ETH Zürich
Dept. Informatik

Prof. Markus Gross
WS 05/06

Informationstheorie

Übung 11

Ausgabe: 30. Januar 2006

11.1 Minimaldistanz

a) Sei $C_1 := \{010101, 000111, 111000, 010010\}$ ein Code in $GF(2)^6$. Was ist die Minimaldistanz dieses Codes? Wieviele Fehler können bei diesem Code erkannt, wieviele korrigiert werden?

b) Sei C_2 der Code, der aus allen Linearkombinationen von Codewörtern in C_1 besteht. Kann C_2 auch als die Menge von Linearkombinationen von nur drei Codewörtern aus C_1 beschrieben werden?

c) Wie gross ist die Minimaldistanz von C_2? Gibt es ein Codewort, dessen Hamminggewicht genau die Minimaldistanz ist?
(Das Hamminggewicht gibt die Anzahl Zeichen an, die sich von 0 unterscheiden)

d) C_2 ist ein linearer Unterraum von $GF(2)^6$. Beweisen Sie, dass es in jedem Code, der als linearer Unterraum von $GF(2)^n$ aufgefasst werden kann, ein Codewort gibt, dessen Hamminggewicht die Minimaldistanz des Codes ist.
Tipp: Axiome für lineare Codes betrachten.

11.2 Grenzen für die Anzahl Codewörter

In dieser Aufgabe betrachten wir binäre Codes mit Wortlänge N.

a) Wie viele Wörter haben Hamming-Distanz d von einem gegebenen Codewort c?

Für die folgenden Betrachtungen ist es von Nutzen, die Codewörter mit Hamming-Distanz maximal d zu einem gegebenen Codewort c als Kugel im Raum aller Codewörter (der Länge N) mit Radius d und Mittelpunkt c zu betrachten. Sei $m(N, d)$ die Anzahl Codewörter, welche in einer solchen Kugel liegen.

b) Geben Sie einen Ausdruck für $m(N, d)$.

c) Sie möchten einen Code mit möglichst vielen Codewörtern konstruieren bei gegebener Minimaldistanz $d_{min} = d$. Geben Sie eine möglichst grosse untere Schranke für die Anzahl möglicher Codewörter.

Tipp: Platzieren Sie die Codewörter mit der umgebenden Kugel im Raum. Vergleichen Sie anschliessend den verbrauchten Raum aller Kugeln mit dem vorhandenen Raum 2^n.

d) Wie viele Codewörter kann ein Code mit Minimaldistanz $d_{min} = d$ maximal haben? (Gehen Sie gleich vor wie bei der Teilaufgabe **c)**, passen Sie aber die Radien der Kugeln an.)

11.3 Zum Beweis des Kanalcodierungstheorems

Diese Aufgabe soll den zweiten Teil von Shannons Theorem[1] veranschaulichen.

Angenommen, 100 Prüflinge legen einen Test mit 20 verschiedenen Aufgaben ab. Von den 20 Assistierenden eines Instituts erhält jeder eine Aufgabe zur Korrektur. Beim Korrigieren stellen alle fest, dass mehr als 35 Prüflinge „ihre“ Aufgabe korrekt gelöst haben. Schliessen Sie daraus, dass jemand mehr als einen Drittel aller Aufgaben richtig gelöst hat.

11.4 Durch Matrizen definierte Codes

Gegeben sei die Matrix

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

Wir definieren einen linearen *ternären* Code durch folgende Abbildung: Ein Element $c \in GF(3)^3$ wird codiert durch $cG \in GF(3)^6$. (Bemerkung: Ein ternärer Code ist über $GF(3)$ definiert!)

a) Bestimmen Sie diejenigen Codewörter, die durch Codierung von [2 1 0], [1 0 1] und [2 2 2] entstehen.

b) Finden Sie eine Matrix G', die dieselbe Codewortmenge wie G erzeugt und für die jedes Codewort mit dem codierten Element beginnt, d.h. $cG' = [c_1\ c_2\ c_3\ *\ *\ *]$ für jedes $c = [c_1\ c_2\ c_3] \in GF(3)^3$.

[1] Kapitel 12, Folie 7 oder Lemma 4.8 auf Seite 70 des Skripts von Prof. Ueli Maurer