Seminar-Handout zur Griesmer-Schranke

Patrick-Thomas Chmielewski

19.06.2006

Inhaltsverzeichnis

1 Griesmer-Schranke

Die Griesmer-Schranke ist eine Schranke über die Länge eines linearen Codes und wie folgt definiert:

Sei C ein **[n, k, d]**-Code über dem Körper K mit q Elementen[1]. Dann gilt:

$$n \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil$$

Der Beweis erfolgt mit Hilfe einer Induktion über k. Dabei ist für k = 0, 1 die Aussage richtig und es wird der Fall $k \geq 2$ betrachtet. Für ein solches k sei G eine Generatormatrix für den Code C und deren erste Zeile ein Codewort minimalen Gewichts. Es darf durch den Übergang in einen äquivalenten Code[2] angenommen werden, dass G folgende Form hat:

$$\mathbf{A} = \begin{pmatrix} 1 & \cdots & 1 & 0 & \cdots & 0 \\ & G_1 & & & G_2 & \end{pmatrix} = \begin{pmatrix} & z & \\ G_1 & & G_2 \end{pmatrix}$$

Hierbei ist G_1 vom Typ $(k-1, d)$, denn wegen $wt(z) \geq d, z \in C$ sind ja genau die ersten d Komponenten gleich 1. Entsprechend ist G_2 vom Typ $(k-1, n-d)$, weil ja die Worte die Länge n haben und die ersten d-Stellen bereits "1"

[1] Wobei **n** die Wortlänge, **k** die Dimension von C ist und **d** den Minimalabstand.

[2] D.h. ein Code, der durch Vertauschung der Bitpositionen aus dem anderen Code hervorgeht.

sind. Für den weiteren Verlauf ist es notwendig zu zeigen, dass Rang $G_2 = k-1$ ist. Dies erfolgt durch einen Widerspruchsbeweis. Angenommen Rang $G_2 < k-1$, dann lässt sich die Matrix $(G_1 \mid G_2)$ durch Zeilenumformungen auf folgende Gestalt bringen:

$$\begin{pmatrix} a_1 & \cdots & a_d & 0 & \cdots & 0 \\ & * & & & * & \end{pmatrix}$$

Da wir annehmen, dass Rang $G_2 < k-1$, muss eine Zeile in G_2 aus Nullen bestehen. Wäre nun $a_1 = a_2 = \cdots = a_d$, dann wäre dies ein Widerspruch zum Rang G = k, denn durch elementare Zeilenumformungen ließen sich so die $1 \cdots 1$ aus z eliminieren, welche ja genau an den ersten d Stellen stehen. Daraus folgt, dass $0 \neq c = a_1 \cdot z - (a_1 \cdots a_d) \in C$[3]. Da so aber die erste Komponente in c eine Null wäre, ergibt dies einen Widerspruch zu $wt(c) \geq d$. Damit ist bewiesen, dass G_2 eine Generatormatrix für einen $[n-d, k-1, d_2]$-Code C_2 ist.

Sei nun $(u \mid v)$ eine beliebige Zeile in der Matrix $(G_1 \mid G_2)$ und $u = (u_1, \cdots, u_d)$. Desweiteren sei für ein $b \in K$ und ein passendes $a \in K$ $n_b = |\{i \mid u_i = b\}|$ (Anzahl der Komponenten in u gleich b) und $n_a = max\{n_b \mid b \in K\}$. Betrachtet man den ungünstigen Fall der Verteilungen der Elemente aus K in u, so sieht man, dass diese sich alle $q = \mid K \mid$ wiederholen und somit offensichtlich $n_a \geq \lceil d/q \rceil$. Wegen $0 \neq (u \mid v) - az \in C$ (Linearkombination ergibt wieder ein Wort aus C) und somit

$$\begin{aligned} wt((u \mid v) - az) &\geq d \\ d - n_a + wt(v) &\geq d && \mid -d + n_a \\ wt(v) &\geq n_a \geq \lceil d/q \rceil \end{aligned}$$

Durch elementare Zeilenumformungen von $(G_1 \mid G_2)$ kann man jedes $0 \neq v \in C_2$ konstruieren. Somit ist $d_2 \geq \lceil d/q \rceil$.

Induktionsannahme:

$$\begin{aligned} n - d \geq \sum_{i=0}^{k-2} \lceil d_2/q^i \rceil \geq \sum_{i=0}^{k-2} \lceil d/q^{i+1} \rceil = \sum_{i=1}^{k-1} \lceil d/q^i \rceil && \mid +d \\ n \geq \sum_{i=1}^{k-1} \lceil d/q^i \rceil + \lceil d/q^0 \rceil = \sum_{i=0}^{k-1} \lceil d/q^i \rceil && \text{q.e.d.} \end{aligned}$$

[3] $c \in C$, weil in einer Generatormatrix die Zeilen gleichzeitig Codeworte sind und sich jedes Codewort als Linearkombination der Zeilen ausdrücken lässt.

2 Binäre Reed-Muller-Code

Zur kurzen Einführung in den Reed-Muller-Code ist es ersteinmal notwendig zu erklären, was die Plotkin-Konstruktion ist. Denn der Reed-Muller-Code wird eben mit einer solchen rekursiven Methode konstruiert. Anschließend wird noch gezeigt, dass der binäre Reed-Muller-Code erster Ordnung die eben vorgestellte Griesmer-Schranke erreicht.

2.1 Plotkin-Konstruktion

Die Plotkin-Konstruktion ist eine Art Verkettung zweier gleichlanger Codes C_1 und C_2 derart, dass ein neuer rekursiver Code C entsteht. Dieser hat die Form $C = C_1 \propto C_2 := c_1 \circ (c_1 + c_2) \mid c_1 \in C_1, c_2 \in C_2$. Hierbei ist $\circ$ die Konkatenation, definiert als $c \circ c^{'} := (c, c^{'})$:

$$(a_0, a_1, \cdots, a_n) \circ (a_0^{'}, a_1^{'}, \cdots, a_n^{'}) = (a_0, a_1, \cdots, a_n, a_0^{'}, a_1^{'}, \cdots, a_n^{'})$$

Mit $c + c^{'}$ ist die Addition zweier Vektoren gemeint:

$$(a_0, \cdots, a_n) + (a_0^{'}, \cdots, a_n^{'}) = (a_0 + a_0^{'}, \cdots, a_n + a_n^{'})$$

Für einen solchen Code gilt: *Sei C_1 ein $[n, k_1, d_1]$-Code und C_2 ein $[n, k_2, d_2]$-Code über einem Körper $\mathbb{F}_q$, dann ist $C_1 \propto C_2$ ein $[2n, k_1 + k_2, min\{2d_1, d_2\}]$-Code über $\mathbb{F}_q$.*

2.2 Reed-Muller-Code

Wie schon eingangs erwähnt wird mit eben der Plotkin-Konstruktion der bekannte Reed-Muller-Code k-ter Ordnung $\mathcal{R}(k, m)$ für $0 \leq k \leq m$ erzeugt. Seine rekursive Definition lautet:

$$\mathcal{R}(k, m) = \begin{cases} \{0^m, 1^m\} & \text{für k = 0} \\ \mathbb{F}_2^{2^m} & \text{für k = m} \\ \mathcal{R}(k, m-1) \propto \mathcal{R}(k-1, m-1) & \text{für 0 < k < m} \end{cases}$$

Ein solcher Reed-Muller-Code k-ter Ordnung $\mathcal{R}(k, m)$ ist ein $[2^m, \sum_{i=0}^{k} \binom{m}{i}, 2^{m-k}]$-Code. Der Reed-Muller-Code erster Ordnung $\mathcal{R} := \mathcal{R}(1, m)$ wurde in den 1970er Jahren von der NASA bei den Mariner-Mission verwendet[4], um die Bilder vom Mars auf die Erde zu schicken. Eben dieser $\mathcal{R}(m)$-Code mit den Parametern $[2^m, m + 1, 2^{m-1}]$ erreicht die Griesmer-Schranke.

[4] Es wurde der $\mathcal{R}(5)$-Code verwendet

Beweis:

$$2^m \geq \sum_{i=0}^{m} \lceil \frac{2^{m-1}}{2^i} \rceil = 2^{m-1} + 2^{m-2} + \cdots + 2 + 1 + 1$$
$$= \frac{1 - 2^m}{1 - 2} + 1 = 2^m$$
$$q.e.d$$

3 Quellen

Codierungstheorie von Wolfgang Willems, ISBN: 3110158744 - Walter de Gruyter
Skript zur Vorlesung Kodierung und Sicherheit von Dr. Andreas Jakoby - Institut für Theoretische Informatik der Universität zu Lübeck
Codierungstheorie von Ralph-Hardo Schulz, ISBN: 3528164190 - Vieweg Verlag
Lineare Algebra von Albrecht Beutelspacher, ISBN: 352856508X - Vieweg Verlag