Publ. I.R.M.A. Strasbourg, 1984, 229/S–08
Actes 8^e Séminaire Lotharingien, p. 71–74

DIE KONSTRUKTION ALLER MAXIMALEN CODE MIT HILFE VON MDS-CODEN

VON

ULRICH OBERST UND ARNE DÜR

Einführung (vergl. [1]) und Motivation. — Ein *linearer* Code der Länge n über einem endlichen Körper F ist ein Unterraum C von F^n. Das für die Anwendungen wichtigste Beispiel eines solchen F ist das binäre "Alphabet" $F = \{0,1\}$. Bezeichne $\dim({}_F C)$ die Dimension von C. Auf F^n betrachtet man die Hamming-"Norm"

$$\|x\| = \text{Anzahl der von Null verschiedenen Komponenten eines Vektors } x = (x_1, \ldots, x_n) \in F^n.$$

Die normerhaltenden linearen Automorphismen von F^n heißen Isometrien. Man kann die algebraische Codierungstheorie als Geometrie bezüglich der Hammingmetrik oder als Invariantentheorie der Isometriegruppe betrachten.

Die Zahl

$$d(C) = \min\{\|x\| \;;\; x \in D,\ x \neq 0\}$$

heißt die *Distanz* des Codes C. Es gilt

$$\dim(C) + d(C) \leq n + 1. \tag{1}$$

Der Code C heißt *MDS-Code*, falls in (1) die Gleichheit gilt. Der Code C heißt *maximal*, falls er unter allen Coden $\widetilde{C} \subseteq F^n$ mit $d(\widetilde{C}) \geq d(C)$ maximal (bezüglich der Inklusion) ist.

Das Ziel der algebraischen Codierungstheorie ist es, "gute" (z.B. maximale) Code zu finden, für welche sowohl die Dimension als auch die Distanz möglichst groß sind. Informationstheoretisch bedeutet dies, daß man mit Hilfe dieser Code Nachrichten sowohl schnell wie möglichst fehlerfrei über einen gestörten symmetrischen Kanal übertragen kann. Eine bedeutende Klasse von "guten" Coden ist die der *alternanten*, insbesondere der *Goppa* Code : Seien k und n natürliche Zahlen mit $2 \leq k \leq n-2$. Seien K ein endlicher Erweiterungskörper von F mit wenigstens n Elementen und $a_1, \ldots, a_n$ n paarweise verschiedene Elemente von K. Die Vektoren

$$(a_1^i, \ldots, a_n^i), \qquad i = 0, \ldots, k-1$$

sind die Basis eines MDS-Codes der Dimension k und Distanz $d = n+1-k$ über K. Jeder zu einem solchen isometrische Code $Z \subseteq K^n$ heißt *alternanter MDS-Code*. Der Code

$$C := F^n \cap Z$$

hat dann ebenfalls wenigstens die Distanz d, kann aber sehr klein sein. Bei *geeigneter* Wahl von Z erhält man aber "gute" Code. Die so erhaltenen Code heißen *alternant*.

Die folgenden Sätze zeigen, daß man in der Form $C = Z \cap F_n$ *alle* maximalen Code erhält, wenn man von geeigneten MDS-Coden Z ausgeht, und daß die Klasse der alternanten Code "sehr klein" ist.

Ergebnisse.

SATZ 1. — *Seien $C \subseteq F^n$ ein Code der Dimension l und Distanz d und K ein endlicher Oberkörper von F mit wenigtens $\binom{n-1}{d-1} + \binom{n-l-2}{d-1} + 1$ Elementen. Dann gibt es einen MDS-Code $Z \subseteq K^n$ der gleichen Distanz d mit*

$$C \subseteq Z \cap F^n.$$

Ist speziell C maximal, so ist $C = Z \cap F^n$.

Die im vorigen Satz benötigten MDS-Code Z erhält man auf folgende Weise : Sei weiter $2 \leq k \leq n-2$. Ist

$$B = \Big(B(i,j)\ ;\ i = 1, \ldots, k,\ j = k+1, \ldots, n\Big), \quad B(i,j) \in K,$$

eine $k \times (n-k)$-Matrix mit Koeffizienten in K, so sei

$$Z(B) = \{x = (x_1, \ldots, x_n) \in K_n\ ;\ (x_1, \ldots, x_k)B = (x_{k+1}, \ldots, x_n)\}.$$

SATZ 2. — *Bezeichnungen wie oben. Die Abbildung $B \to Z(B)$ induziert eine Bijektion der Menge $\mathbf{V}(K)$ aller $k \times (n-k)$-Matrizen mit Koeffizienten in K, deren quadratische Unterdeterminanten ungleich 0 sind, auf die Menge $\mathbf{C}(K)$ aller MDS-Code der Dimension k in K^n.*

Wie uns die Kollegen HEISE (München) und HERGERT (Darmstadt) mitteilten, ist eine Version dieses Satzes bekannt und insbesondere enthalten in dem Buch [2]. Dieses war uns bis jetzt nicht zugänglich. Von Interesse ist nach SATZ 1 die Dimension von $F_n \cap Z(B)$.

SATZ 3. — *Sei $F \subset K$ eine Erweiterung der Dimension m und habe F q Elemente. Seien $Z = S(B) \subseteq K^n$ wie in* SATZ 2 *und $C := Z \cap F^n$ wie in* SATZ 1 *definiert. Dann ist*

$$\dim({}_F C) = k - \mathrm{Rang}(B^{(1)} - B, \ldots, B^{(m-1)} - B). \tag{2}$$

Dabei ist

$$B^{(l)} = \Big(B(i,j)^{q(l)};\ i = 1, \ldots, k,\ j = k+1, \ldots, n\Big), \quad q(l) = q^l.$$

Die Matrix auf der rechten Seite von (2) *hat die Gestalt* $k \times (m-1)(n-k)$.

Die Menge $\mathbf{V}(K)$ in Satz 2 ist auf offensichtliche Weise die Menge der K-rationalen Punkte der $k(n-k)$-*dimensionalen affinen algebraischen Mannigfaltigkeit* $\mathbf{V}(\widetilde{F})$, wobei $\widetilde{F} \supseteq K$ der algebraische Abschluß von F ist. Durch Strukturtransport bildet dann auch die Menge $\mathbf{C}(\widetilde{F})$ der MDS-Code der Dimension k in $\widetilde{F}^n$ eine solche Mannigfaltigkeit und $\mathbf{C}(K)$ ist deren Menge der K-rationalen Punkte. Bezeichne $\mathrm{Alt}(K)$ die Menge der alternanten MDS-Code der Dimension k in K^n. Der nächste Satz zeigt, daß eine "kleine" Untermannigfaltigkeit von $\mathbf{C}$ ist. Sei

$$Z = Z(B) \subseteq K^n, \quad B \in \mathbf{V}(K),$$

ein MDS-Code der Dimension k in K^n. Betrachte die zugehörige normalisierte Matrix

$$A = \big(A(i,j)\ ;\ i = 2, \ldots, k,\ j = k+2, \ldots, n\big),$$
$$A(i,j) := \frac{B(i,j)\,B(1,k+1)}{B(i,k+1)\,B(1,j)}$$

und die $(k-2)(n-k-2)$ Relationen

$$\text{(3)} \qquad \frac{A(i,j)-1}{A(i,j)A(2,j)^{-1}-1} = \frac{A(i,j+1)-1}{A(i,j+1)A(2,j+1)^{-1}-1}, \quad i = 3, \ldots, k, \quad j = k+2, \ldots, n.$$

Satz 4. — *Voraussetzungen und Bezeichnungen wie oben. Der Code* $Z(B)$ *is genau dann ein alternanter MDS-Code, wenn die Gleichungen* (3) *erfüllt sind. Die Menge* $\mathrm{Alt}(\widetilde{F})$ *ist eine* $(2n-4)$-*dimensionale abgeschlossene Untermannigfaltigkeit von* $\mathbf{C}(\widetilde{F})$. *Insbesondere ist*

$$\mathrm{Alt}(\widetilde{F}) \underset{\neq}{\subset} \mathbf{C}(\widetilde{F}) \qquad \text{für } 3 \leq k \leq n-3.$$

Dies bedeutet, daß es für $3 \leq k \leq n-3$ *sehr wenige alternante Code gibt oder, anders, daß die Alternanz keine generische Eigenschaft von Coden ist.*

Die Sätze 1 und 4 machen die Suche nach neuen Klassen von MDS-Coden auf neue Weise interessant.

LITERATUR

[1] VAN LINT (J.H.). — *Introduction to coding theory.* — Berlin, Springer-Verlag, 1982.
[2] MAC WILLIAMS (F.J.) and SLOANE (N.J.A.). — *The theory of error-correcting codes.* — North-Holland, 1977.

Ulrich OBERST u. Arne DÜR,
Institut für Mathematik
der Universität,
Innrain 52,
A-6020 Innsbruck.