Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

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

Departement Informatik
15. 3. 2006

Informationstheorie

Frühling 2006

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	16		
2	6		
3	16		
4	6		
5	12		
6	15		
7	10		
8	6		
9	14		
10	19		
Total	120		Note:

Aufgabe 1: Entropie I *16 (2/2/2/2/6/2) Punkte*

Die gemeinsame Verteilung zweier Zufallsvariablen X und Y sei gegeben als

P_{XY}		Y			
		1	2	3	4
	1	1/8	0	1/16	1/16
X	2	0	1/16	1/16	1/8
	3	1/16	1/8	0	1/16
	4	1/16	1/16	1/8	0

a) Bestimmen Sie P_X und P_Y sowie die Entropien H(X) und H(Y).

b) Zeigen oder widerlegen Sie: X und Y sind unabhängig.

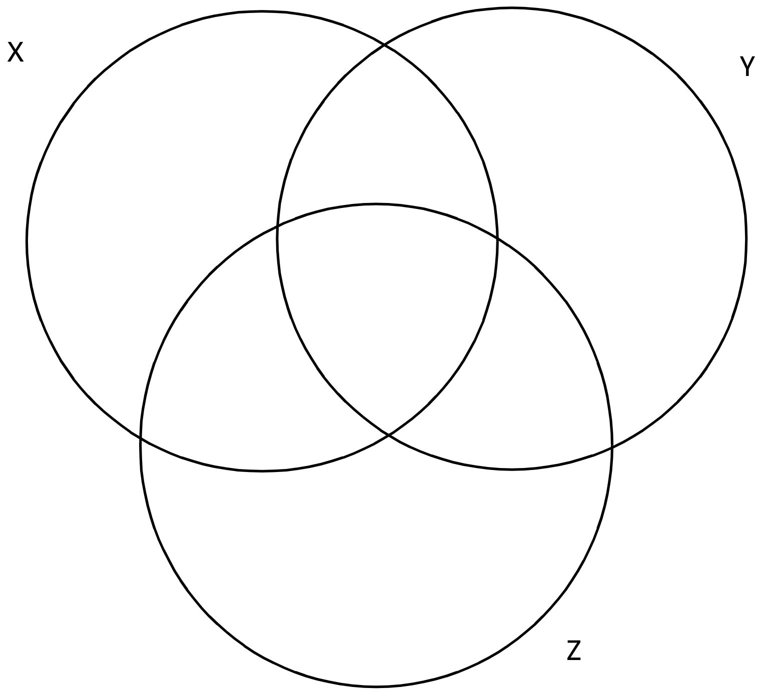
c) Bestimmen Sie $P_{X|Y}$ und $P_{Y|X}$ sowie die Entropien H(X|Y) und H(Y|X).

Sei eine Zufallsvariable Z gegeben als $Z = \begin{cases} 1 \,\|\, X & \text{falls } Y \text{ gerade.} \\ 0 \,\|\, X & \text{falls } Y \text{ ungerade.} \end{cases}$
Das Symbol $\|$ stellt die Konkatenation dar.

d) Benennen Sie alle Felder im unten stehenden Entropiediagramm.

e) Tragen Sie Zahlenwerte für alle Felder in das Entropiediagramm ein.
Tipp: Berechnen Sie zuerst I(Y;Z|X) und tragen Sie alle Werte ein, die Null sind.

f) Ist X -> Y -> Z eine Markov-Kette? Begründen Sie Ihre Antwort.



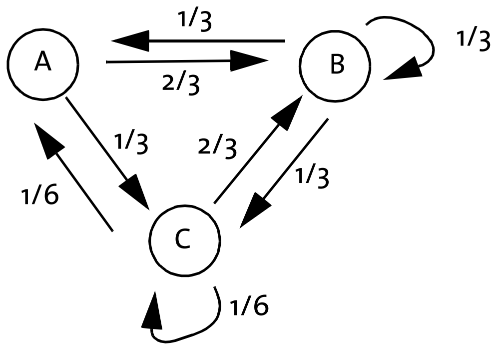
Aufgabe 2: Entropie II *6 Punkte*

Seien X, Y, Z Zufallsvariablen und f, g beliebige Funktionen. Setzen Sie jeweils die präziseste allgemeingültige Vergleichsbeziehung ($<, >, \geq, \leq, =, \neq$) für '~' ein. Schreiben Sie '?', wenn keine Beziehung allgemeingültig ist.

- $H(X) \sim H(f(X))$
- $H(XY) \sim H(X) + H(Y)$
- $H(f(X)f(Y)) \sim H(XY) - H(XY \mid f(X)f(Y))$
- $I(X ; f(X)) \sim I(Y ; f(Y))$
- $I(f(X) ; g(Y)) \sim I(X ; Y)$
- $I(f(X) ; f(Y)) \sim I(X ; Y)$

Aufgabe 3: Markov-Prozess *16 (2/8/2/4) Punkte*

Ein Spielautomat hat 3 mögliche Zustände A, B, und C. Nach jedem Spiel wechselt er den Zustand zufällig entsprechend den Wahrscheinlichkeiten aus folgendem Diagramm.



In Zustand A gibt der Automat das Doppelte des Einsatzes zurück. In Zustand B behält er die Hälfte des Einsatzes ein, und in Zustand C behält er 90% des Einsatzes ein.

a) Stellen Sie die Zustandsübergangsmatrix auf.

b) Wenn man sehr (unendlich) lange spielt und in jeder Runde denselben Betrag einsetzt, um welchen Faktor hat man das ingesamt eingesetzte Geld vermehrt oder verringert?

c) Der Automat befinde sich im Zustand B. Mit welcher Wahrscheinlichkeit hat der Spieler im vorangegangenen Spiel etwas gewonnen?

d) Die stationären Wahrscheinlichkeiten der Zustände des gegebenen Automaten sind unabhängig vom Ausgangszustand. Ändern Sie die Übergangswahrscheinlichkeiten so ab, dass die stationären Wahrscheinlichkeiten vom Ausgangszustand abhängen.

Aufgabe 4: Codierungsverfahren *6 Punkte*

Kreuzen Sie an, ob folgende Aussagen richtig oder falsch sind:

	richtig	falsch
a) Das Codierungsverfahren für ganze Zahlen eignet sich zur Komprimierung	☐	☐
b) Intervalllängen-Codierung ist ein universelles Datenkompressionsverfahren	☐	☐
c) Arithmetische Codierung ist asymptotisch optimal	☐	☐
d) Intervalllängen-Codierung ist asymptotisch optimal	☐	☐
e) Ein Code, der die Kraft'sche Ungleichung erfüllt, ist eindeutig decodierbar	☐	☐
f) Suffixfreie Codes erfüllen die Kraft'sche Ungleichung	☐	☐

Aufgabe 5: Shannon-Fano-Codierung *12 (2/5/5) Punkte*

a) Die Shannon-Fano-Codierung ist nur suboptimal. Weshalb? Begründen Sie anhand des Codierungsalgorithmus.

b) Geben Sie einen Algorithmus an, um aus einem beliebigen String mit gegebener Wahrscheinlichkeitsverteilung mittels Shannon-Fano-Codierung einen *ternären* Code zu erzeugen.

c) Gegeben sei der folgende String: "HAFFEGABBCEEAFAGGAAEHAFA". Finden Sie einen ternären Code für eine kürzeste Shannon-Fano-Codierung des obigen Strings auf dem Alphabet {A..H}. Schätzen Sie dazu die Wahrscheinlichkeiten der Zeichen des Eingabealphabets anhand des obigen Strings.

Aufgabe 6: Quellencodierung *15 (4/2/6/3) Punkte*

Aus einem Alphabet {A..E} erzeugt eine Quelle Q einen String wie folgt: Zuerst wird ein Zeichen aus X = {A, B, C} gewählt mit folgender Wahrscheinlichkeitsverteilung: $p_X(A) = 1/4$, $p_X(B) = 1/4$, $p_X(C) = 1/2$. Unabhängig davon wird anschliessend ein Zeichen aus Y = {D, E} gewählt mit $p_Y(D) = 1/8$, $p_Y(E) = 7/8$. Diese zwei Schritte werden beliebig oft wiederholt.

Anmerkung: Sie können für die Berechnungen die binäre Entropiefunktion h(.) verwenden.

a) Berechnen Sie die Quellen-Entropie (pro Zeichen) von Q.

b) Finden Sie ein optimale binäre Codierung für Q.

c) Finden Sie eine optimale binäre Codierung für Q, wenn Blockcodes der Länge 2 benutzt werden, und berechnen Sie die Coderedundanz.

d) Gibt es einen eindeutig decodierbaren *ternären* Code mit den folgenden Codewortlängen für Blockcodes der Länge 2: 3, 3, 3, 2, 2, 1, 1? Begründen Sie Ihre Antwort!

Aufgabe 7: Komprimierung *10 (5/2/3) Punkte*

Ein String wird mit folgendem Algorithmus codiert: Jedes Zeichen führt einen Zähler mit, der anfänglich auf 0 gesetzt ist. Solange es benachbarte Paare von Zeichen gibt, bei denen das Linke lexikographisch grösser ist als das Rechte, vertauschen wir die zwei Zeichen und addieren eins zum Zähler des Zeichens, das nach rechts gewandert ist, und -1 zum Zeichen, das nach links gewandert ist.

Im Beispiel (siehe unten stehende Abbildung) beginnen wir mit AABCBA als Input und erhalten W=0,0,-3,1,0,2 als Output. Zusätzlich werden auch noch die Anzahl der einzelnen Zeichen gespeichert, also in diesem Beispiel A=3, B=2, und C=1.

1.	A	A	B	C	B	A
	0	0	0	0	0	0
2.	A	A	B	**B**	**C**	A
	0	0	0	**−1**	**1**	0
3.	A	A	B	B	**A**	**C**
	0	0	0	−1	**−1**	**2**
4.	A	A	B	**A**	**B**	C
	0	0	0	**−2**	**0**	2
5.	A	A	**A**	**B**	B	C
	0	0	**−3**	**1**	0	2

a) Sie erhalten folgenden Output: A = 6, B= 2, C = 2, W=0,-1,-1,-1,-3,-4,5,2,2,1. Beschreiben Sie kurz einen möglichst effizienten Algorithmus zur Decodierung, und bestimmen Sie hiermit den Input-String.

b) Wie können Sie den Output so verbessern, dass weniger Redundanz gespeichert wird? Geben Sie den verbesserten Output für die Teilaufgabe a) aus.
Tipp: Überlegen Sie sich, ob die Codierung in W für alle Zeichen des Inputalphabets gespeichert werden muss.

c) Ist dieses Kompressionsverfahren geeignet für die Praxis? Begründen Sie!

Aufgabe 8: Codierung fehlerbehafteter Kanäle *6 (2/2/2) Punkte*

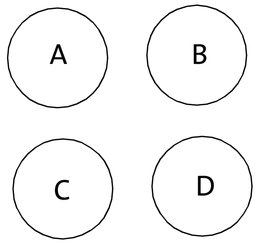
a) In welcher Reihenfolge werden Codierung zur Fehlerkorrektur und Codierung zur Kompression bei der Übertragung über einen fehlerbehafteten Kanal mit beschränkter Bandbreite sinnvollerweise angewandt? Begründen Sie Ihre Antwort.

b) Nennen Sie je eine praktische Anwendung, wo I) Fehlerkorrektur durch Wiederholung verwendet wird oder II) prinzipbedingt durch Rekonstruktion (Forward-Error-Correction) erfolgen muss.

c) Unter welchen Bedingungen werden im Kontext der Fehlerkorrektur das Minimum-Error-Verfahren (ME) oder das Maximum-Likelihood-Verfahren (ML) angewandt? Welche Wahrscheinlichkeitsgrössen werden hierbei jeweils maximiert? Definieren Sie alle Variablen.

Aufgabe 9: Kanalmodellierung und Kapazität *14 (4/5/3/2) Punkte*

Um Informationen unerkannt zu übertragen, treffen sich zwei Agenten in einem Pub mit vier in einer 2 x 2 Matrix angeordneten Dartscheiben.



Mit 26.6% Wahrscheinlichkeit treffen sie die gewünschte Zielscheibe, die jeweils ein Symbol (A, B, C oder D) repräsentiert. Mit je 26.6% Wahrscheinlichkeit treffen sie stattdessen eine der beiden direkt horizontal oder vertikal benachbarten Scheiben oder mit 20% Wahrscheinlichkeit die Wand. Es wird angenommen, dass ein Pfeil in der Wand keine Informationen über das ursprüngliche Ziel innerhalb dieser Dartscheibenanlage mehr verrät.

a) Stellen Sie diesen diskreten, gedächtnisfreien Kanal in unserer üblichen graphischen Notation dar!

b) Wie gross ist die Kapazität C_1 des Kanals? Begründen Sie.
Logarithmen und die Entropiefunktion H(.) dürfen Sie stehen lassen.

c) Wir nehmen für diese Teilaufgabe an, eine analoge Dartscheibenanlage befinde sich in einem anderen Raum. Die Agenten wählen nun vor jeder Symbolübertragung zusätzlich einen der Räume. Wie gross wird die Kapazität C_2 des neuen Kanals?

d) Angenommen die Agenten können aus dem Gang gleichzeitig in beide Räume je einen Pfeil mit den oben genannten Trefferquoten werfen. Wie gross ist die Kapazität C_3 dieses Aufbaus?

Aufgabe 10: Hamming-Codes *19 (3/4/3/4/1/2/2) Punkte*

a) Generieren Sie für r = 2 einen Hamming-Code und geben Sie dessen systematische Generatormatrix und Parity-Check-Matrix an!

b) Leiten Sie die Minimaldistanz des in Teilaufgabe a) konstruierten Codes mit zwei verschiedenen Fakten her, die bei Hamming-Codes gelten.
Wieviele Fehler können bei diesem Code erkannt, wieviele korrigiert werden?

c) Erklären Sie intuitiv, was der resultierende Hamming-Code bei der Codierung macht. Wieviele Kontrollbits weist der Code auf? Wie gross ist seine Rate?

d) Entwerfen Sie einen Syndromdecoder für den in Teilaufgabe a) konstruierten Code durch bestimmen der Fehlermuster aller Syndrome!
Decodieren Sie hiermit die empfangenen Codeworte 101 und 011.

e) Benötigen wir in dem Beispiel von Teilaufgabe d) wirklich eine vollständig tabellierte Syndromdecodierung, oder finden Sie eine einfachere und effizientere Korrekturvorschrift?

f) Sie möchten Daten über einen Kanal senden, der eine hohe Fehlerrate aufweist. Sie haben einen Hamming-Code oder einen dualen Hamming-Code zur Auswahl. Welchen sollten Sie wählen? Begründen Sie.

g) Hamming-Codes gehören bekanntlich zu den linearen Codes. Wie verhält es sich mit den Polynomevaluationscodes? Begründen Sie anhand der Definition linearer Codes.