha^j.$$

Dies sind $h \cdot n$ Gleichungen. Da in diesem Fall $v_t \in V$ ist und $C = C_V(P_1, \dots, P_n)$, gilt $v_t(P_l)_{1 \leq l \leq n} \in C$, somit hat man

$$wt(v_t(P_l)_{1 \leq l \leq n}) \geq d.$$

Daraus folgt $v_t(P_l) \neq 0$ für mindestens d der $l \in \{1, \dots, n\}$. Für jedes dieser mindestens d verschiedenen l existieren höchstens t , und damit (für den Fall $t = s$) höchstens s verschiedene $\alpha \in H$ derart, daß $u(R_l^{(\alpha)}) = 0$, denn $\sum_{j=0}^t v_j(P_l)\alpha^j$ kann als Polynom in α höchstens t Nullstellen besitzen. Umgekehrt existieren also mindestens $h - s$ Elemente $\alpha \in H$ mit $u(R_l^{(\alpha)}) \neq 0$ (für jedes der mindestens d verschiedenen $l \in \{1, \dots, n\}$), d.h.

$$wt(\psi(u)) \geq (h - s)d.$$

Im zweiten Fall sei $s + 1 \leq t \leq r$. Also gilt jetzt $v_t \in \mathbb{F}_q$. Mit der natürlichen Einbettung $\mathbb{F}_q \hookrightarrow O_{P_l}/P_l : a \mapsto a(P_l)$ hat man insbesondere, daß $v_t(P_l) = v_t \neq 0$. Für $l \in \{1, \dots, n\}$ und $\alpha \in H$ schreiben wir

$$u(R_l^{(\alpha)}) = v_t \alpha^t + \sum_{j=0}^{t-1} v_j(P_l) \alpha^j.$$

Für jedes $l \in \{1, \dots, n\}$ gibt es somit höchstens t , und damit höchstens r verschiedene $\alpha \in H$ mit $u(R_l^{(\alpha)}) = 0$. Umgekehrt existieren also für jedes $l \in \{1, \dots, n\}$ mindestens $h - r$ Elemente $\alpha \in H$ mit $u(R_l^{(\alpha)}) \neq 0$. Es folgt

$$wt(\psi(u)) \geq (h - r)n.$$

Damit ist gezeigt, daß der Minimalabstand von $\text{Im}(\psi) \geq \min\{(h - s)d, (h - r)n\}$ ist. Darüber hinaus weiß man, daß ψ injektiv ist. Denn sei $u \in U$, $u \neq 0$. Wegen $wt(\psi(u)) \geq \min\{(h - s)d, (h - r)n\} > 0$, folgt $\psi(u) \neq 0$.

Aus der Injektivität folgt wiederum

$$\dim(\text{Im}(\psi)) = \dim(U) = k(s + 1) + r - s.$$

□

Kapitel III

Bemerkungen zu der NX-Konstruktion von Özbudak und Stichtenoth

In diesem Kapitel wird eine Arbeit von Ferruh Özbudak und Henning Stichtenoth behandelt ([10]). Diese bezieht sich direkt auf die durch Niederreiter und Xing vorgestellte Konstruktion aus dem vorigen Kapitel. Wie wir im vorherigen gesehen haben, ist die NX-Konstruktion ziemlich kompliziert. Es werden zudem Kenntnisse über algebraische Funktionenkörper und algebraische Goppa-Codes vorausgesetzt. Özbudak und Stichtenoth haben in ihrer Arbeit gezeigt, daß die NX-Konstruktion ein Spezialfall einer einfachen Konstruktion ist, welche mit linearer Algebra auskommt.

III.1 Eine Konstruktion von Özbudak und Stichtenoth

Wir werden nun die oben erwähnte einfache Konstruktion vorstellen, welche wir im folgenden auch als ÖS-Konstruktion bezeichnen werden. Gegeben seien dazu

1. ein $[m, k]$ -Code C über \mathbb{F}_q und
2. k ($=\dim(C)$) lineare Codes W_1, \dots, W_k , alle von der Länge n .

Die Elemente von C werden von uns als Zeilenvektoren und die Elemente von W_j als Spaltenvektoren aufgefaßt. Wir wählen eine Basis $(c^{(1)}, \dots, c^{(k)})$ von C fest aus und bezeichnen mit G die $k \times m$ -Matrix, welche $c^{(1)}, \dots, c^{(k)}$ als Zeilenvektoren hat. Damit ist G eine Erzeugermatrix von C . Für $1 \leq j \leq k$ setzen wir

$$C_j := \text{span}\{c^{(1)}, \dots, c^{(j)}\} \subseteq \mathbb{F}_q^m.$$

Da die $c^{(1)}, \dots, c^{(j)}$ linear unabhängig sind, ist C_j ein j -dimensionaler linearer Unterraum von C . Also ist C_j ein $[m, j]$ Untercode von C , und es gilt

$$C_1 \subseteq C_2 \subseteq \dots \subseteq C_k = C.$$

Sei M die Menge aller $n \times k$ Matrizen, deren j -te Spalte aus W_j für $1 \leq j \leq k$. M ist ein linearer Unterraum von $\text{Mat}(n \times k)$ der Dimension

$$\dim(M) = \sum_{j=1}^k \dim(W_j).$$

Denn: Sei $\dim(W_j) = r_j$. Für $1 \leq j \leq k$ wählen wir eine Basis $(w_{j1}, \dots, w_{jr_j})$ von W_j . Man beachte dabei, daß die $w_{jl} \in \mathbb{F}_q^m$ sind. Da die Spalten einer Matrix aus M jeweils aus W_j sind, bilden die $n \times k$ -Matrizen

$$\begin{array}{ccccccc} (w_{11}, 0, \dots, 0), & (w_{12}, 0, \dots, 0), & \cdots, & (w_{1r_1}, 0, \dots, 0), \\ (0, w_{21}, 0, \dots, 0), & (0, w_{22}, 0, \dots, 0), & \cdots, & (0, w_{2r_2}, 0, \dots, 0), \\ \vdots & & & \\ (0, \dots, 0, w_{k1}), & (0, \dots, 0, w_{k2}), & \cdots, & (0, \dots, 0, w_{kr_k}) \end{array}$$

eine Basis von M . Somit ist $\dim(M) = \sum_j r_j$.

Der nächste Satz enthält den eigentlichen Code, der eine Verallgemeinerung der Code-Konstruktion von Niederreiter-Xing ist.

Satz III.1.1 *Die Bezeichnungen seien dieselben wie oben. Dann hat der lineare Code*

$$W := \{A \cdot G \mid A \in M\}$$

folgende Parameter:

$$\text{Länge}(W) = \text{Länge}(C) \cdot \text{Länge}(W_j) = m \cdot n,$$

$$\dim(W) = \sum_{j=1}^k \dim(W_j),$$

$$d(W_j) \geq \min\{d(W_j) \cdot d(C_j) \mid 1 \leq j \leq k\}.$$

Beweis. Zuerst zeigen wir, daß es sich bei W um einen Code handelt. Dies ist leicht mit dem Distributivgesetz für Matrizenmultiplikation zu sehen. Seien $B, C \in M$, dann gilt $(B \cdot G) + (C \cdot G) = (B + C) \cdot G$. Da W ein Vektorraum ist, liegt $(B + C)$ in M , und daher $(B + C) \cdot G$ wieder in W . Die Elemente aus W sind $n \times m$ -Matrizen. Sie können als Vektoren aus $\mathbb{F}_q^{n \cdot m}$ aufgefaßt werden. Somit ist W ein linearer Code der Länge $n \cdot m = \text{Länge}(C) \cdot \text{Länge}(W_j)$ (man beachte, daß alle W_j dieselbe Länge haben).

Als nächstes beweisen wir die Aussage bezüglich der Dimension. Für $A \in M$ bezeichnen wir mit $a^{(i)}$ die i -te Zeile von A . Damit ist

$$A \cdot G = \begin{pmatrix} a^{(1)} \cdot G \\ \vdots \\ a^{(n)} \cdot G \end{pmatrix}.$$

Die Zeilen $a^{(i)} \cdot G$ sind dabei aus C für $1 \leq i \leq n$. Da die Zeilen von G linear unabhängig sind, folgt für $A \neq 0$ auch $A \cdot G \neq 0$. Denn ist $A \neq 0$, so existiert ein $j \in \{1, \dots, n\}$ mit $a^{(j)} \neq 0$. Wir setzen $a^{(j)} = (a_1^{(j)}, \dots, a_k^{(j)})$ und $G = (g_{ij})_{i,j}$. Es gilt

$$a^{(j)} \cdot G = \left(\sum_{i=1}^k a_i^{(j)} g_{i1}, \dots, \sum_{i=1}^k a_i^{(j)} g_{im} \right) = \sum_{i=1}^k a_i^{(j)} \underbrace{(g_{i1}, \dots, g_{im})}_{i\text{-te Zeile von } G}.$$

Da nicht alle $a_i^{(j)} = 0$ und die Zeilen von G linear unabhängig sind, ist $a^{(j)} \cdot G \neq 0$ und daher auch $A \cdot G \neq 0$. Somit ist die lineare Abbildung $G : M \rightarrow W$ mit $G(A) := A \cdot G$ (für

$A \in M$) nicht nur surjektiv, sondern auch injektiv. Folglich gilt

$$\dim(W) = \dim(M) = \sum_{j=1}^k \dim(W_j).$$

Es fehlt uns jetzt nur noch der Beweis zu der Aussage über den Minimalabstand $d(W)$. Wir wählen uns dazu ein Codewort $X \neq 0$ aus W . Wir schreiben $X = A \cdot G$ mit $A \in M$ und bezeichnen mit w_1, \dots, w_k die Spalten von A (d.h. $w_j \in W_j$ für $1 \leq j \leq k$). Sei $l := \max\{j \mid w_j \neq 0\}$. Dann sind bei allen Zeilen $a^{(1)}, \dots, a^{(n)}$ von A die hinteren Stellen ab der l -ten Stelle gleich Null. Folglich genügen für die Darstellung von $a^{(i)} \cdot G$ für $1 \leq i \leq n$ die ersten l Zeilen von G . Das bedeutet, daß $a^{(i)} \cdot G$ ein Codewort aus C_l ist.

Da $w_l \in W_l$ nicht das Nullcodewort ist, besitzt w_l mindestens $d(W_l)$ Stellen, die ungleich Null sind. Deshalb hat die Matrix A mindestens $d(W_l)$ Zeilen, die keine Nullvektoren sind. Für diese Zeilen hat der Vektor $a^{(i)} \cdot G \in C_l$ das Gewicht $\geq d(C_l)$ (man beachte, daß - wie oben gesehen - für $a^{(i)} \neq 0$ auch $a^{(i)} \cdot G \neq 0$ ist). Das Codewort $X \in W$ hat also mindestens $d(W_l)$ Zeilen $\neq 0$, welche jeweils aus C_l sind und deren Gewicht deshalb $\geq d(C_l)$ ist. Insgesamt gilt

$$wt(X) = \sum_{i=1}^n wt(a^{(i)} \cdot G) \geq d(W_l) \cdot d(C_l).$$

□

Korollar III.1.2 *Gilt in der Situation von oben zusätzlich*

$$d(C_i) = wt(c^{(i)}) \quad \text{für } 1 \leq i \leq k,$$

dann folgt

$$d(W) = \min\{d(W_j) \cdot d(C_j) \mid 1 \leq j \leq k\}.$$

Beweis. Sei $l \in \{1, \dots, k\}$ derart, daß $d(W_l) \cdot d(C_l)$ minimal ist. Wir wählen dann ein $w_l = (w_{1l}, \dots, w_{nl})^t \in W_l$ vom Gewicht $d(W_l)$ und betrachten die $n \times k$ -Matrix $A := (0, \dots, 0, w_l, 0, \dots, 0) \in M$, deren l -te Spalte gerade gleich w_l ist. Dann hat die Matrix $X = A \cdot G$ genau $d(W_l)$ Zeilen, die keine Nullvektoren sind. Für jede Zeile $x^{(i)}$ von X gilt ferner $x^{(i)} = w_{il} \cdot c^{(l)} \in C_l$. Ist $x^{(i)}$ keine Nullzeile (d.h. $w_{il} \neq 0$), dann gilt $wt(x^{(i)}) = wt(c^{(l)}) = d(C_l)$. Die Matrix X hat somit genau $d(W_l)$ Zeilen $\neq 0$ vom Gewicht $d(C_l)$, d.h.

$$wt(X) = d(W_l) \cdot d(C_l) = \min\{d(W_j) \cdot d(C_j) \mid 1 \leq j \leq k\}.$$

□

Bemerkung 1. Die Definition des Codes W hängt - ebenso wie die Aussage über den Minimalabstand - nicht nur von den Codes W_1, \dots, W_k , sondern auch von der Wahl der Basis $(c^{(1)}, \dots, c^{(k)})$ von C ab. Mit einem einfachen Beispiel kann man sehen, daß man unter Umständen einen anderen Code W erhält, wenn nur die Reihenfolge der Basisvektoren $c^{(i)}$ verändert wird. Seien etwa $C = \mathbb{F}_q^k$ (d.h. C ist der $[k, k, 1]$ -Code), $\mathcal{A} = (e^{(1)}, \dots, e^{(k)})$ die kanonische Basis des \mathbb{F}_q^k und $G_{\mathcal{A}}$ die zu \mathcal{A} gehörige Erzeugermatrix von C (d.h. $G_{\mathcal{A}}$

ist die $k \times k$ Einheitsmatrix). Seien W_1, \dots, W_k wieder Codes der Länge n , wobei sich aber mindestens zwei der W_j voneinander unterscheiden, o.E. gelte $W_1 \neq W_2$. Wir setzen - analog zu oben - $W_{\mathcal{A}} = \{A \cdot G_{\mathcal{A}} \mid A \in M\}$, wobei M wie oben definiert ist. Trivialerweise ist dann $W_{\mathcal{A}} = M$. Wir wählen nun mit $\mathcal{B} = (e^{(2)}, e^{(1)}, e^{(3)}, \dots, e^{(k)})$ eine weitere Basis von C . Verglichen mit \mathcal{A} sind also lediglich die ersten beiden Basisvektoren vertauscht worden. Bezeichnet $G_{\mathcal{B}}$ die zu \mathcal{B} die gehörige Erzeugermatrix von C , dann ist

$$W_{\mathcal{B}} := \{A \cdot G_{\mathcal{B}} \mid A \in M\} \\ = \{A \in \text{Mat}(n \times k) \mid 1.\text{Spalte} \in W_2, 2.\text{Spalte} \in W_1, 3.\text{Spalte} \in W_3, \dots, k\text{-te Spalte} \in W_k\}.$$

Da aber $W_1 \neq W_2$ ist, gilt $W_{\mathcal{A}} \neq W_{\mathcal{B}}$.

Bemerkung 2. Für $W_1 = \dots = W_k = B$ ist W gleich dem Produktcode $B \otimes C$, und die Konstruktion kann als Verallgemeinerung des Produktcodes mit der bekannten Eigenschaft $d(B \otimes C) = d(B) \cdot d(C)$ angesehen werden. Ein Produktcode ist wie folgt definiert: Gegeben seien ein $[n_1, k_1, d_1]$ -Code A und ein $[n_2, k_2, d_2]$ -Code B . Dann ist das *direkte Produkt* $A \otimes B$ ein $[n_1 n_2, k_1 k_2, d_1 d_2]$ -Code, der aus allen $n_1 \times n_2$ Matrizen besteht, deren Spalten aus A und deren Zeilen aus B sind (siehe [1, S. 568]).

Sind (a_1, \dots, a_{n_1}) und (b_1, \dots, b_{n_2}) Basen von A bzw. B , dann lassen sich die Elemente von $A \otimes B$ als Linearkombinationen der Vektorprodukte $a_i \times b_j$ darstellen. Dabei ist für $\mathbf{u} = (u_1, \dots, u_m) \in \mathbb{F}_q^m$, $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{F}_q^n$ das Vektorprodukt definiert durch:

$$\mathbf{u} \times \mathbf{v} := \begin{pmatrix} u_1(v_1, \dots, v_n) \\ u_2(v_1, \dots, v_n) \\ \vdots \\ u_m(v_1, \dots, v_n) \end{pmatrix} \in \text{Mat}(m \times n).$$

Bemerkung 3. Die durch Özbudak und Stichtenoth vorgestellte Code-Konstruktion wurde in ähnlicher Weise schon durch andere eingeführt. Unter anderem durch

- i) A.S. Marchukov in [5]. Marchukov konstruiert aus gegebenen Codes a_1, a_2, \dots, a_k der Länge m durch die direkte Summe einen Code $\tilde{A} := a_1 \oplus a_2 \oplus \dots \oplus a_k$ und bezeichnet mit $A_i := a_1 \oplus a_2 \oplus \dots \oplus a_i$ ($1 \leq i \leq k$) einen Untercode von \tilde{A} . Der Minimalabstand von A_i wird mit u_i bezeichnet. Da $A_1 \subseteq \dots \subseteq A_k$, gilt $u_1 \geq u_2 \geq \dots \geq u_k$. Ist $u_1 > u_2 > \dots > u_k$, so heißt $a_1 \oplus a_2 \oplus \dots \oplus a_k$ *monotone Entwicklung* des Codes \tilde{A} . Ab jetzt habe \tilde{A} eine monotone Entwicklung. Für k Codes B_i , alle der selben Länge n und jeweils mit Minimalabstand v_i , bildet Marchukov

$$F := (a_1 \otimes B_1) \oplus (a_2 \otimes B_2) \oplus \dots \oplus (a_k \otimes B_k)$$

(dabei ist mit $a_i \otimes B_i$ der Produktcode gemeint). Der neue Code hat die Länge $m \cdot n$ und den Minimalabstand $d(F) \geq \min\{d(a_i) \cdot d(B_i) \mid 1 \leq i \leq k\}$. Gilt zudem $d(a_i) = u_i$ (die monotone Entwicklung von A wird in in diesem Fall *regulär* genannt), so gilt $d(F) = \min\{d(a_i) \cdot d(B_i) \mid 1 \leq i \leq k\}$. Über die Dimension macht Marchukov an dieser Stelle keine Aussagen.

Die ÖS-Konstruktion ist ein Spezialfall dieses Codes F . Setzt man nämlich

$a_i = \text{span}\{c^{(i)}\}$ und $B_i = W_i$ ($1 \leq i \leq k$, mit $c^{(i)}$ und W_i wie oben), d.h. insbesondere $\dim(a_i) = 1$, $A_i = C_i$ und $\tilde{A} = C$, dann gilt

$$F^t = W.$$

$$\text{Denn: Sei } A = \begin{pmatrix} w_{11} & w_{12} & \cdots & w_{1k} \\ w_{21} & w_{22} & \cdots & w_{2k} \\ \vdots & \vdots & & \vdots \\ w_{n1} & w_{n2} & \cdots & w_{nk} \end{pmatrix} \in M \text{ und } G = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1m} \\ c_{21} & c_{22} & \cdots & c_{2m} \\ \vdots & \vdots & & \vdots \\ c_{k1} & c_{k2} & \cdots & c_{km} \end{pmatrix}$$

(d.h. $(c_{i1}, c_{i2}, \dots, c_{im}) = c^{(i)}$ für $1 \leq i \leq k$).

Dann folgt

$$\begin{aligned} W \ni A \cdot G &= \sum_{i=1}^k \begin{pmatrix} w_{1i} \cdot c_{i1} & w_{1i} \cdot c_{i2} & \cdots & w_{1i} \cdot c_{im} \\ w_{2i} \cdot c_{i1} & w_{2i} \cdot c_{i2} & \cdots & w_{2i} \cdot c_{im} \\ \vdots & \vdots & & \vdots \\ w_{ni} \cdot c_{i1} & w_{ni} \cdot c_{i2} & \cdots & w_{ni} \cdot c_{im} \end{pmatrix} \\ &= \sum_{i=1}^k \begin{pmatrix} c_{i1}(w_{1i}, \dots, w_{ni}) \\ \vdots \\ c_{im}(w_{1i}, \dots, w_{ni}) \end{pmatrix}^t \in \bigoplus_{i=1}^k (\text{span}\{c^{(i)}\} \otimes W_i)^t = F^t. \end{aligned}$$

Also ist $W \subseteq F^t$. Die andere Inklusion kann man in analoger Weise zeigen. Es ist noch anzumerken, daß Marchukov in seiner Arbeit noch etwas allgemeiner wird und das Produkt zweier regulärer monotoner Entwicklungen betrachtet. Er kommt dabei auch bezüglich der Dimension zu vergleichbaren Parametern wie Özbudak und Stichtenoth.

- ii) S. Hirasawa, M. Kasahara, Y. Sugiyama und T. Namekawa in [6]. Sie betrachten dabei ausschließlich Codes über \mathbb{F}_2 (d.h. *binäre* Codes). Sie gehen von einem Produkt $A_2 \otimes A_1$ eines $[n_1, k_1]$ -Codes A_1 und eines $[n_2, k_2]$ -Codes A_2 aus und verallgemeinern das Produkt, indem sie A_2 durch eine Folge von Codes $A_2^{(1)}, A_2^{(2)}, \dots, A_2^{(k_1)}$ ersetzen, wobei $A_2^{(j)}$ ein $[n_2, k_2^{(j)}]$ -Code ist (für $1 \leq j \leq k_1$) und zusätzlich $k_2^{(1)} \leq k_2^{(2)} \leq \dots \leq k_2^{(k_1)}$ gilt. Die j -te Spalte eines Codewortes dieses Codes, der mit $[A_2^{(1)}, A_2^{(2)}, \dots, A_2^{(k_1)}]$ bezeichnet wird, ist jeweils aus $A_2^{(j)}$. Ferner ist A_1 so gewählt, daß A_1 Untercode $A_1 = A_1^{(k_1)} \supseteq A_1^{(k_1-1)} \supseteq \dots \supseteq A_1^{(1)}$ besitzt. Der resultierende Code $A_L := [A_2^{(1)}, A_2^{(2)}, \dots, A_2^{(k_1)}] \otimes A_1$ ist dann ein $[n_1 \cdot n_2, k_2^{(1)} + k_2^{(2)} + \dots + k_2^{(k_1)}]$ -Code. Die Autoren beschreiben anschaulich, wie das Produkt $[A_2^{(1)}, A_2^{(2)}, \dots, A_2^{(k_1)}] \otimes A_1$ zu verstehen ist und wie mit A_L codiert wird: Die zu versendende Information wird in eine „Matrix“ D eingetragen, deren j -te Spalte ($1 \leq j \leq k_1$) von der Länge $k_2^{(j)}$ ist. Diese Spalten werden nun jeweils mit $A_2^{(j)}$ codiert. Man erhält eine $n_2 \times k_1$ -Matrix, deren j -te Spalte aus $A_2^{(j)}$ ist. Als nächstes werden die Zeilen der $n_2 \times k_1$ -Matrix alle mit A_1 codiert. Als Codewort von A_L bekommt man dann eine $n_2 \times n_1$ -Matrix B . Codiert man mit $A_2^{(j)}$ (bzw. mit A_1) in der Weise, daß den Informationen in D spaltenweise (bzw. zeilenweise) nur noch Komponenten hinzugefügt werden, um Codewörter von $A_2^{(j)}$ (bzw. A_1) zu bekommen (d.h. die Matrix D bleibt erhalten und steht links

oben; siehe [1, S.5], daß dies möglich ist), so ist die j -te Spalte von B aus $A_2^{(j)}$, und die Zeilen von B sind alle aus A_1 . Das erklärt die Schreibweise $[A_2^{(1)}, A_2^{(2)}, \dots, A_2^{(k_1)}] \otimes A_1$. Ferner hat man für $A_2 = A_2^{(1)} = A_2^{(2)} = \dots = A_2^{(k_1)}$, daß A_L der bekannte Produktcode ist.

Der Zusammenhang zwischen dieser Konstruktion und der von Özbudak und Stichtenoth ist leicht zu sehen: Diese Konstruktion ist ein Spezialfall der ÖS-Konstruktion. Man wähle sich zuerst eine Basis $(a_1^{(1)}, \dots, a_1^{(k_1)})$ von A_1 derart, daß $A_1^{(i)} = \text{span}\{a_1^{(1)}, \dots, a_1^{(i)}\}$ (für $1 \leq i \leq k_1$). Wählt man dann mit den Bezeichnungen dieses Abschnitts III.1 $W_j = A_2^{(j)}$ (für $1 \leq j \leq k_1$), $C = A_1$ und $c^{(i)} = a_1^{(i)}$ (für $1 \leq i \leq k_1$), so gilt $M = [A_2^{(1)}, A_2^{(2)}, \dots, A_2^{(k_1)}]$ und

$$W = A_L.$$

- iii) E. L. Blokh und V. V. Zyablov in [7]. L. M. G. M. Tolhuizen hat sich mit dieser Konstruktion in [8] beschäftigt, welche ein Spezialfall einer Konstruktion von Zinov'ev ist (siehe [1, S.590]).

Sei G eine $k \times m$ -Matrix eines $[m, k]$ -Codes über \mathbb{F}_q . Für $i = 1, \dots, r$ sei B_i ein $(n, |B_i|, d_i)$ -Code über $\mathbb{F}_{q^{a_i}}$ (d.h. B_i kann auch ein nichtlinearer Code sein; ein (nichtlinearer) Code wird als (N,M,D)-Code bezeichnet, wobei N die Länge, M die Mächtigkeit, und D der Minimalabstand ist) und $\Psi_i : \mathbb{F}_{q^{a_i}} \rightarrow \mathbb{F}_q^{a_i}$ sei eine Bijektion. Dabei seien die a_i derart, daß $\sum_{s=1}^r a_i = k$ gelte.

Definition. Für $i = 1, \dots, r$ ist der i -te Block einer $k \times l$ -Matrix diejenige $a_i \times l$ -Untermatrix, die aus den j -ten Zeilen für $\sum_{s=1}^{i-1} a_s < j \leq \sum_{s=1}^i a_s$ besteht.

Definition. Für $i = 1, \dots, r$ sei $\mathbf{x}_i \in (\mathbb{F}_{q^{a_i}})^n$. Die $k \times n$ -Matrix $M(\mathbf{x}_1, \dots, \mathbf{x}_r)$ ist die Matrix, dessen i -ter Block mit \mathbf{x}_i wie folgt zusammenhängt: Ist $\mathbf{x}_i = (x_{i1}, \dots, x_{in})$, so ist für $j \in \{1, \dots, n\}$ die j -te Spalte des i -ten Blocks von $M(\mathbf{x}_1, \dots, \mathbf{x}_r)$ gleich $(\Psi_i(x_{ij}))^t$. Die $m \times n$ -Matrix $C(\mathbf{x}_1, \dots, \mathbf{x}_r)$ wird definiert als $C(\mathbf{x}_1, \dots, \mathbf{x}_r) := G^t \cdot M(\mathbf{x}_1, \dots, \mathbf{x}_r)$. Man beachte, daß sämtliche Spalten von $C(\mathbf{x}_1, \dots, \mathbf{x}_r)$ aus A_1 sind.

Nun betrachten wir den eigentlichen Blokh-Zyablov Code :

$$Z := \{C(\mathbf{b}_1, \dots, \mathbf{b}_r) \mid \mathbf{b}_i \in B_i, 1 \leq i \leq r\}$$

Es gilt: Länge(Z)= $n \cdot m$ und $|Z| = \prod_{i=1}^r |B_i|$. Sind ferner alle B_i lineare Codes der Dimension k_i und alle Ψ_i \mathbb{F}_q -linear, dann ist Z ein linearer Code der Dimension $\sum_{i=1}^r a_i k_i$. Für $A_i := \{\mathbf{m}G \mid \mathbf{m} \in \mathbb{F}_q^k, m_j = 0 \text{ für } 1 \leq j \leq \sum_{s=1}^{i-1} a_s\}$ (d.h. A_i wird von den letzten $r - i + 1$ Blöcken von G erzeugt) wird der Minimalabstand von A_i mit e_i bezeichnet. Dann gilt

$$d(Z) \geq \min\{d_i e_i \mid 1 \leq i \leq r\}.$$

Zusammenhang zwischen dieser Konstruktion und der von Özbudak und Stichtenoth: Wählt man $r = k$ (d.h. $a_i = 1$), $\Psi_i = \text{id}_{\mathbb{F}_q}$, $B_i = W_i$ und $A_1 = C$, so ist offensichtlich $M(\mathbf{b}_1, \dots, \mathbf{b}_r)^t \in M$ (für $\mathbf{b}_i \in B_i$) und $Z^t = W$. Man beachte, daß die Aussagen über den Minimalabstand voneinander abweichen, da $A_i \neq C_i$. Beide Aussagen sind aber sehr ähnlich und werden in fast gleicher Weise bewiesen.

Eine weitere, etwas umfangreichere Bemerkung enthält der nächste Abschnitt:

III.2 Die NX-Konstruktion als Spezialfall der Konstruktion von Özbudak und Stichtenoth

In diesem Abschnitt werden wir zeigen, daß die NX-Konstruktion tatsächlich ein Spezialfall der ÖS-Konstruktion ist. Die bei Niederreiter und Xing wählbaren Parameter h, r, s (mit $2 \leq h \leq q$, $1 \leq r < h$ und $0 \leq s \leq r$) sind dabei noch freier wählbar, so daß man mehr gute lange Codes finden kann.

Satz III.2.1 *Die Bezeichnungen seien die gleichen wie im vorherigen Abschnitt. Sei C nun ein verallgemeinerter Reed-Solomon (GRS) Code der Länge h und der Dimension $r + 1$ (wobei $2 \leq h \leq q$ und $1 \leq r < h$ ist). Wir wählen für die $C_j \subseteq C$ GRS Codes der Dimension j und mit Minimalabstand $d(C_j) = h + 1 - j$ (für $1 \leq j \leq r + 1$). Sei $W_1 = \dots = W_{s+1}$ ein $[n, k, d]$ Code, und $W_{s+2} = \dots = W_{r+1}$ der Wiederholungscode mit den Parametern $[n, 1, n]$. Dann hat der Code W nach Satz III.1.1 die Parameter*

$$\text{Länge}(W) = \text{Länge}(C) \cdot \text{Länge}(W_j) = h \cdot n,$$

$$\dim(W) = \sum_{j=1}^{r+1} \dim(W_j) = (s+1) \cdot k + (r-s),$$

$$d(W_j) \geq \min\{d(W_j) \cdot d(C_j) \mid 1 \leq j \leq k\} = \min\{d \cdot (h-s), n \cdot (h-r)\},$$

welche den Parametern der NX-Konstruktion entsprechen.

Bevor wir diesen Satz beweisen, wollen wir uns vorher kurz GRS Codes in Erinnerung rufen:

Definition III.2.2 *Sei $2 \leq k \leq n \leq q$. Sei etwa $\alpha = (\alpha_1, \dots, \alpha_n)$, wobei $\alpha_i \in \mathbb{F}_q$ paarweise verschieden, und $v = (v_1, \dots, v_n)$ mit $v_i \in \mathbb{F}_q \setminus \{0\}$. Dann heißt*

$$\text{GRS}_k(\alpha, v) := \{v_1 f(\alpha_1), \dots, v_n f(\alpha_n) \mid f(x) \in \mathbb{F}_q[x], \deg(f) < k\}$$

verallgemeinerter Reed-Solomon Code zu k, α, v .

Bemerkungen.

- i) $\text{GRS}_k(\alpha, v)$ ist ein $[n, k]$ -Code über \mathbb{F}_q . Man kann leicht sehen, daß

$$G := \begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ \alpha_1 v_1 & \alpha_2 v_2 & \cdots & \alpha_n v_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \cdots & \alpha_n^{k-1} v_n \end{pmatrix} \in \text{Mat}(k \times n)$$

eine Erzeugermatrix ist.

- ii) Da f höchstens $k - 1$ Nullstellen hat, ist der Minimalabstand d mindestens $n - k + 1$. Mit der Singleton-Schranke folgt, daß $d = n - k + 1$ ist. $\text{GRS}_k(\alpha, v)$ ist also ein MDS Code.

iii) Durch die Erzeugermatrizen

$$G_j := \begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ \alpha_1 v_1 & \alpha_2 v_2 & \cdots & \alpha_n v_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{j-1} v_1 & \alpha_2^{j-1} v_2 & \cdots & \alpha_n^{j-1} v_n \end{pmatrix} \in \text{Mat}(j \times n)$$

erhält man für $1 \leq j \leq k$ lineare Untercodes C_j von $\text{GRS}_k(\alpha, v)$. Wie man an der Form der Erzeugermatrix G_j sehen kann, ist C_j (für $2 \leq j \leq k$) gleich $\text{GRS}_j(\alpha, v)$. Ferner ist $C_1 = \text{span}\{v\}$. Da $v \in (\mathbb{F}_q \setminus \{0\})^n$, hat C_1 den Minimalabstand n . Für $1 \leq j \leq k$ hat C_j also die Parameter $[n, j, n - j + 1]$, und es gilt $C_1 \subseteq C_2 \subseteq \dots \subseteq C_k = \text{GRS}_k(\alpha, v)$.

iv) Der zu $\text{GRS}_k(\alpha, v)$ duale Code ist $\text{GRS}_{n-k}(\alpha, v')$ (für ein gewisses $v' = (v'_1, \dots, v'_n) \in \mathbb{F}_q^n$, $v'_i \neq 0$) (Beweis siehe [1, S. 304]). Man findet in der Literatur (z.B. [3, Beispiel 1.2.10]) deshalb auch die Definition der GRS Codes über deren Kontrollmatrix, d.h. für $2 \leq d \leq n \leq q$, α wie oben, und $\bar{v} = (\bar{v}_1, \dots, \bar{v}_n) \in \mathbb{F}_q^n$, $\bar{v}_i \neq 0$ setzt man

$$\bar{H} := \begin{pmatrix} \bar{v}_1 & \bar{v}_2 & \cdots & \bar{v}_n \\ \alpha_1 \bar{v}_1 & \alpha_2 \bar{v}_2 & \cdots & \alpha_n \bar{v}_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{d-2} \bar{v}_1 & \alpha_2^{d-2} \bar{v}_2 & \cdots & \alpha_n^{d-2} \bar{v}_n \end{pmatrix} \in \text{Mat}(d-1 \times n).$$

Der *Reed-Solomon Code* zu d, α, \bar{v} ist dann definiert als der Code, der \bar{H} als Kontrollmatrix hat, d.h. $\text{GRS}_d(\alpha, \bar{v}) = \{x \in \mathbb{F}_q^n \mid \bar{H} \cdot x^t = 0\}$. Man beachte, daß d hier der Minimalabstand und nicht etwa die Dimension ist. $\text{GRS}_d(\alpha, \bar{v})$ ist ein $[n, n+1-d, d]$ -Code.

Wir werden im folgenden aber die Definition III.2.2 benutzen.

Wir kommen nun zum

Beweis von Satz III.2.1. Sei $H = \{\alpha_1, \alpha_2, \dots, \alpha_h\}$ eine Teilmenge von \mathbb{F}_q mit paarweise verschiedenen α_j . Dann wählen wir für $\alpha := (\alpha_1, \alpha_2, \dots, \alpha_h)$ und $v := (1, \dots, 1) \in \mathbb{F}_q^h$

$$C = \text{GRS}_{r+1}(\alpha, v),$$

$$\text{und } G := \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_h \\ \vdots & \vdots & & \vdots \\ \alpha_1^r & \alpha_2^r & \cdots & \alpha_h^r \end{pmatrix} \in \text{Mat}((r+1) \times h)$$

als Erzeugermatrix von C . Für $2 \leq j \leq r+1$ ist dann $C_j = \text{GRS}_j(\alpha, v)$ und $C_1 = \text{span}\{(1, \dots, 1)\}$ (siehe Bemerkung iii)), insbesondere gilt $d(C_j) = h - j + 1$ für $1 \leq j \leq r+1$.

Wir betrachten nun M (d.h. die Menge aller $n \times (r+1)$ Matrizen, deren j -te Spalte $\in W_j$ für $1 \leq j \leq r+1$) und nehmen uns ein beliebiges $A \in M$ heraus. Da nach Voraussetzung $W_{s+2} = \dots = W_{r+1}$ der $[n, 1, n]$ -Wiederholungscode ist, hat A folgende Form:

$$A = \begin{pmatrix} w_{11} & \cdots & w_{1s+1} & w_{1s+2} & \cdots & w_{1r+1} \\ w_{21} & \cdots & w_{2s+1} & w_{1s+2} & \cdots & w_{1r+1} \\ \vdots & & \vdots & \vdots & & \vdots \\ w_{n1} & \cdots & w_{ns+1} & w_{1s+2} & \cdots & w_{1r+1} \end{pmatrix}.$$

Multipliziert mit G erhalten wir ein Element aus $W = \{A \cdot G \mid A \in M\}$:

$$\begin{aligned}
A \cdot G &= \begin{pmatrix} w_{11} & \cdots & w_{1s+1} & w_{1s+2} & \cdots & w_{1r+1} \\ w_{21} & \cdots & w_{2s+1} & w_{1s+2} & \cdots & w_{1r+1} \\ \vdots & & \vdots & \vdots & & \vdots \\ w_{n1} & \cdots & w_{ns+1} & w_{1s+2} & \cdots & w_{1r+1} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_h \\ \vdots & \vdots & & \vdots \\ \alpha_1^r & \alpha_2^r & \cdots & \alpha_h^r \end{pmatrix} \\
&= \begin{pmatrix} \sum_{i=1}^{r+1} w_{1i} \cdot \alpha_1^{i-1} & \cdots & \sum_{i=1}^{r+1} w_{1i} \cdot \alpha_h^{i-1} \\ \vdots & & \vdots \\ \sum_{i=1}^{r+1} w_{ni} \cdot \alpha_1^{i-1} & \cdots & \sum_{i=1}^{r+1} w_{ni} \cdot \alpha_h^{i-1} \end{pmatrix} \\
&= \sum_{i=1}^{s+1} \begin{pmatrix} w_{1i} \cdot \alpha_1^{i-1} & \cdots & w_{1i} \cdot \alpha_h^{i-1} \\ \vdots & & \vdots \\ w_{ni} \cdot \alpha_1^{i-1} & \cdots & w_{ni} \cdot \alpha_h^{i-1} \end{pmatrix} + \sum_{i=s+2}^{r+1} \begin{pmatrix} w_{1i} \cdot \alpha_1^{i-1} & \cdots & w_{1i} \cdot \alpha_h^{i-1} \\ \vdots & & \vdots \\ w_{1i} \cdot \alpha_1^{i-1} & \cdots & w_{1i} \cdot \alpha_h^{i-1} \end{pmatrix}.
\end{aligned}$$

Elemente aus W können somit in folgender Form dargestellt werden:

$$A \cdot G = \sum_{i=1}^{s+1} \begin{pmatrix} w_{1i} \cdot (\alpha_1^{i-1}, \dots, \alpha_h^{i-1}) \\ \vdots \\ w_{ni} \cdot (\alpha_1^{i-1}, \dots, \alpha_h^{i-1}) \end{pmatrix} + \sum_{i=s+2}^{r+1} w_{1i} \cdot \begin{pmatrix} \alpha_1^{i-1} & \cdots & \alpha_h^{i-1} \\ \vdots & & \vdots \\ \alpha_1^{i-1} & \cdots & \alpha_h^{i-1} \end{pmatrix}. \quad (3.1)$$

Wir werden als nächstes (unter Benutzung der Bezeichnungen aus Kapitel II) die Elemente des Codes $\psi(U)$ der NX-Konstruktion betrachten und zeigen, daß diese sich in derselben Form wie in (3.1) darstellen lassen.

Wir gehen dabei von $B := W_1 = \dots = W_{s+1}$ aus. Da dies ein $[n, k, d]$ -Code über \mathbb{F}_q ist, existieren nach Lemma II.2.2 ein Funktionenkörper F/\mathbb{F}_q , n paarweise verschiedene rationale Stellen P_1, \dots, P_n von F/\mathbb{F}_q und ein k -dimensionaler \mathbb{F}_q -linearer Unterraum V von F derart, daß $W_1 = \dots = W_{s+1} = B_V(P_1, \dots, P_n) = \{(f(P_1), \dots, f(P_n))^t \mid f \in V\}$ ist. Wir betrachten nun ein beliebiges $u = \sum_{j=0}^r v_j y^j \in U$ (wie in Kapitel II, d.h. $v_j \in V$ für $0 \leq j \leq s$, und $v_j \in \mathbb{F}_q$ für $s+1 \leq j \leq r$). Unter ψ erhalten wir

$$\psi(u) = (u(R_l^{(\alpha)}))_{1 \leq l \leq n, \alpha \in H}.$$

Dies liegt in $\mathbb{F}_q^{n \cdot h}$. Wir fassen daher $\psi(u)$ als $n \times h$ -Matrix über \mathbb{F}_q auf und schreiben

$$\psi(u) = \begin{pmatrix} u(R_1^{(\alpha_1)}) & \cdots & u(R_1^{(\alpha_h)}) \\ \vdots & & \vdots \\ u(R_n^{(\alpha_1)}) & \cdots & u(R_n^{(\alpha_h)}) \end{pmatrix} \in \text{Mat}(n \times h).$$

Unter Benutzung der Darstellung der $u(R_l^{\alpha_i})$ in (2.12) hat man dann

$$\psi(u) = \begin{pmatrix} \sum_{j=0}^r v_j(P_1) \alpha_1^j & \cdots & \sum_{j=0}^r v_j(P_1) \alpha_h^j \\ \vdots & & \vdots \\ \sum_{j=0}^r v_j(P_n) \alpha_1^j & \cdots & \sum_{j=0}^r v_j(P_n) \alpha_h^j \end{pmatrix}$$

$$\begin{aligned}
&= \sum_{j=0}^r \begin{pmatrix} v_j(P_1)\alpha_1^j & \cdots & v_j(P_1)\alpha_h^j \\ \vdots & & \vdots \\ v_j(P_n)\alpha_1^j & \cdots & v_j(P_n)\alpha_h^j \end{pmatrix} \\
&= \sum_{j=0}^s \begin{pmatrix} v_j(P_1)\alpha_1^j & \cdots & v_j(P_1)\alpha_h^j \\ \vdots & & \vdots \\ v_j(P_n)\alpha_1^j & \cdots & v_j(P_n)\alpha_h^j \end{pmatrix} + \sum_{j=s+1}^r \begin{pmatrix} v_j(P_1)\alpha_1^j & \cdots & v_j(P_1)\alpha_h^j \\ \vdots & & \vdots \\ v_j(P_n)\alpha_1^j & \cdots & v_j(P_n)\alpha_h^j \end{pmatrix}. \\
&= \sum_{j=1}^{s+1} \begin{pmatrix} v_{j-1}(P_1)(\alpha_1^{j-1}, \dots, \alpha_h^{j-1}) \\ \vdots \\ v_{j-1}(P_n)(\alpha_1^{j-1}, \dots, \alpha_h^{j-1}) \end{pmatrix} + \sum_{j=s+2}^{r+1} \begin{pmatrix} v_{j-1}(P_1)(\alpha_1^{j-1}, \dots, \alpha_h^{j-1}) \\ \vdots \\ v_{j-1}(P_n)(\alpha_1^{j-1}, \dots, \alpha_h^{j-1}) \end{pmatrix}.
\end{aligned}$$

- Für $1 \leq j \leq s+1$ ist $\begin{pmatrix} v_{j-1}(P_1) \\ \vdots \\ v_{j-1}(P_n) \end{pmatrix}$ ein Element aus $B_V(P_1, \dots, P_n) = W_j$.
- Für $s+2 \leq j \leq r+1$ und $1 \leq l \leq n$ ist $v_{j-1}(P_l) = v_{j-1}$, da in diesem Fall $v_{j-1} \in \mathbb{F}_q$. Daher gilt, daß $\begin{pmatrix} v_{j-1}(P_1) \\ \vdots \\ v_{j-1}(P_n) \end{pmatrix} = \begin{pmatrix} v_{j-1} \\ \vdots \\ v_{j-1} \end{pmatrix}$ ein Codewort des $[n, 1, n]$ -Wiederholungscodes W_j ist.

Insgesamt haben wir

$$\psi(u) = \sum_{j=1}^{s+1} \begin{pmatrix} v_{j-1}(P_1)(\alpha_1^{j-1}, \dots, \alpha_h^{j-1}) \\ \vdots \\ v_{j-1}(P_n)(\alpha_1^{j-1}, \dots, \alpha_h^{j-1}) \end{pmatrix} + \sum_{j=s+2}^{r+1} v_{j-1} \begin{pmatrix} \alpha_1^{j-1} & \cdots & \alpha_h^{j-1} \\ \vdots & & \vdots \\ \alpha_1^{j-1} & \cdots & \alpha_h^{j-1} \end{pmatrix},$$

was genau der Form aus (3.1) entspricht. □

Korollar III.2.3 *In der Situation von Satz III.2.1 sei $s = 0$. Dann hat W die Parameter*

$$\text{Länge}(W) = hn, \quad \dim(W) = k + r, \quad d(W) = \min\{dh, (h-r)n\}.$$

Beweis. Wir müssen nur noch die Gleichheit für den Minimalabstand zeigen. Dazu geben wir jeweils ein Element an, das vom Gewicht dh bzw. $(h-r)n$ ist:

Als erstes wählen wir ein Element $w_1 = (w_{11}, w_{21}, \dots, w_{n1})^t$ aus W_1 vom Gewicht d . Wir setzen

$$A = \begin{pmatrix} w_{11} & 0 & \cdots & 0 \\ w_{21} & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ w_{n1} & 0 & \cdots & 0 \end{pmatrix} \in M \subseteq \text{Mat}(n \times r + 1).$$

Dann folgt

$$A \cdot G = \begin{pmatrix} w_{11} & \cdots & w_{11} \\ \vdots & & \vdots \\ w_{n1} & \cdots & w_{n1} \end{pmatrix} \in \text{Mat}(n \times h).$$

Diese Matrix hat h Spalten vom Gewicht d . Damit gilt $wt(A \cdot G) = dh$.

Als nächstes wählen wir r verschiedene $\alpha_{i_1}, \dots, \alpha_{i_r} \in \{\alpha_1, \dots, \alpha_h\}$, wobei o.E. $\alpha_{i_1} = 0$. Wir betrachten nun für $i = 1, \dots, h$

$$\prod_{j=1}^r (\alpha_i - \alpha_{i_j}) = \sum_{j=0}^r \gamma_j \alpha_i^j, \quad (\gamma_j \in \mathbb{F}_q).$$

Wir wählen

$$A = \begin{pmatrix} \gamma_0 & \gamma_1 & \cdots & \gamma_r \\ \vdots & \vdots & & \vdots \\ \gamma_0 & \gamma_1 & \cdots & \gamma_r \end{pmatrix} \in \text{Mat}(n \times r + 1).$$

Man beachte dabei, daß $\gamma_0 = 0$ (wegen $\alpha_{i_1} = 0$), und somit die erste Spalte von A als Nullvektor ein Element aus W_1 ist. Es folgt

$$\begin{aligned} A \cdot G &= \begin{pmatrix} \sum_{j=0}^r \gamma_j \alpha_1^j & \cdots & \sum_{j=0}^r \gamma_j \alpha_h^j \\ \vdots & & \vdots \\ \sum_{j=0}^r \gamma_j \alpha_1^j & \cdots & \sum_{j=0}^r \gamma_j \alpha_h^j \end{pmatrix} \\ &= \begin{pmatrix} \prod_{j=1}^r (\alpha_1 - \alpha_{i_j}) & \cdots & \prod_{j=1}^r (\alpha_h - \alpha_{i_j}) \\ \vdots & & \vdots \\ \prod_{j=1}^r (\alpha_1 - \alpha_{i_j}) & \cdots & \prod_{j=1}^r (\alpha_h - \alpha_{i_j}) \end{pmatrix} \in \text{Mat}(n \times h). \end{aligned}$$

Da $\prod_{j=1}^r (\alpha_i - \alpha_{i_j})$ genau dann Null ist, wenn $\alpha_i = \alpha_{i_j}$ ist, hat $A \cdot G$ genau r Nullspalten und $h - r$ Spalten vom Gewicht n . Somit gilt $wt(A \cdot G) = (h - r)n$. □

III.3 Numerische Resultate

Es folgen hier einige Beispiele der durch die ÖS-Konstruktion (bzw. durch die NX-Konstruktion) erhältlichen Codes. Man kann mit diesen viele *optimale* Codes (d.h. zu gegebenen q, n, k existiert kein Code mit größerem Minimalabstand) konstruieren (vgl. [9], [4]).

Beispiel 1. $q = 2$, C sei $[2, 2, 1]$ -Code (d.h. $C = \mathbb{F}_2^2$), und C_1 sei $[2, 1, 2]$ -Code. Man beachte, daß $C_1 \subseteq C$ existiert. Denn wählt man z.B. für C einen GRS Code, so bekommt man sofort einen Untercode C_1 mit den Parametern $[2, 1, 2]$ (nämlich $C_1 = \text{span}\{(1, 1)\}$; siehe III.2.2 Bemerkung iii)). W_1, W_2 seien Codes mit Parametern den $[20, 19, 2]$ bzw. $[20, 14, 4]$. Der MDS-Code W_1 ist der duale Code zu dem $[20, 1, 20]$ -Code W_1^\perp (dabei ist $W_1^\perp = \text{span}\{(1, \dots, 1)^t\}$). Um einen Code mit den Parametern von W_2 zu erhalten,

betrachten wir zuerst den $[16, 15, 2]$ -Code A_1 (d.h. $A_1^\perp = \text{span}\{(1, \dots, 1)^t\} \subseteq \mathbb{F}_2^{16}$) und den $[16, 11, 4]$ -Code A_2 , welcher der erweiterte Code des binären Hamming-Codes mit den Parametern $[15, 11, 3]$ sei. Wendet man die *Plotkin-Konstruktion* (siehe [3, 1.2.12]; auch als *u | u + v-Konstruktion* bezeichnet) an, so bekommt man einen Code $A := A_1 \times A_2 = \{(a_1, a_1 + a_2) \mid a_1 \in A_1, a_2 \in A_2\}$ mit den Parametern $[32, 26, 4]$. Durch Verkürzen von A erhält man schließlich einen $[20, 14, 4]$ -Code W_2 .

Der Code W hat somit die Parameter

$$\text{Länge}(W) = 2 \cdot 20 = 40,$$

$$\dim(W) = 19 + 14 = 33,$$

$$d(W) \geq 4.$$

Mit Korollar III.1.2 hat man zudem $d(W) = 4$, denn $wt(c^{(1)}) = 2 = d(C_1)$ und $wt(c^{(2)}) = 1 = d(C)$ (man beachte, daß $c^{(2)} = (\alpha_1, \alpha_2) \in \mathbb{F}_2^2$, wobei $\alpha_1 \neq \alpha_2$). W hat somit die Parameter $[40, 33, 4]$ und ist nach [9] optimal.

Beispiel 2. $q = 3$. Wir benutzen in diesem Beispiel Korollar III.2.3. Sei W_1 ein $[9, 3, 6]$ -Code. Solch einen Code erhält man z.B. durch Verkürzen des erweiterten ternären Golay Code \mathcal{G}_{12} , der die Parameter $[12, 6, 6]$ hat (siehe [1, Seite 490]). Desweiteren sei $h = 3$ und $r = 1$ (d.h. C hat die Parameter $[3, 2, 2]$). Mit Korollar III.2.3 folgt, daß W folgende Parameter besitzt:

$$\text{Länge}(W) = 3 \cdot 9 = 27,$$

$$\dim(W) = 3 + 1 = 4,$$

$$d(W) = \min\{6 \cdot 3, 2 \cdot 9\} = 18.$$

Nach [9] ist W optimal.

Beispiel 3. $q = 5$, C sei $[3, 3, 1]$ -Code (also $C = \mathbb{F}_5^3$), $d(C_1) = 3$, $d(C_2) = 2$, $d(C_3) = 1$, und W_1, W_2, W_3 seien Codes mit den Parametern $[12, 12, 1]$, bzw. $[12, 11, 2]$, bzw. $[12, 9, 3]$. D.h. $W_1 = \mathbb{F}_5^{12}$ und $W_2^\perp = \text{span}\{(1, \dots, 1)^t\} \subseteq \mathbb{F}_5^{12}$. Einen $[12, 9, 3]$ -Code W_3 erhält man durch Verkürzen des Hamming-Codes mit den Parametern $[31, 28, 3]$. Wählt man $C = GRS_3(\alpha, v)$, erhält man sofort Untercode C_1, C_2, C_3 mit den angegebenen Minimalabständen (siehe III.2.2 Bemerkung iii)). Der resultierende Code W hat dann die Parameter $[36, 32, \geq 3]$. Da nach [9] aber kein Code dieser Länge und Dimension mit Minimalabstand > 3 existiert, muß W ein $[36, 32, 3]$ -Code sein und ist optimal.

Anhang A

Sei $q \in \mathbb{N}$ beliebig. Wir werden in diesem Anhang zeigen, daß ein Funktionenkörper F/\mathbb{F}_q mit beliebig großer Anzahl rationaler Stellen existiert. Insbesondere existiert ein Funktionenkörper mit n rationalen Stellen, wie wir es für den Beweis des Lemma II.1.2 benötigt haben. Wir geben dazu einfach ein Beispiel eines solchen Funktionenkörpers an. Anschließend bestimmen wir zur Abrundung sein Geschlecht. Denn wie wir schon am Ende des ersten Kapitels angedeutet haben, ist es für die Anwendung algebraischer Funktionenkörper auf die Codierungstheorie von großem Interesse, das Geschlecht und die Anzahl der rationalen Stellen zu kennen.

A.1 Beispiel eines Funktionenkörpers F_n/\mathbb{F}_q mit beliebig vielen rationalen Stellen

Wir betrachten die Konstruktion

$$\begin{array}{c} F_n := F_{n-1}(x_n) \\ | \\ \vdots \\ | \\ F_2 := F_1(x_2) \\ | \\ F_1 := \mathbb{F}_q(x_1) \\ | \\ \mathbb{F}_q \end{array}$$

definiert durch

$$x_{i+1}^q - x_{i+1} - (x_i^{q+1} - x_i^2) = 0 \quad \text{für } i = 1, \dots, n-1, \quad (\text{a.1})$$

wobei x_1 ein beliebiges über \mathbb{F}_q transzendentes Element ist.

Um einen Funktionenkörpern mit beliebig vielen rationalen Stellen zu erhalten, müssen wir nur den Turm entsprechend hoch bauen, denn es gilt

Satz A.1.1 *Seien die Bezeichnungen wie oben. Dann besitzt der Funktionenkörper F_n/\mathbb{F}_q genau $q^n + 1$ rationale Stellen.*

Beweis. Im ersten Schritt des Beweises zeigen wir zuerst

$$[F_{i+1} : F_i] = q \quad \text{für } i=1, \dots, n-1 \quad (\text{a.2})$$

(d.h. die Polynome

$$\varphi_i(T) := T^q - T - (x_i^{q+1} - x_i^2) \in F_i[T] \quad , \quad (i=1, \dots, n-1) \quad (\text{a.3})$$

sind irreduzibel in F_i). Außerdem betrachten wir die rationale Stelle $P^{(1)} := P_\infty \in \mathbb{P}_{F_1}$ und Fortsetzungen davon auf F_i . Diese Fortsetzungen von P_∞ bezeichnen wir jeweils mit $P^{(i)} \in \mathbb{P}_{F_i}$. Gleichzeitig mit Behauptung (a.2) zeigen wir im ersten Schritt zudem, daß

$$P^{(i+1)} \mid P^{(i)} \text{ voll verzweigt} \quad (\text{a.4})$$

ist und

$$v_{P^{(i+1)}}(x_{i+1}) = -(q+1)^i \quad \text{für } i=1, \dots, n-1. \quad (\text{a.5})$$

Dies beweisen wir induktiv.

$j=1$: Es gilt

$$\begin{aligned} v_{P^{(2)}}(x_2^q - x_2) &\stackrel{(\text{a.1})}{=} v_{P^{(2)}}(x_1^{q+1} - x_1^2) \\ &= e(P^{(2)} \mid P_\infty) \cdot v_{P_\infty}(x_1^{q+1} - x_1^2) \\ &= e(P^{(2)} \mid P_\infty) \cdot (-(q+1)) < 0. \end{aligned} \quad (\text{a.6})$$

Andererseits hat man mit der scharfen Dreiecksungleichung

$$v_{P^{(2)}}(x_2^q - x_2) = \min\{q \cdot v_{P^{(2)}}(x_2), v_{P^{(2)}}(x_2)\}.$$

Da nach (a.6) $v_{P^{(2)}}(x_2^q - x_2) < 0$, ist auch $v_{P^{(2)}}(x_2) < 0$. Also ist $q \cdot v_{P^{(2)}}(x_2)$ das Minimum. Es gilt damit

$$v_{P^{(2)}}(x_2^q - x_2) = q \cdot v_{P^{(2)}}(x_2) = e(P^{(2)} \mid P_\infty) \cdot (-(q+1)). \quad (\text{a.7})$$

Betrachtet man die letzte Gleichung, so weiß man, da q und $(q+1)$ teilerfremd sind, daß q ein Teiler von $e(P^{(2)} \mid P_\infty)$ sein muß. Insbesondere gilt somit $q \leq e(P^{(2)} \mid P_\infty)$.

Nun wissen wir, daß mit der Summenformel aus Satz I.2.16 $\sum e_i f_i = [F_2 : F_1]$ ist. Da nun $[F_2 : F_1] \leq \deg(\varphi_1(T)) = q$ und $e(P^{(2)} \mid P_\infty)$ eines der e_i ist, gilt $e(P^{(2)} \mid P_\infty) \leq [F_2 : F_1] \leq q$.

Es folgt $q \leq e(P^{(2)} \mid P_\infty) \leq [F_2 : F_1] \leq q$, und wir haben schließlich

$$[F_2 : F_1] = q$$

und

$$e(P^{(2)} \mid P_\infty) = q. \quad (\text{a.8})$$

Setzt man (a.8) in (a.7) ein, so bekommt man

$$v_{P^{(2)}}(x_2) = -(q+1).$$

$j \rightarrow j+1, 1 \leq j \leq n-1$: Analog zu oben gilt

$$v_{P^{(j+1)}}(x_{j+1}^q - x_{j+1}) = v_{P^{(j+1)}}(x_j^{q+1} - x_j^2)$$

$$\begin{aligned}
&= e(P^{(j+1)} | P^{(j)}) \cdot v_{P^{(j)}}(x_j^{q+1} - x_j^2) \\
&\stackrel{I.V.}{=} e(P^{(j+1)} | P^{(j)}) \cdot (q+1)(-(q+1)^{j-1}) < 0.
\end{aligned}$$

Mit der scharfen Dreiecksungleichung gilt

$$v_{P^{(j+1)}}(x_{j+1}^q - x_{j+1}) = \min\{q \cdot v_{P^{(j+1)}}(x_{j+1}), v_{P^{(j+1)}}(x_{j+1})\}.$$

Wie oben hat man wegen des Vorzeichens

$$v_{P^{(j+1)}}(x_{j+1}^q - x_{j+1}) = q \cdot v_{P^{(j+1)}}(x_{j+1}) = e(P^{(j+1)} | P^{(j)}) \cdot (-(q+1)^j). \quad (\text{a.9})$$

Betrachtet man die letzte Gleichung, so weiß man, da $\text{ggT}(q, (q+1)^j) = 1$, daß q ein Teiler von $e(P^{(j+1)} | P^{(j)})$ sein muß. Insbesondere gilt somit $q \leq e(P^{(j+1)} | P^{(j)})$.

Über die Summenformel aus Satz I.2.16 erhalten wir wie oben $e(P^{(j+1)} | P^{(j)}) \leq [F_{j+1} : F_j] \leq q$.

Es folgt $q \leq e(P^{(j+1)} | P^{(j)}) \leq [F_{j+1} : F_j] \leq q$. Wir haben schließlich

$$[F_{j+1} : F_j] = q$$

und

$$e(P^{(j+1)} | P^{(j)}) = q. \quad (\text{a.10})$$

Setzt man (a.10) in (a.9) ein, so bekommt man

$$v_{P^{(j+1)}}(x_{j+1}) = -(q+1)^j.$$

Damit haben wir den ersten Schritt bewiesen. Man beachte, daß insbesondere $P^{(i+1)} \in \mathbb{P}_{F_{i+1}}$ (für $i = 0, \dots, n-1$) eine rationale Stelle ist, denn wegen der Summenformel $\sum e_i f_i = [F_{i+1} : F_i] = q$ und wegen $e(P^{(i+1)} | P^{(i)}) = q$ folgt $f(P^{(i+1)} | P^{(i)}) = 1$. Damit gilt $O_{P^{(i+1)}}/P^{(i+1)} = O_{P^{(i)}}/P^{(i)} = \dots = O_{P_\infty}/P_\infty = \mathbb{F}_q$.

Im zweiten Schritt werden wir zeigen, daß bis auf $P^{(i)}$ alle rationalen Stellen von F_i voll zerlegt sind in F_{i+1} und daß deren Fortsetzungen ebenfalls rational sind. Wir wissen bereits, daß F_1 neben P_∞ noch genau q weitere rationale Stellen besitzt. Sind diese q Stellen voll zerlegt in F_2 und die Fortsetzungen rational, dann besitzt F_2 mindestens $q^2 + 1$ rationale Stellen. Dies sind bereits alle rationalen Stellen von F_2 , denn ist $P' \in \mathbb{P}_{F_2}$ eine beliebige rationale Stelle, dann existiert eine Stelle $P \in \mathbb{P}_{F_1}$ derart, daß $P' | P$ (nämlich $P = P' \cap F_1$). Es gilt $\mathbb{F}_q \subseteq O_P/P \subseteq O_{P'}/P' = \mathbb{F}_q$. Also ist P' Fortsetzung einer rationalen Stelle von F_1 , und P' wurde bereits mitgezählt. Verfährt man so weiter, erhält man für F_3 genau $q^3 + 1$ rationale Stellen, und schließlich für F_n genau $q^n + 1$ rationale Stellen.

Wir beweisen den zweiten Schritt ebenfalls induktiv:

$j = 1$: Wir betrachten für ein beliebiges $\alpha \in \mathbb{F}_q$ die Stelle $P_\alpha := P_{x_1 - \alpha}$ und das Polynom

$$\varphi_1(T) = T^q - T - (x_1^{q+1} - x_1^2) \in F_1[T].$$

Es gilt dann

$$v_{P_\alpha}(x_1^{q+1} - x_1^2) = v_{P_\alpha}(x_1) \cdot \prod_{\beta \in \mathbb{F}_q} (x_1 - \beta)$$

$$= v_{P_\alpha}(x_1) + \sum_{\beta \in \mathbb{F}_q} v_{P_\alpha}(x_1 - \beta) = \left\{ \begin{array}{ll} 0 + 1 & \text{für } \alpha \neq 0 \\ 1 + 1 & \text{für } \alpha = 0 \end{array} \right\} > 0.$$

Insbesondere ist $(x_1^{q+1} - x_1^2) \in P_\alpha$, und damit $\varphi_1(T) \in O_{P_\alpha}[T]$.

Betrachten wir nun $\varphi_1(T)$ als Polynom in $\overline{F}_\alpha := O_{P_\alpha}/P_\alpha$, so erhalten wir

$$\overline{\varphi}_1(T) = T^q - T = \prod_{\beta \in \mathbb{F}_q} (T - \beta) \in \overline{F}_\alpha[T].$$

Nach dem Satz von Kummer (siehe Satz II.2.2 in Kapitel II) folgt: Für jedes $\gamma \in \mathbb{F}_q$ existiert genau eine Stelle $R_\alpha^{(\gamma)}$ von F_2 mit $R_\alpha^{(\gamma)} \mid P_\alpha$ und $(x_2 - \gamma) \in R_\alpha^{(\gamma)}$. Zusätzlich gilt $f(R_\alpha^{(\gamma)} \mid P_\alpha) = 1$ (d.h. $R_\alpha^{(\gamma)}$ ist rational). Jedes der q verschiedenen P_α hat also genau q rationale Fortsetzungen $R_\alpha^{(\gamma)}$, für die $(x_2 - \gamma) \in R_\alpha^{(\gamma)}$ gilt. Das sind zusammen q^2 rationale Stellen von F_2 . Mit $P^{(2)}$ sind es insgesamt $q^2 + 1$ rationale Stellen.

$j \rightarrow j + 1, 1 \leq j \leq n - 1$: Wir betrachten $P \in \mathbb{F}_{F_j}, P \neq P^{(j)}$ eine rationale Stelle von F_j (davon gibt es nach I.V. q^j verschiedene) und

$$\varphi_j(T) = T^q - T - (x_j^{q+1} - x_j^2) \in F_j[T].$$

Dann gilt

$$\begin{aligned} v_P(x_j^{q+1} - x_j^2) &= v_P(x_j \cdot \prod_{\beta \in \mathbb{F}_q} (x_j - \beta)) \\ &= v_P(x_j) + \sum_{\beta \in \mathbb{F}_q} v_P(x_j - \beta). \end{aligned} \quad (\text{a.11})$$

Nach Induktionsvoraussetzung existiert ein $\beta' \in \mathbb{F}_q$ derart, daß $(x_j - \beta') \in P$ (d.h. $v_P(x_j - \beta') > 0$). Über die Dreiecksungleichung

$$\underbrace{v_P(x_j - \beta')}_{>0} \geq \min\{v_P(x_j), \underbrace{v_P(\beta')}_{\geq 0}\}$$

folgt somit wegen des Vorzeichens, daß $v_P(x_j) \geq 0$ ist. Für $\beta' \neq \beta \in \mathbb{F}_q$ gilt daher

$$v_P(x_j - \beta) \geq \min\{\underbrace{v_P(x_j)}_{\geq 0}, \underbrace{v_P(\beta)}_{\geq 0}\} \geq 0.$$

Damit sind in (a.11) alle Summanden ≥ 0 und mindestens ein Summand > 0 . Wir haben somit $v_P(x_j^{q+1} - x_j^2) > 0$. Betrachten wir nun $\varphi_j(T)$ als Polynom in $\overline{F} := O_P/P$, so erhalten wir

$$\overline{\varphi}_j(T) = T^q - T = \prod_{\beta \in \mathbb{F}_q} (T - \beta) \in \overline{F}[T].$$

Mit dem Satz von Kummer folgt: Für jedes $\gamma \in \mathbb{F}_q$ existiert genau eine Stelle $R^{(\gamma)}$ von F_{j+1} mit $R^{(\gamma)} \mid P$ und $(x_{j+1} - \gamma) \in R^{(\gamma)}$. Zusätzlich gilt $f(R^{(\gamma)} \mid P) = 1$ (d.h. $R^{(\gamma)}$ ist rational). Das sind zusammen q^{j+1} rationale Stellen von F_{j+1} . Mit $P^{(j+1)}$ sind es insgesamt $q^{j+1} + 1$ rationale Stellen. □

A.2 Das Geschlecht von F_n/\mathbb{F}_q

Wir benutzen wieder die Bezeichnungen aus dem letzten Abschnitt und bestimmen hier das Geschlecht von F_n ($n \geq 2$; das Geschlecht von F_1 ist bekanntermaßen Null).

Satz A.2.1 F_n/\mathbb{F}_q ($n \geq 2$) hat das Geschlecht

$$g(F_n) = \frac{q-1}{2} \cdot \sum_{k=1}^{n-1} [(q+1)^k - 1] \cdot q^{n-1-k}.$$

Den Beweis werden wir hauptsächlich mittels [2, III.7.10. Proposition] führen. Deshalb geben wir diesen Satz, der eine Verallgemeinerung des Satzes über Artin-Schreier-Erweiterungen ist, hier zuerst an (ohne Beweis):

Satz A.2.2 Sei F/K ein algebraischer Funktionenkörper mit Konstantenkörper K der Charakteristik $\text{char}(K) = p$, und $a(T) \in K[T]$ ein additiv separables Polynom vom Grad p^n , dessen Nullstellen alle in K liegen. Sei $u \in F$. Existiert für jedes $P \in \mathbb{P}_F$ ein $z \in F$ (abhängig von P) derart, daß

$$v_P(u - a(z)) \geq 0 \quad (\text{a.12})$$

oder

$$v_P(u - a(z)) = -m \quad \text{mit } m > 0 \text{ und } m \not\equiv 0 \pmod{p}, \quad (\text{a.13})$$

dann definiert man $m_P := -1$ für den Fall (a.12) und $m_P := m$ für den Fall (a.13). m_P ist wohldefiniert. Sei $F' = F(y)$ eine Körpererweiterung von F , wobei y die Gleichung

$$a(y) = 0$$

erfüllt. Falls mindestens eine Stelle $Q \in \mathbb{P}_F$ mit $m_Q > 0$ existiert, dann gilt:

- (i) F'/F ist galoisch, $[F' : F] = p^n$, und die Galoisgruppe von F'/F ist isomorph zu der additiven Gruppe $\{\alpha \in K \mid a(\alpha) = 0\}$ und somit isomorph zu $(\mathbb{Z}/p\mathbb{Z})^n$.
- (ii) K ist algebraisch abgeschlossen in F' .
- (iii) Jedes $P \in \mathbb{P}_F$ mit $m_P = -1$ ist unverzweigt in F'/F .
- (iv) Jedes $P \in \mathbb{P}_F$ mit $m_P > 0$ ist voll verzweigt in F'/F , und der Differentenexponent $d(P' \mid P)$ (Def. siehe [2, S.82]) der Fortsetzung P' von P in F' ist

$$d(P' \mid P) = (p^n - 1)(m_P + 1).$$

- (v) Sei g' (bzw. g) das Geschlecht von F' (bzw. F). Dann gilt

$$g' = p^n \cdot g + \frac{p^n - 1}{2} \left(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1) \cdot \text{deg} P \right). \quad (\text{a.14})$$

Bemerkungen.

- Für $1 \leq j \leq n$ gilt für eine Stelle $P \in \mathbb{P}_{F_j}$, $P \neq P^{(j)}$:

$$v_P(x_j^{q+1} - x_j^2) \geq 0.$$

Denn: $j = 1$: Sei $P \in \mathbb{P}_{F_1}$, $P \neq P_\infty$. $x_1^{q+1} - x_1^2$ ist ein Polynom in $\mathbb{F}_q[x_1] \subseteq O_P$. Daraus folgt sofort

$$v_P(x_1^{q+1} - x_1^2) \geq 0.$$

$j \rightarrow j+1$, $1 \leq j \leq n-1$: Sei nun $P' \in \mathbb{P}_{F_j}$, $P' \neq P^{(j)}$ Fortsetzung einer Stelle $P \in \mathbb{P}_{F_{j-1}}$ in F_j . Dann gilt einerseits

$$\begin{aligned} v_{P'}(x_j^{q+1} - x_j^2) &= v_{P'}(x_j \cdot \underbrace{(x_j^q - x_j)}_{(x_{j-1}^{q+1} - x_{j-1}^2)}) \\ &= v_{P'}(x_j) + v_{P'}(x_{j-1}^{q+1} - x_{j-1}^2) \\ &= v_{P'}(x_j) + e(P' | P) \cdot v_P(x_{j-1}^{q+1} - x_{j-1}^2). \end{aligned}$$

Nach Induktionsvoraussetzung ist $v_P(x_{j-1}^{q+1} - x_{j-1}^2) \geq 0$, und da der Verzweigungsgrad stets > 0 ist, gilt $\alpha := e(P' | P) \cdot v_P(x_{j-1}^{q+1} - x_{j-1}^2) \geq 0$.

Andererseits gilt mit der scharfen Dreiecksungleichung (o.E. $v_{P'}(x_j) \neq 0$; sonst sind wir hier bereits fertig)

$$v_{P'}(x_j^{q+1} - x_j^2) = \min\{(q+1) \cdot v_{P'}(x_j), 2 \cdot v_{P'}(x_j)\}.$$

Angenommen, es gelte $v_{P'}(x_j) < 0$. Dann folgt

$$v_{P'}(x_j^{q+1} - x_j^2) = v_{P'}(x_j) + \alpha = (q+1) \cdot v_{P'}(x_j).$$

Somit ist

$$\alpha = q \cdot v_{P'}(x_j) < 0.$$

Dies wäre aber ein Widerspruch zu $\alpha \geq 0$. Also gilt $v_{P'}(x_j) \geq 0$, und somit auch

$$v_{P'}(x_j^{q+1} - x_j^2) \geq 0.$$

- Für $P^{(j)} \in \mathbb{P}_{F_j}$ (d.h. für die Fortsetzung von P_∞ in F_j) wissen wir aus dem letzten Abschnitt (siehe (a.5))

$$v_{P^{(j)}}(x_j^{q+1} - x_j^2) = (q+1) \underbrace{v_{P^{(j)}}(x_j)}_{=-(q+1)^{j-1}} = -(q+1)^j.$$

Man beachte dabei, daß $(q+1)^j > 0$ und $\text{ggT}((q+1)^j, p) = 1$ (insbes. $(q+1)^j \not\equiv 0 \pmod{p}$).

Für $p^n = q$, $K = \mathbb{F}_q$, F_i/\mathbb{F}_q ($i = 1, \dots, n-1$), $a(T) := T^q - T = \prod_{\beta \in \mathbb{F}_q} (T - \beta) \in \mathbb{F}_q[T]$ und $u = x_i^{q+1} - x_i^2$ sind damit die Voraussetzungen von Satz A.2.2 erfüllt. Für jede Stelle $P \in \mathbb{P}_{F_i}$ gilt mit $z = 0$ entweder (a.12) oder (a.13). Man bekommt

$$m_P = -1 \quad \text{für } P \neq P^{(i)}$$

und

$$m_{P^{(i)}} = (q+1)^i > 0. \quad (\text{a.15})$$

Wir kommen schließlich zum *Beweis von Satz A.2.1*. Wir gehen dabei wieder induktiv vor. $j = 2$: Aus der Bemerkung von oben wissen wir, daß $P = P_\infty$ die einzige Stelle aus \mathbb{P}_{F_1} ist, für die $m_P + 1 \neq 0$. Da bekanntlich $g(F_1) = 0$, folgt nun mit den Formeln (a.14) und (a.15)

$$g(F_2) = 0 + \frac{q-1}{2}(-2 + (q+1) + 1) = \frac{q-1}{2} \cdot q.$$

Auf der anderen Seite ist

$$\frac{q-1}{2} \cdot \sum_{k=1}^{2-1} [(q+1)^k - 1] \cdot q^{2-1-k} = \frac{q-1}{2} \cdot ([(q+1)^1 - 1] \cdot q^0) = \frac{q-1}{2} \cdot q.$$

$j \rightarrow j+1$, $2 \leq j \leq n-1$: Für alle Stellen $P' \in \mathbb{P}_{F_j}$, $P' \neq P^{(j)}$ ist $m_{P'} = -1$. $P = P^{(j)}$ ist damit die einzige Stelle von F_j , für welche $m_P + 1 \neq 0$ ist. Mit den Formeln (a.14), (a.15) und der Induktionsvoraussetzung gilt

$$\begin{aligned} g(F_{j+1}) &\stackrel{(\text{a.14})}{=} q \cdot g(F_j) + \frac{q-1}{2} \left(-2 + \sum_{P \in \mathbb{P}_{F_j}} (m_P + 1) \cdot \deg P \right) \\ &\stackrel{IV, (\text{a.15})}{=} q \cdot \frac{q-1}{2} \cdot \sum_{k=1}^{j-1} [(q+1)^k - 1] \cdot q^{j-1-k} + \frac{q-1}{2} (-2 + (q+1)^j + 1) \\ &= \frac{q-1}{2} \cdot \left(\sum_{k=1}^{j-1} [(q+1)^k - 1] \cdot q^{j-k} + ((q+1)^j - 1) \right) \\ &= \frac{q-1}{2} \cdot \sum_{k=1}^j [(q+1)^k - 1] \cdot q^{j-k}. \end{aligned}$$

□

Anhang B

Das *Hutproblem* und Hamming-Codes

In diesem Abschnitt behandeln wir das *Hutproblem*, über welches auch die Wochenzeitung *Die Zeit* im Mai 2001 ([11]) berichtete. Es geht dabei um ein Spiel, bei dem n Leute jeweils entweder einen roten oder einen blauen Hut auf dem Kopf tragen und versuchen müssen, die Farbe des Hutes auf ihrem eigenen Kopf richtig zu tippen. Dabei wird vorher die Hutfarbe für jeden Spieler einzeln ausgelost (mit einer Wahrscheinlichkeit von jeweils $\frac{1}{2}$). Jeder Spieler kennt nur die Farben der anderen, darf sich aber nicht mit ihnen absprechen. Alle n Spieler geben gleichzeitig entweder einen Tip ab oder passen, und das Spiel ist gewonnen, wenn mindestens ein Spieler richtig, und keiner falsch getippt hat. Das Problem lautet: Auf welche Strategie sollen sich die Spieler vor dem Auslosen der Farben einigen, um ihre Gewinnchancen zu maximieren?

Wir betrachten hier den Spezialfall $n = 2^r - 1$ ($r \in \mathbb{N}$) und zeigen, daß man mit Hilfe der Hamming-Codes eine erstaunliche Gewinnwahrscheinlichkeit erreichen kann, die sehr viel größer ist als die auf den ersten Blick vermutete Gewinnchance von $\frac{1}{2}$.

B.1 Für drei Spieler

Im Fall $n = 3$ kann man - auch ohne Hamming-Codes - leicht eine gute Strategie durch bloßes Abzählen entwickeln. Betrachtet man alle acht möglichen Hutverteilungen, so sieht man, daß in 6 der 8 Fälle die Verteilung zwei zu eins ist (d.h. zwei Spieler haben Hüte derselben Farbe auf, während der dritte einen Hut der anderen Farbe auf dem Kopf trägt). Einigen sich die Spieler vorher darauf, zu passen, wenn sie zwei verschiedene Farben auf den Köpfen ihrer Mitspieler sehen, und auf rot zu tippen, wenn die Mitspieler beide blaue Hüte tragen (bzw. auf blau zu tippen, wenn die Mitspieler rote Hüte tragen), dann haben sie eine Gewinnchance von $\frac{6}{8} = \frac{3}{4}$. Die Spieler tippen nur dann falsch, wenn alle Spieler Hüte derselben Farbe tragen. In diesem Fall geben alle Spieler einen falschen Tip ab.

B.2 Für $n = 2^r - 1$ Spieler

Im Fall $n = 2^r - 1$ ($r \in \mathbb{N}$, $r \geq 3$) ist das Problem nicht mehr ohne weiteres durch Abzählen zu lösen.

Satz B.2.1 *Sei die Anzahl der Spieler $n = 2^r - 1$ ($r \in \mathbb{N}$). Dann ist die Gewinnwahrscheinlichkeit des Hutproblems $\geq \frac{n}{n+1}$.*

Beweis. Wir benötigen

Definition B.2.2 (Hamming-Code). Sei $r \geq 2$. Auf $\mathbb{F}_q^r \setminus \{0\}$ definieren wir eine Äquivalenzrelation

$$(a_1, \dots, a_r) \sim (b_1, \dots, b_r) : \Leftrightarrow \text{ex. } \lambda \in \mathbb{F}_q \text{ mit } b_i = \lambda \cdot a_i \text{ für } i = 1, \dots, r.$$

Die zugehörigen Äquivalenzklassen bezeichnen wir mit $(a_1 : a_2 : \dots : a_r)$. Dann heißt

$$\mathbb{P}^{r-1} := \{(a_1 : a_2 : \dots : a_r) \mid a_i \in \mathbb{F}_q, \text{ nicht alle } a_i = 0\}$$

der $(r-1)$ -dimensionale projektive Raum über \mathbb{F}_q . Elementet von \mathbb{P}^{r-1} heißen *Punkte*. Für jeden Punkt $P_i \in \mathbb{P}^{r-1}$ wählen wir einen Repräsentanten $h_i^t = (a_{1i}, \dots, a_{ri}) \in \mathbb{F}_q^r$ und setzen

$$H := (h_1, \dots, h_n)$$

(wobei $n := \#\mathbb{P}^{r-1}$; man beachte, daß die Reihenfolge der Spalten nicht eindeutig ist).

Der Code $C \leq \mathbb{F}_q^r$ mit der Kontrollmatrix H heißt *Hamming-Code*, d.h.

$$C = \{u \in \mathbb{F}_q^r \mid H \cdot u^t = 0\}.$$

Der Hamming-Code ist ein $[n, k, d]$ -Code mit

$$n = \frac{q^r - 1}{q - 1}, \quad k = n - r, \quad d = 3.$$

Zudem ist dieser *perfekt*, d.h. es gilt

$$\mathbb{F}_q^r = \bigcup_{c \in C} B_1(c)$$

(dabei ist $B_1(c)$ die Kugel vom Radius $1 = \lfloor \frac{d-1}{2} \rfloor$ um das Element $c \in C$).

Wir betrachten für das Hutproblem den Fall $q = 2$. Wir setzen etwa 1 für rot und 0 für blau. Der Hamming-Code hat im Fall $q = 2$ die Parameter

$$n = 2^r - 1, \quad k = n - r, \quad d = 3.$$

Die Matrix H enthält als Spalten alle Vektoren aus $\mathbb{F}_2^r \setminus \{0\}$, denn zwei Vektoren sind im Fall $q = 2$ nur dann äquivalent, wenn sie gleich sind.

Es folgt nun die Strategie, mit der die $n = 2^r - 1$ Spieler eine Gewinnwahrscheinlichkeit von $\geq \frac{n}{n+1} = \frac{2^r-1}{2^r}$ erreichen. Jeder Spieler geht dabei wie folgt vor:

Für $i = 1, \dots, n$ sieht Spieler i die Hutverteilung

$$\hat{a} := \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ * \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{F}_2^n$$

(* steht dabei für die Farbe seines eigenen Hutes, den er nicht sehen kann). Spieler i setzt nun für * einmal 1 und einmal 0, etwa

$$\hat{a}^{(1)} := \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ 1 \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{F}_2^n \quad \text{und} \quad \hat{a}^{(0)} := \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ 0 \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{F}_2^n,$$

und berechnet dann $H \cdot \hat{a}^{(1)}$ und $H \cdot \hat{a}^{(0)}$.

Ist

$$H \cdot \hat{a}^{(1)} = 0 \quad \wedge \quad H \cdot \hat{a}^{(0)} \neq 0$$

(bzw. $H \cdot \hat{a}^{(1)} \neq 0 \quad \wedge \quad H \cdot \hat{a}^{(0)} = 0$),

so tippt Spieler i * = 0 (bzw. * = 1), andernfalls paßt er.

Um zu zeigen, daß man mit dieser Methode eine Gewinnwahrscheinlichkeit von $\geq \frac{n}{n+1}$ hat, muß man nur beweisen, daß bei allen Hutverteilungen $b \notin C$ mindestens ein Spieler richtig tippt, und die anderen keine falschen Tips abgeben. Denn es gilt

$$\frac{n}{n+1} = \frac{2^r - 1}{2^r} = \frac{2^n - 2^{n-r}}{2^n} = \frac{\#\mathbb{F}_2^n - \#C}{\#\mathbb{F}_2^n} = \frac{\#(\mathbb{F}_2^n \setminus C)}{\#\mathbb{F}_2^n}.$$

Sei also $b := \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \notin C$. Da der Hamming-Code perfekt ist, existiert ein $\tilde{b} \in C$ derart,

daß $b \in B_1(\tilde{b})$. Somit unterscheidet sich b von \tilde{b} nur in einer Komponente. Sei etwa

$$\tilde{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_j + 1 \\ \vdots \\ b_n \end{pmatrix} \in C$$

(d.h. b und \tilde{b} unterscheiden sich nur in der j -ten Komponente).
Spieler j sieht die Hutverteilung

$$\hat{b} := \begin{pmatrix} b_1 \\ \vdots \\ b_{j-1} \\ * \\ b_{j+1} \\ \vdots \\ b_n \end{pmatrix} \in \mathbb{F}_2^n.$$

Er setzt nun $* = 1$ (bzw. $* = 0$) und berechnet $H \cdot \hat{b}^{(1)}$ (bzw. $H \cdot \hat{b}^{(0)}$). Offensichtlich gilt hier entweder

$$b = \hat{b}^{(1)} \quad \text{und} \quad \tilde{b} = \hat{b}^{(0)}$$

oder

$$b = \hat{b}^{(0)} \quad \text{und} \quad \tilde{b} = \hat{b}^{(1)}.$$

Da $b \notin C$ und $\tilde{b} \in C$, folgt $H \cdot \hat{b}^{(1)} = 0 \wedge H \cdot \hat{b}^{(0)} \neq 0$ (bzw. $H \cdot \hat{b}^{(1)} \neq 0 \wedge H \cdot \hat{b}^{(0)} = 0$). Spieler j gibt somit einen Tip ab. Und zwar tippt er $* = l$ ($l \in \{1, 2\}$) so, daß $H \cdot \hat{b}^{(l)} \neq 0$. Dies kann nur für $\hat{b}^{(l)} = b$ sein, da die andere Möglichkeit \tilde{b} aus C ist. Somit tippt Spieler j die Farbe seines Hutes richtig.

Wir müssen nun noch zeigen, daß die anderen Spieler nicht falsch tippen. Wir betrachten für $i \in \{1, \dots, n\} \setminus \{j\}$ den Spieler i . Dieser sieht die Hutverteilung

$$\hat{b} := \begin{pmatrix} b_1 \\ \vdots \\ b_{i-1} \\ * \\ b_{i+1} \\ \vdots \\ b_n \end{pmatrix} \in \mathbb{F}_2^n$$

und setzt jeweils einmal $* = 1$ und einmal $* = 0$. Von \tilde{b} unterscheiden sich $\hat{b}^{(1)}$ und $\hat{b}^{(0)}$ jetzt mindestens in einer, aber höchstens in zwei Komponenten - nämlich neben der j -ten höchstens noch in der i -ten Komponente. Da aber der Minimalabstand von C gleich 3 ist, ist weder $\hat{b}^{(0)}$ noch $\hat{b}^{(1)}$ ein Codewort aus C . Daher ist $H \cdot \hat{b}^{(1)} \neq 0$ und $H \cdot \hat{b}^{(0)} \neq 0$. Somit paßt Spieler i .

□

Bemerkung 1. Ist die Hutverteilung gerade so, daß diese einem Codewort aus C entspricht, dann tippen mit der oben angegebenen Methode alle Spieler falsch. Denn jeder Spieler erhält je einen Vektor aus C und einen Vektor, der nicht aus C ist, wenn er für $*$ jeweils 1 und 0 einsetzt. Multipliziert er diese Vektoren mit der Matrix H , dann ist das Ergebnis einmal $= 0$ und einmal $\neq 0$. Nach der obigen Methode würde nun jeder Spieler einen Tip abgeben. Dabei tippt er $*$ so, daß die beobachtete Hutverteilung zusammen mit $*$ kein Codewort aus C ist. Jeder Spieler würde also falsch tippen. Damit ist die Gewinnwahrscheinlichkeit mit der oben angegebenen Methode genau gleich $\frac{n}{n+1}$.

Bemerkung 2. Die Spielstrategie aus Abschnitt B.1 entspricht genau der obigen Methode für $3 = 2^2 - 1$ Spieler.

Literaturverzeichnis

1. F. J. MacWilliams & N. J. A. Sloane, The Theory of Error-Correcting Codes; Amsterdam: North-Holland 1977
2. H. Stichtenoth, Algebraic Function Fields and Codes, Berlin: Springer 1993
3. W. Willems, Codierungstheorie, Berlin: de Gruyter 1999
4. AAECC Vol.10(2000) Issue 6; Niederreiter & Xing, A Propagation Rule for Linear Codes; Springer 2000
5. A. S. Marchukov, Summation of the Products of Codes, Problemy Peredachi Informatsii (Problems of Information Transmission), Vol.4, No.2, S.11-20, 1968
6. S. Hirasawa, M. Kasahara, Y. Sugiyama und T. Namekawa, Modified Product Codes, IEEE Transactions on Information Theory, Vol.IT-30, No.2, S.299-306, März 1984
7. E. L. Blokh und V. V. Zyablov, Coding of generalized cascade codes, Problems of Information Transmission, Vol.10, No.3, S.218-222, 1974
8. L. M. G. M. Tolhuizen, New Binary Linear Block Codes, IEEE Transactions on Information Theory, Vol.IT-33, No.5, September 1987
9. A. E. Brouwer, Bounds on the Minimum Distance of Linear Codes, www.win.tue.nl/~aeb/voorlincod.html
10. F. Özbudak & H. Stichtenoth, Note on Niederreiter-Xing's Propagation Rule for Linear Codes, Preprint 2000
11. Denksport für Hutträger, Die Zeit, Nr.19, S.46, 3.Mai 2001