Department Mathematik
der Universität Hamburg
Bereich Algebra und Zahlentheorie
Prof. Dr. G. Höhn

Bundesstrasse 55
20146 Hamburg
Tel. (040) 42838-5172
hoehn@math.uni-hamburg.de

Übungen zur Vorlesung Codes, Gitter und Vertexalgebren

Sommersemester 2009

Blatt 1

Abgabe: Montag, 13.4.2009

Aufgabe 1: (Entropie)

a) Es seien $(p_1, \ldots, p_m)$ and $(q_1, \ldots, q_m)$ zwei m-Tupel reeller Zahlen mit $p_i \geq 0$ und $q_i > 0$ für $i = 1, \ldots, m$, sowie $\sum_{i=1}^m p_i = \sum_{i=1}^m q_i = 1$. Man beweise die Ungleichung

$$-\sum_{i=1}^m p_i \log p_i \leq -\sum_{i=1}^m p_i \log q_i. \qquad \textit{(1 Punkt)}$$

(*Hinweis:* Man verwende für reelles $x > 0$ die Ungleichung $\log x \leq (x-1)\log e$.)

b) Man zeige, daß die Entropiefunktion

$$H_m : D_m := \left\{ (p_1, \ldots, p_m) \in (\mathbf{R}_{\geq 0})^m \mid \sum_{i=1}^m p_i = 1 \right\} \longrightarrow \mathbf{R}, \quad (p_1, \ldots, p_m) \mapsto -\sum_{i=1}^m p_i \cdot \log p_i$$

an der Stelle $(\frac{1}{m}, \ldots, \frac{1}{m})$ ihr globales Maxium annimmt. *(1 Punkt)*

c) Es sei $G_m : D_m \longrightarrow \mathbf{R}$, $m \in \mathbf{N}$, eine Familie stetiger Funktionen, mit folgenden Eigenschaften:

i) $G_m(\frac{1}{m}, \ldots, \frac{1}{m})$, $m \in \mathbf{N}$, ist eine streng monoton steigende Folge;

ii) $G_{ml}(\frac{1}{ml}, \ldots, \frac{1}{ml}) = G_m(\frac{1}{m}, \ldots, \frac{1}{m}) + G_l(\frac{1}{l}, \ldots, \frac{1}{l})$;

iii) $G_m(p_1, \ldots, p_m) = G_2(p_1 + \cdots + p_k, p_{k+1} + \cdots + p_m) +$
$(p_1 + \cdots + p_k) \cdot G_k\left(\frac{p_1}{\sum_{i=1}^k p_i}, \ldots, \frac{p_k}{\sum_{i=1}^k p_i}\right) + (p_{k+1} + \cdots + p_m) \cdot G_{m-k}\left(\frac{p_{k+1}}{\sum_{i=k+1}^m p_i}, \ldots, \frac{p_m}{\sum_{i=k+1}^m p_i}\right)$
für $1 \leq k < m$, $\sum_{i=1}^k p_i > 0$ und $\sum_{i=k+1}^m p_i > 0$.

Man zeige, daß es eine positive reelle Konstante α gibt, so das $G_m = \alpha \cdot H_m$ für alle $m \in \mathbf{N}$. *(2 Punkte)*

(*Anleitung:* Man zeige nacheinander (1) $G_m(\frac{1}{m}, \ldots, \frac{1}{m}) = \alpha \cdot \log m$, (2) $G_2(p, 1-p) = \alpha \cdot H_2(p, 1-p)$ für rationales $p = \frac{r}{s}$, wozu man iii) auf $G_s(\frac{1}{s}, \ldots, \frac{1}{s})$ anwende und (3) schließlich durch vollständige Induktion $G_m = \alpha \cdot H_m$ für alle $m \in \mathbf{N}$.)

Aufgabe 2: (Quellencodierung)

Es sei $Q = (S, p)$ eine diskrete gedächtnislose Informationsquelle und T ein weiteres endliches Alphabet mit ℓ Elementen.

Man zeigem daß es keine decodierbare Codierung (also einen injektiven Halbgruppenhomomorphismus) $c : S^* \longrightarrow T^*$ geben kann, für die die durchschnittliche Wortlänge $N(c) = \sum_{s \in S} p(s) \cdot |c(s)|$ kleiner als $\frac{H(Q)}{\log \ell}$ ist. (X^* bezeichne die von einer Menge X erzeugte freie Halbgruppe und $|x|$ die Wortlänge von $x \in X^*$.) *(4 Punkte)*

(*Anleitung:* Es seien n_i die Längen der Worte $c(s_i)$. Dann ist $\sum_{i=1}^{|S|} \ell^{-n_i} \leq 1$. Man schätze dazu $\left(\sum_{i=1}^{|S|} \ell^{-n_i}\right)^g$ durch Ausdistribuieren nach oben ab, ziehe die g-te Wurzel und lasse g nach unendlich laufen. Schließlich verwende man die Ungleichung aus Aufgabe 1 a).)

Aufgabe 3: (Binäre Hammingcodes)

Der allgemeine binäre Hammingcode $\mathcal{H}_k$ ist ein binärer Blockcode der Länge $2^k - 1$, der dadurch entsteht, daß man in die Liste der $2^k - k - 1$ Datenbits x_1, x_2, …, x_{2^k-k-1} zusätzlich k Korrekturbits y_1, y_2, …, y_k einfügt und zwar so, daß y_i, $i = 1, \ldots, k$, an der Position $2^i - 1$ steht und — unter Verwendung der so erhaltenen neuen Numerierung $(z_1, z_2, \ldots, z_{2^k-1}) = (y_1, y_2, x_1, y_3, x_2, x_3, x_4, y_4, \ldots, x_{2^k-k-1})$ — die folgenden k Gleichungen gelten:

$$\begin{aligned}
0 &= z_1 + z_3 + z_5 + z_7 + \cdots + z_{2^k-3} + z_{2^k-1}, \\
0 &= z_2 + z_3 + z_6 + z_7 + \cdots + z_{2^k-6} + z_{2^k-5} + z_{2^k-2} + z_{2^k-1}, \\
0 &= z_4 + z_5 + z_6 + z_7 + z_{12} \cdots + z_{2^k-4} + z_{2^k-3} + z_{2^k-2} + z_{2^k-1}, \\
\ldots &\quad \ldots \quad \ldots \\
0 &= z_{2^{k-1}} + z_{2^{k-1}+1} + z_{2^{k-1}+2} + \cdots + z_{2^k-2} + z_{2^k-1}.
\end{aligned}$$

a) Zeige, daß $\mathcal{H}_2$ zum Wiederholungscode W_3 und $\mathcal{H}_3$ zum Hammingcode H_7 aus der Vorlesung äquivalent ist. *(1 Punkt)*

b) Erläutere, wieso die k Korrekturbits y_i und damit der Code wohldefiniert sind. *(1 Punkt)* (*Hinweis:* Schreibe 1, 2, …, $2^k - 1$ im Dualsystem auf.)

c) Man zeige, daß $\mathcal{H}_k$ einen Übertragungsfehler von bis zu einem Bit korrigieren kann und man gebe die Datenrate von $\mathcal{H}_k$ an. *(1 Punkt)*

d) Man berechne die Wahrscheinlichkeit für einen nicht korrigierbaren Übertragungsfehler, falls man eine Nachricht mit $\mathcal{H}_k$ kodiert und dann durch den binären symmetrischen Kanal mit Fehlerwahrscheinlichkeit ϵ schickt. *(1 Punkt)*

Aufgabe 4: (Kusszahlen)

Es sei τ_n die Kußzahl im $\mathbf{R}^n$, d.h. die Maximalanzahl von Kugeln von festem Radius R, die eine weitere Kugel von diesem Radius gleichzeitig berühren können. Man beweise:

a) $\tau_2 = 6$; *(1 Punkt)*

b) $\tau_3 \geq 12$ durch die explizite Konstruktion von zwölf Punkten $P_i \in \mathbf{R}^3$ mit $||P_i|| = 1$ und $||P_i - P_j|| \geq 1$ für $i \neq j$; *(1 Punkt)*

c) $\tau_3 \leq 13$; (*Hinweis:* Kugelkappenoberflächen abschätzen); *(1 Punkt)*

d*) $\tau_3 \leq 12$. *(1 Punkt)*

Sie finden alle Übungsblätter auch im Internet unter der Adresse
`http://www.math.uni-hamburg.de/home/hoehn/cogiva`