Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Prof. Dr. Markus Gross
Daniel Cotting, Richard Keiser, Michael Waschbüsch, Martin Wicke

Departement Informatik
24. 2. 2005

Informationstheorie

Frühling 2005

Name : ....

Vorname : ....

ETH-Nummer : ....

Unterschrift : ....

Wichtige Hinweise

Tragen Sie als erstes Ihren Namen, Vornamen sowie Ihre ETH-Nummer ein und unterschreiben Sie die Prüfung. Legen Sie Ihre Legitimationskarte zur Kontrolle auf den Tisch.

Für die Prüfung stehen Ihnen 2 Stunden (120 Minuten) zur Verfügung. Die Punkte einer Aufgabe widerspiegeln ungefähr die Zeit in Minuten, die für die Lösung aufgewendet werden sollte. Verschaffen Sie sich zuerst einen Überblick über alle Aufgaben, bevor Sie zu viel Zeit in eine Aufgabe investieren.

Beginnen Sie jede Aufgabe mit einem neuen Blatt und versehen sie **jedes Blatt mit Ihrer Leginummer** und der Nummer der gelösten Teilaufgabe.

Schreiben Sie deutlich und benutzen Sie keinen Bleistift oder Rotstift.

Pro Aufgabe darf höchstens ein gültiger Lösungsversuch abgegeben werden. Ungültige Lösungsversuche müssen klar durchgestrichen sein.

Bitte beachten Sie, dass sie **keine Hilfsmittel** verwenden dürfen.

Viel Glück!

Aufgabe	erreichbare Punkte	erreichte Punkte	Visum
1	12		
2	11		
3	20		
4	40		
5	37		
Total	120		Note:

Aufgabe 1: Entropie I *12 (4/2/6) Punkte*

Eine binäre Informationsquelle sendet ein Bit A aus dem Alphabet $\{0, 1\}$ mit der Wahrscheinlichkeit $P(A = 1) = 2/3$ aus. Ein angeschlossener Empänger empfängt das Bit B, welches mit einer Wahrscheinlichkeit von $3/4$ dem gesendeten A entspricht. Im Fehlerfall wird dagegen das invertierte Bit empfangen.

a) Berechnen Sie die Verbundwahrscheinlichkeiten $P(AB)$ für alle möglichen Fälle.

b) Zeichnen Sie das Entropiediagramm von A und B und tragen Sie die folgenden Bezeichner an den entsprechenden Stellen ein: $H(A)$, $H(B)$, $H(A|B)$, $H(B|A)$, $H(AB)$, $I(A;B)$.

c) Geben Sie $H(A)$, $H(B)$, $H(A|B)$, $H(B|A)$, $H(AB)$ sowie $I(A;B)$ an. Verwenden Sie dazu die binäre Entropiefunktion $h(p)$.

Aufgabe 2: Entropie II *11 (1/1/1/4/4) Punkte*

Sei $X_1 \ldots X_N$ eine Folge von N unabhängigen Würfen einer unfairen Münze. Die Wahrscheinlichkeitsverteilung der Münze sei unbekannt, also $P(X_i = 1) = p$ und $P(X_i = 0) = 1 - p$. Weiterhin sei die Länge N der Folge variabel.

a) Berechnen Sie $H(X_1 \ldots X_N | N = n)$ als Funktion von n und p unter Verwendung der binären Entropiefunktion $h(p)$.

b) Geben Sie eine Formel für $H(X_1 \ldots X_N | N)$ an.

Sei nun $N = n$ fest. Aus den n unfairen Münzwürfen $X_1 \ldots X_n$ sollen K faire Münzwürfe $Z_1 \ldots Z_K$ mit $P(Z_i = 1) = P(Z_i = 0) = 1/2$ berechnet werden. Dies geschehe mit einer Funktion f, also $f(X_1, \ldots, X_n) = (Z_1, \ldots, Z_K)$. K kann dabei, abhängig von der jeweiligen Eingabe $(X_1, \ldots, X_n)$, verschiedene Werte annehmen und darf in bestimmten Fällen auch Null sein.

c) Was gilt für das Verhältnis zwischen $H(X_1 \ldots X_n)$ und $H(Z_1 \ldots Z_K, K)$? Begründen Sie!

d) Beweisen Sie nun, dass aus $X_1 \ldots X_n$ im Mittel nicht mehr als $n \cdot h(p)$ faire Münzwürfe erzeugt werden können, also dass $E(K) \leq n \cdot h(p)$. $E(K)$ bezeichnet den Erwartungswert von K.

e) Geben Sie die Funktion f für Eingabefolgen der Länge $n = 2$ an. Vermeiden Sie dabei die triviale Lösung, bei welcher f für alle Eingaben eine leere Folge ausgibt.

Aufgabe 3: Markov-Prozess *20 (4/2/1/7/1/5) Punkte*

Gegeben sei das unten abgebildete Schachbrett mit 3×3 Feldern.

E	S	E
S	M	S
E	S	E

Darauf werde auf einem beliebigen Feld ein Läufer gestartet. Dieser kann sich mit jedem Zug **diagonal** um ein oder zwei Felder weiterbewegen. Wir wollen die möglichen Positionen des Läufers als Markov-Prozess modellieren. Dabei interessiert uns nicht das genaue Feld, auf dem sich der Läufer befindet, sondern nur die drei Zustände:

- E - Der Läufer befindet sich auf einem Eckfeld.
- S - Der Läufer befindet sich auf einem Seitenfeld.
- M - Der Läufer befindet sich im mittleren Feld.

a) Zeichnen Sie den Zustandsgraphen mit den Zuständen als Knoten und den Überganswahrscheinlichkeiten als Kanten.

b) Der Markov-Prozess kann durch das lineare Gleichungssystem

$$\begin{bmatrix} p_E^{(i+1)} \\ p_M^{(i+1)} \\ p_S^{(i+1)} \end{bmatrix} = M \cdot \begin{bmatrix} p_E^{(i)} \\ p_M^{(i)} \\ p_S^{(i)} \end{bmatrix}$$

beschrieben werden. $p_X^{(i)}$ beschreibt dabei die Wahrscheinlichkeit des Zustands X zum Zeitpunkt i, M ist die Übergangsmatrix. Geben Sie M für den obigen Prozess an.

c) Der Läufer wird nun auf ein Startfeld gesetzt, welches gleichverteilt aus den 9 Feldern des Schachbretts ausgewählt wird. Geben Sie den entsprechenden Startvektor für das obige Gleichungssystem an.

d) Berechnen Sie die stationären Zustandswahrscheinlichkeiten, wenn der Läufer gemäss dem oben gewählten Startvektor gestartet wird.

e) Ist der Markov-Prozess ergodisch? Begründen Sie!

f) Sei $X_0 \to X_1 \to \ldots$ eine allgemeine, ergodische Markov-Kette erster Ordnung. Man versucht nun, aus dem momentanen Zustand X_i Informationen über den Startzustand X_0 zu erhalten. Zeigen Sie, dass die Unsicherheit in dieser Information grösser wird oder gleich bleibt, je weiter i voranschreitet.

Aufgabe 4: Quellencodierung/Kompression *40 (2/4/4/8/6/6/8/2) Punkte*

a) Wann heisst ein Code optimal?

b) Eine Quelle ist beschrieben durch die folgende Verteilung von 3-Bit-Blöcken:

q	000	001	010	011	100	101	110	111
P(q)	10/64	7/64	6/64	14/64	4/64	11/64	8/64	4/64

Konstruieren Sie einen Huffman-Code für die Quelle.

Codieren Sie mit Ihrem Code die Zeichenfolge
0 0 1 0 1 0 0 0 1 1 1 0 1 1 0 1 1 1 1 0 0 1 0 1 0 1 0 0 1 1 0 0 0.

c) Eine Quelle sei beschrieben durch die Zufallsvariable Q:

q	1	2	3	4
P(q)	1/2	1/4	1/8	1/8

Für diese Quelle ist ein präfixfreier Code C definiert als:

q	1	2	3	4
C(q)	0	11	100	101

Zeigen Sie: C ist ein optimaler Code für Q.

d) Arithmetische Codierung
Sei x ein Wort, das mit Wahrscheinlichkeit $P(x)$ auftritt. Zeigen Sie: Es existiert ein binäres Codewort c für x mit der Länge

$$l(c) = \left\lceil \log \frac{1}{P(x)} \right\rceil.$$

Tip: Überlegen Sie zuerst, welche Werte die möglichen Codeworte der Länge $k = l(c)$ annehmen können. Zeigen Sie dann, dass in jedem Intervall $I_x = [u(x), o(x))$ mit $o(x) - u(x) = P(x)$ mindestens eines dieser Codeworte liegen muss.

e) Codieren Sie den folgenden Bitstring mit dem original Lempel-Ziv-Algorithmus, so wie er in der Vorlesung behandelt wurde. Verwenden Sie 3 Bits zur Codierung der Präfixposition.

`0 0 1 0 0 1 1 1 0 1 0 0 1 1 0 1 0 1`

f) Decodieren Sie den folgenden Bitstring mit dem original Lempel-Ziv-Algorithmus. Es wurden 3 Bits benutzt, um die Position des Präfix zu codieren.

`0 0 0 1 0 0 1 1 0 0 1 0 0 0 0 0 0 1 1 0 1 0 1 1 1 0 0 0 1 0 0 1`

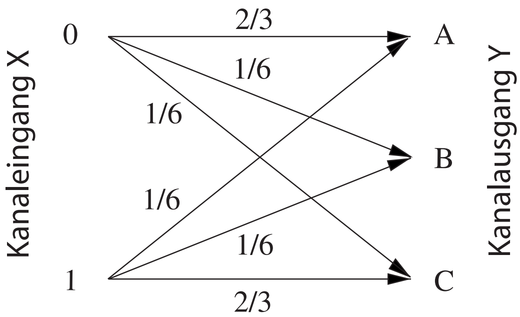
g) Erweitern Sie den Lempel-Ziv-Algorithmus so, dass die Anzahl der Bits zur Codierung des Präfix dynamisch bestimmt wird. Wie wird die benötigte Länge des Präfix bestimmt? Tip: Es wird nur noch ein Pass über die Daten benötigt, um einen String zu kodieren.

h) Was ist der Vorteil des Lempel-Ziv-Verfahrens im Vergleich zur Huffman-Codierung?

Aufgabe 5: Kanalcodierung *37 (2/7/8/7/7/6) Punkte*

Bemerkungen:
Alle Teilaufgaben dieser Aufgabe können unabhängig voneinander gelöst werden.
Um Punkte für eine Aufgabe zu bekommen, muss der Lösungsweg ersichtlich sein!

Alice und Bob verabreden sich jeweils heimlich zum Mittagessen in der Hauptmensa, der Infobar, der Clausiusbar oder der Gloriabar. Dazu steht ihnen folgender Kanal zur Verfügung:



Als Informationswörter sollen zwei Bits verwendet werden: 00 für die Hauptmensa, 01 für die Infobar, 10 für die Clausiusbar und 11 für die Gloriabar. Um die Übertragung sicherer zu machen, wird folgender linearer Code benutzt: 0000 für die Hauptmensa, 1101 für die Infobar, 1011 für die Clausiusbar und 0110 für die Gloriabar.

a) Definieren Sie mit Worten in einem einzigen Satz den Begriff "Kapazität eines Kanals".

b) Berechnen Sie die Kapazität obigen Kanals. Geben Sie die Lösung in der H([p_1,...,p_k])-Notation an. Sie müssen die Lösung nicht numerisch ausrechnen!

c) Nehmen Sie an, dass Bob folgenden Output empfängt: B A B C.

   c.1) Wenn Sie den Maximum-Likelihood (ML) Decoder verwenden, in welche Mensa wird Bob gehen? Stellen Sie dafür eine Wahrscheinlichkeitstabelle auf, die angibt, mit welcher Wahrscheinlichkeit der Output mit den Codewörtern übereinstimmt.

   c.2) Bob kennt Alice schon länger und weiss, dass sie mit einer Wahrscheinlichkeit von 0.5 in die Hauptmensa, mit 0.2 in die Infobar, mit 0.1 in die Clausiusbar und mit 0.2 in die Gloriabar gehen möchte. Wenn Bob den Minimum-Error (ME) Decoder benutzt, wohin wird er dann gehen?

d) Berechnen Sie die Generator- und die Parity-Check-Matrix für den oben gegebenen linearen Code, und berechnen Sie die Minimaldistanz.

e) Wir benutzen nun einen neuen linearen Code sowie folgende Generator- und Parity-Check-matrizen. Achtung, das sind *nicht* die gesuchten Matrizen von Teilaufgabe d).

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

   Entwerfen Sie einen Syndromdecoder für den gegeben Code.
   Nehmen Sie weiter an, dass Bob folgenden Code von Alice erhält: 11100. In welche Mensa wird Bob gehen, unter der Annahme, dass alle Möglichkeiten gleich wahrscheinlich sind?

f) Bilden Sie für einen [7,4]-Hammingcode die Parity-Check- und die Generator-Matrix. Wieviele Fehler können mit diesem Code detektiert und wieviele korrigiert werden? Begründen Sie!