ETH Zürich
Dept. Informatik

Prof. Markus Gross
WS 05/06

Informationstheorie

Lösung 11

11.1 Minimaldistanz

a) Die Minimaldistanz ist $d_{min} = 2$. Um Fehler detektieren zu können, muss für die Anzahl Fehler r folgendes gelten: $d_{min}(C) \geq r + 1$. Daraus folgt, dass maximal 1 Fehler erlaubt ist.
Um Fehler korrigieren zu können dürfen maximal s Fehler auftreten. s ist begrenzt durch $d_{min}(C) \geq s * 2 + 1$. Daraus folgt, es darf kein Fehler auftreten.

b) Da die Codewörter in C_1 linear abhängig sind, ist es möglich.
Eine lineare Abhängikeit ist $010101 \oplus 010010 = 000111$, deshalb kann eines dieser Codewörter weggelassen werden. Die drei Codewörter stellen eine Basis von C_2 dar. Eine Lösung ist zum Beispiel $C_2 = \text{span}\{010101, 000111, 111000\}$.

c) $C_2 = \{000000, 000111, 111000, 010101, 010010, 101101, 111111, 101010\}$. Die Minimaldistanz ist immer noch 2 und 010010 hat Hamminggewicht 2.

d) Sei d die Minimaldistanz des Codes. D.h. es gibt zwei Codewörter c, c' mit Hammingdistanz d. Da der Code ein linearer Unterraum ist, ist auch $c \oplus c'$ ein Codewort. $c \oplus c'$ ist genau dort ungleich Null, wo sich c und c' unterscheiden. Dies ist an d Stellen der Fall, also hat $c \oplus c'$ Hamminggewicht d.

11.2 Grenzen für die Anzahl Codewörter

a) Es gibt genau $\binom{N}{d}$ Codewörter, welche von einem gegebenen Codewort c Abstand d haben.

b) Aus Teilaufgabe a) folgt direkt

$$m(N, d) = \sum_{i=0}^{d} \binom{N}{i}.$$

c) Sei $A(N, d)$ die maximale Anzahl Codewörter eines Codes mit Codewörtern der Länge N und Minimaldistanz d. Wir zeigen, dass

$$A(N, d) \geq \frac{2^N}{\sum_{i=0}^{d-1} \binom{N}{i}}. \tag{1}$$

Sei also $\mathcal{C}$ ein Code mit maximaler Anzahl Codewörtern. Wir betrachten alle Kugeln vom Radius $d - 1$ um jedes Codewort in $\mathcal{C}$ und denken uns jedes Element, welches sich in (mindestens) einer dieser Kugeln befindet, als markiert. Damit haben wir höchstens $A(N,d) \cdot m(N,d-1)$ Elemente des Vektorraums markiert. Gäbe es jetzt noch ein unmarkiertes Element (also Hammingdistanz zu beliebigem Codewort mindestens d), wäre dieses ein zusätzliches Codewort und der Code hätte nicht die maximale Anzahl Codewörter. Also bleibt kein Element des Vektorraums unmarkiert, und es gilt $2^N \leq A(N,d) \cdot m(N,d-1)$, woraus der Ausdruck (1) direkt folgt.

d) Sei $\mathcal{C}$ ein Code mit Minimaldistanz d. Wir denken uns um jedes Codewort in $\mathcal{C}$ eine Kugel mit Radius $\lceil d/2 \rceil - 1$. Da der Abstand zwischen zwei beliebigen Codewörtern mindestens d ist, überschneiden sich diese Kugeln nicht. Jede Kugel um ein Codewort überdeckt aber mindestens $m(N, \lceil d/2 \rceil - 1)$ Elemente. Analog zur Teilaufgabe **c)** gilt $2^N \geq A(N,d) \cdot m(N, \lceil d/2 \rceil - 1)$. Als obere Schranke für die Anzahl Codewörter ergibt sich somit

$$A(N,d) \leq \frac{2^N}{\sum_{i=0}^{\lceil d/2 \rceil - 1} \binom{N}{i}}.$$

11.3 Zum Beweis des Kanalcodierungstheorems

Bezeichnen wir mit $M_{ij} \in \{0,1\}$, ob Student i Aufgabe j gelöst hat.
Betrachten wir die erwartete Punktezahl:

$$\frac{1}{100} \sum_{i=1}^{100} \left(\sum_{j=1}^{20} M_{ij} \right) = \frac{1}{100} \sum_{j=1}^{20} \left(\sum_{i=1}^{100} M_{ij} \right) \geq \frac{1}{100} \sum_{j=1}^{20} 35 = 7$$

Die über die Studenten gemittelte Punktezahl ist also grösser (oder gleich) 7. Somit muss es auch einen Studenten geben, der mindestens 7 Punkte erreicht hat. (Sonst wäre nämlich $\frac{1}{100} \sum_{i=1}^{100} \left(\sum_{j=1}^{20} M_{ij} \right) < \frac{1}{100} \sum_{i=1}^{100} 7 = 7$).
Der Matrixeintrag M_{ij} in dieser Aufgabe entspricht der Fehlerwahrscheinlichkeit des Codeworts mit Index j bei Verwendung des i-ten zufällig gewählten Codes im Beweis des Kanalcodierungstheorems auf S. 72 des Skriptes.

11.4 Durch Matrizen definierte Codes

a) Es gilt

$$\begin{aligned} [2\,1\,0]\,G &= [0\,2\,1\,2\,0\,0] \\ [1\,0\,1]\,G &= [1\,2\,1\,1\,1\,2] \\ [2\,2\,2]\,G &= [1\,1\,1\,2\,1\,0]. \end{aligned}$$

b) Die gesuchte Matrix muss die Form

$$G' = \begin{bmatrix} 1 & 0 & 0 & * & * & * \\ 0 & 1 & 0 & * & * & * \\ 0 & 0 & 1 & * & * & * \end{bmatrix}$$

haben (damit die zweite gestellte Bedingung erfüllt ist) und ihre Zeilen müssen aus Linearkombinationen der Zeilen von G bestehen. Mit anderen Worten muss G' aus

G entstehen, indem Zeilen addiert, mit Faktoren multipliziert und/oder vertauscht werden. Wir können also wie beim Gauss-Eliminationsverfahren vorgehen.

Wir eliminieren zuerst die 1 in der ersten Spalte der zweiten Zeile von G, indem wir die erste Spalte von der zweiten subtrahieren (dieses Vorgehen bezeichnen wir mit $\rightarrow^{(2')\leftarrow 2(1)+(2)}$, da dies der Addition der zweifachen ersten Zeile zur zweiten entspricht). Damit erhalten wir

$$G \rightarrow^{(2')\leftarrow 2(1)+(2)} \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 2 & 1 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Weiter verfahren wir wie folgt:

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 2 & 1 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \rightarrow^{(3')\leftarrow(2)+(3)} \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 2 & 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 & 1 \end{bmatrix}$$

$$\rightarrow^{(2')\leftarrow 2(2)} \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 & 1 \end{bmatrix} \rightarrow^{(3')\leftarrow 2(3)} \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 2 \end{bmatrix}$$

$$\rightarrow^{(2')\leftarrow(3)+(2)} \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 2 & 0 & 2 \\ 0 & 0 & 1 & 1 & 0 & 2 \end{bmatrix} \rightarrow^{(1')\leftarrow 2(2)+(1)} \begin{bmatrix} 1 & 0 & 0 & 2 & 1 & 2 \\ 0 & 1 & 0 & 2 & 0 & 2 \\ 0 & 0 & 1 & 1 & 0 & 2 \end{bmatrix}$$

Damit haben wir folgende Lösung gefunden:

$$G' = \begin{bmatrix} 1 & 0 & 0 & 2 & 1 & 2 \\ 0 & 1 & 0 & 2 & 0 & 2 \\ 0 & 0 & 1 & 1 & 0 & 2 \end{bmatrix}.$$