Fakultät für Informatik

Hochschule **Rosenheim**
University of Applied Sciences

Prüfung	**WS 2012/13**
Fach:	Grundlagen der Informatik 1
Prüfer:	Prof. Dr. J. Schmidt
Prüfung:	28.1.2013

90 Minuten. Hilfsmittel: alle Unterlagen außer Laptop, Handy, u.ä.
Insgesamt sind 90 Punkte zu erreichen. Die Punktzahl gibt damit auch einen Anhaltspunkt für die Bearbeitungszeit.
Sollten Ihrer Meinung nach Angaben in der Aufgabenbeschreibung fehlen, machen Sie sinnvolle Annahmen und dokumentieren Sie diese.
Der Berechnungsweg muss ersichtlich sein.
Die Seiten dürfen nicht getrennt werden.
Konzeptpapier muss (mit Namen versehen) mit abgegeben werden.

Aufgabe	1	2	3	4	5	6	7	8	ges.
Punkte									

Note:

Name: ______________________________ **Matrikelnr.:**________________

Aufgabe 1: Zahlendarstellung (20 Punkte)

a) Geben Sie die Zahl 814 im System zur Basis Fünf an.

$814_{dez} = 11224_{fünf}$

b) Rechnen Sie die Zahl $101_{(25)}$ vom System zur Basis 25 ins System zur Basis 5 um.

Umrechnung: aus einer Ziffer werden 2
$101_{25} = 10001_5$

c) Führen Sie die Rechenoperation 10.0625 – 111.9375 in binärer Arithmetik unter Verwendung des Zweierkomplements (mit 8 Vorkommastellen) aus und rechnen Sie das Ergebnis in dezimale, oktale und hexadezimale Form um!

00001010.0001	10.0625
01101111.1111	111.9375
10010000.0000	Stellenkomplement von 111.9375
10010000.0001	Zweierkomplement
00001010.0001	10.0625
10011010.0010	Summe
01100101.1101	Stellenkomplement Summe
01100101.1110	Zweierkomplement

$-101.875_{dez} = -145.7_{okt} = -65,E_{hex}$

d) Geben Sie $-8.012225 \cdot 10^4$ als 32-Bit Gleitpunktzahl nach IEEE-Format sowohl in binärer Form als auch in hexadezimaler Form an.

$-8.012225 \cdot 10^4 = -80122{,}25$
Vorkommastellen:
$80122_{dez} = 138FA_{16}$
Nachkommastellen:
$0{,}25 = 0{,}4_{16}$
$\rightarrow 138FA{,}4_{16} =$ $0001\ 0011\ 1000\ 1111\ 1010\ ,\ 01_2$
Normalform: $1,\ 0011\ 1000\ 1111\ 1010\ 01_2 \cdot 2^{16}$
$\rightarrow$ e = 16, c = 16 + 127 = 143 = 10001111 Exponent
Vorzeichen = 1 (negativ)
Mantisse: 0011 1000 1111 1010 01 (führende 1 fehlt)
Ergebnis:
$-8.012225 \cdot 10^4$ = 1 10001111 001110001111101001 00000
= 1100 0111 1001 1100 0111 1101 0010 0000
= C7 9C 7D 20

e) Dividieren Sie die Gleitpunktzahl aus der vorhergehenden Teilaufgabe durch vier und geben Sie das Ergebnis nach IEEE-Format in binärer Form an.

Exponent anpassen (2 subtrahieren): 10001111 → 10001101
Zahl aus (d): 1 10001111 001110001111101001 00000
Zahl / 4: 1 10001101 001110001111101001 00000

Aufgabe 2: Codierung (15 Punkte)
Gegeben sei eine Nachrichtenquelle, die das folgende tabellierte Alphabet mit den Zeichen $\{x_i\}$ und den zugehörigen Auftrittswahrscheinlichkeiten $\{p_i\}$ sendet.

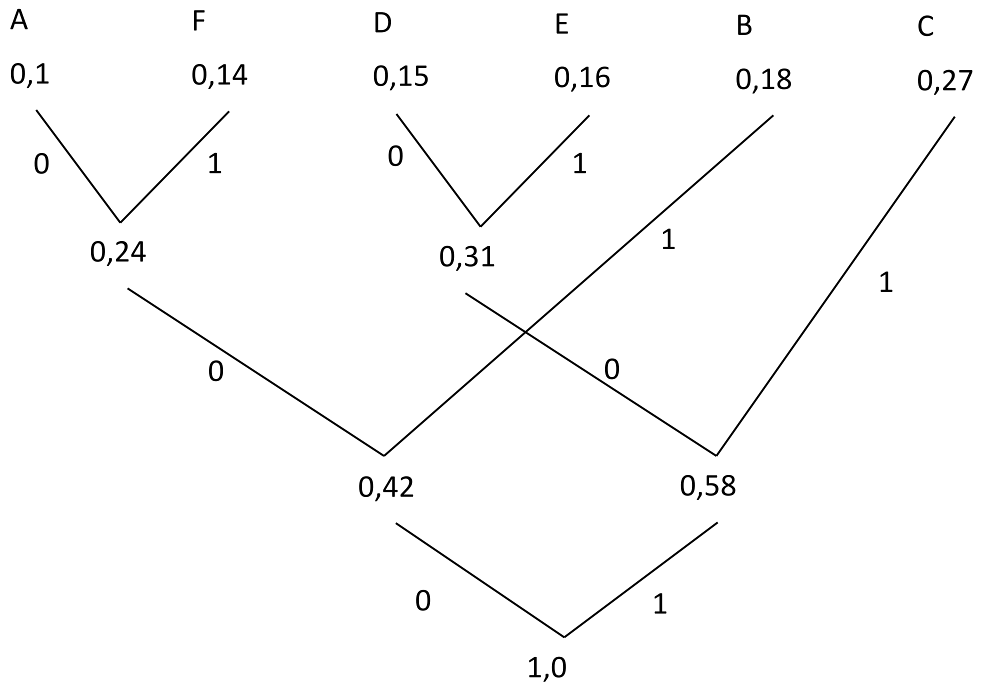
x_i	p_i	I_i	l_i	Code-Wörter
A	0.1			
B	0.18			
C	0.27			
D	0.15			
E	0.16			
F	0.14			

a) Berechnen Sie die Informationsgehalte I_i für das Alphabet und tragen Sie die Ergebnisse (mit 2 Nachkommastellen) in die oben stehende Tabelle ein. Berechnen Sie daraus die Entropie.

$$H = \sum p_i \cdot ld(1/p_i) = 0.1 \cdot 3.32 + 0.18 \cdot 2.47 + 0.27 \cdot 1{,}89 + 0.15 \cdot 2.74 + 0.16 \cdot 2.64 + 0.14 \cdot 2.84 = 2.5179 \text{ [Bit/Zeichen]}$$

x_i	p_i	I_i	l_i	Code-Wörter
A	0.1	3,32	3	000
B	0.18	2,47	2	01
C	0.27	1,89	2	11
D	0.15	2,74	3	100
E	0.16	2,64	3	101
F	0.14	2,84	3	001

b) Bilden Sie den optimalen Binär-Code für das Alphabet mit Hilfe des Huffman-Verfahrens, zeichnen Sie den zugehörigen Code-Baum und tragen Sie die Wortlängen l_i und die Code-Wörter in die obige Tabelle ein.



c) Berechnen Sie nun die mittlere Wortlänge und die Redundanz für den in (b) ermittelten Code.

$L = \sum p_i l_i$ $= 0.1 \cdot 3 + 0.18 \cdot 2 + 0.27 \cdot 2 + 0.15 \cdot 3 + 0.16 \cdot 3 + 0.14 \cdot 3$
$= 2.55$ [Bit/Zeichen]

$R = L - H$ $= 2.55 - 2.5179$
$= 0.0321$ [Bit/Zeichen]

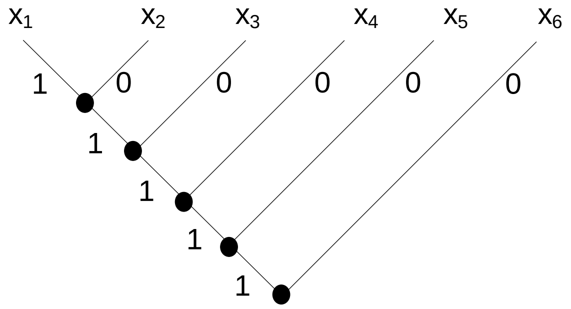
d) Geben Sie die Wortlänge des kürzesten Block-Codes für das Alphabet an. Mit welchem Kompressionsfaktor kann man unter Verwendung des Huffman-Codes die Länge eines mit dem Alphabet formulierten Textes im Vergleich zu dem kürzesten Block-Code verringern?

$L_{Block} = 3$
Kompressionsfaktor $k = L_{Huff}/L_{Block} = 2.55/3 = 0.85$

Aufgabe 3: Codierung (7 Punkte)

a) Es sei ein Alphabet mit n Zeichen gegeben. Für die nach Größe geordneten Auftrittswahrscheinlichkeiten p_1 bis p_n soll gelten: $\sum_{i=1}^{k-1} p_i < p_k$ für alle k von 1 bis n.
Wie sieht in diesem Fall der entstehende Code-Baum aus?
Wie lang ist die Wortlänge für das Zeichen mit dem längsten Code-Wort, wie lang ist das kürzeste Code-Wort?

Das Codewort des längsten Wortes hat die Länge n-1. Dies folgt aus dem sich im Extremfall ergebenden entarteten Huffman-Baum, der nachfolgend für den Fall n=6 angegeben ist. Das längste Codewort 11111 für das Zeichen x_1 hat also die Länge 5.
Das kürzeste hat immer Länge 1.



Ordnet man die Auftrittswahrscheinlichkeiten der Größe nach, so erhält man die oben stehende Bedingung dafür, dass dieser Extremfall eintritt.

b) Warum ist die Kompressionsleistung der arithmetischen Codierung im Allgemeinen etwas besser als die des Huffman-Verfahrens?

Beim Huffman-Verfahren werden Einzelzeichen binär codiert. Die codierten Zeichen müssen daher eine ganzzahlige Anzahl von Bits aufweisen. Bei der arithmetischen Codierung wird dagegen der gesamte Text mit einer bestimmten Anzahl von Bits codiert, so dass sich pro Zeichen auch eine gebrochene Wortlänge ergeben kann. Daraus resultiert oft eine etwas stärkere Redundanzminimierung und damit eine bessere Kompressionsleistung, als beim Huffman-Verfahren.

Aufgabe 4: Verschlüsselung (10 Punkte)

Beim RSA-Verfahren wird für jeden Teilnehmer ein öffentlicher Schlüssel im Schlüsselverzeichnis veröffentlicht. Dieser besteht aus einer Zahl n, die das Produkt zweier großer Primzahlen p und q ist, sowie einem Exponenten c. Jeder Teilnehmer erhält ferner einen geheimen Schlüssel d.

a) Es seien p = 7 und q = 19. Berechnen Sie daraus n und den Wert der eulerschen Funktion ϕ(n).
b) Warum kommt c = 10 als Teil des öffentlichen Schlüssels nicht in Frage?
   Zeigen Sie, dass c = 25 als Teil des öffentlichen Schlüssels geeignet ist.
c) Alice verwendet c = 25 als Teil des öffentlichen Schlüssels.
   Berechnen Sie ihren geheimen Schlüssel d.
d) Alice empfängt eine aus einem einzigen Zeichen bestehende verschlüsselte Nachricht: 20.
   Wie lautet die Nachricht im Klartext?
   Die Rechenschritte der modularen Exponentiation müssen erkennbar sein.

a) Man erhält $n=7\cdot 19=133$ und $\Phi(n)=(7-1)\cdot(19-1)=108$.

b) Ein gültiger Schlüssel $1 < c < \Phi(n)$ darf mit $\Phi(n)$ keine gemeinsamen Teiler haben. Da $c=10=2\cdot 5$ den gemeinsamen Teiler 2 mit $\Phi(n)=108=2*2*27$ hat, ist es als Schlüssel nicht geeignet.
Da c=25 keinen gemeinsamen Teiler mit $\Phi(n)$ hat, ist es als Schlüssel geeignet.

c) Der geheime Schlüssel d ist die modular Inverse von c=25 bzgl. $\Phi(n)=108$. Man erhält sie z.B. als ganzzahlige Lösung von $d=(\Phi(n)\cdot i+1)/c \bmod n$, indem man i mit 1 beginnend hoch zählt.
Mit i=3 findet man:

$$d = (108 \cdot 3 + 1)/25 = 325/25 = 13$$

d) Alice kann nun die Nachricht wie folgt entschlüsseln:
$x = y^d \bmod n = 20^{13} \bmod 133 = ((20^2 * 20)^2)^2\ 20 =$
$((1 * 20)^2)^2\ 20 = (1)^2\ 20 = 20$

Aufgabe 5: Kompression (10 Punkte)
Daten bestehend aus Zeichen des Alphabets A = {B, U,V, Z} wurden mit dem LZW-Verfahren komprimiert. Die initiale Code-Tabelle sieht wie folgt aus: 0 → Z, 1 → U, 2 → B, 3 → V
Dekodieren Sie das Codewort 1 3 4 0 6 4.
Der Rechenweg muss ersichtlich sein, ebenso die vollständige sich ergebende Code-Tabelle!

LZW-Dekompression einer Nachricht

Initialisiere die Code-Tabelle mit den Eingabezeichen
Weise dem Präfix *P* den Leerstring zu
Wiederhole, solange Eingabezeichen vorhanden sind:
- Lies nächstes Eingabezeichen *c*
- Wenn *c* in der Code-Tabelle enthalten ist:
  - Gib den zu *c* gehörenden String aus
  - Setze *k* = erstes Zeichen dieses Strings
  - Trage *Pk* in die Code-Tabelle ein, falls noch nicht drin
  - Setze *P* auf den zu dem Code *c* gehörigen String
- Sonst (Sonderfall):
  - setze *k* = erstes Zeichen von *P*
  - Gib *Pk* aus
  - Trage *Pk* in die Code-Tabelle ein
  - Setze *P=Pk*

Ende der Schleife

Schritt	Code	Eintrag in Code-Tabelle	Ausgabe=Präfix
0	134064	Vorbesetzung	-
1	1	-	U
2	3	UV=4	V
3	4	VU=5	UV
4	0	UVZ=6	Z
5	6	ZU=7	UVZ
6	4	UVZU=8	UV

Code-Tabelle	
0	Z
1	U
2	B
3	V
4	UV
5	VU
6	UVZ
7	ZU
8	UVZU

Aufgabe 6: CRC (7 Punkte)
Zur Absicherung während der Übertragung sollen Daten mit einem CRC-Code versehen werden.
Die (binäre) zu sendende Nachricht lautet: 1100 0110
Als Generatorpolynom wird $x^4 + x + 1$ verwendet.

Wie lautet die zu sendende Nachricht inklusive des angehängten CRC-Codes?

Generator: 10011
k = 4 → 4 Nullen an Nachricht anhängen

```
1100 0110 0000
1001 1
______
 101 11
 100 11
 ______
   1 0010
   1 0011
   ______
        1 0000
        1 0011
        ______
            11 = Rest = CRC
```

zu senden: 1100 0110 0011

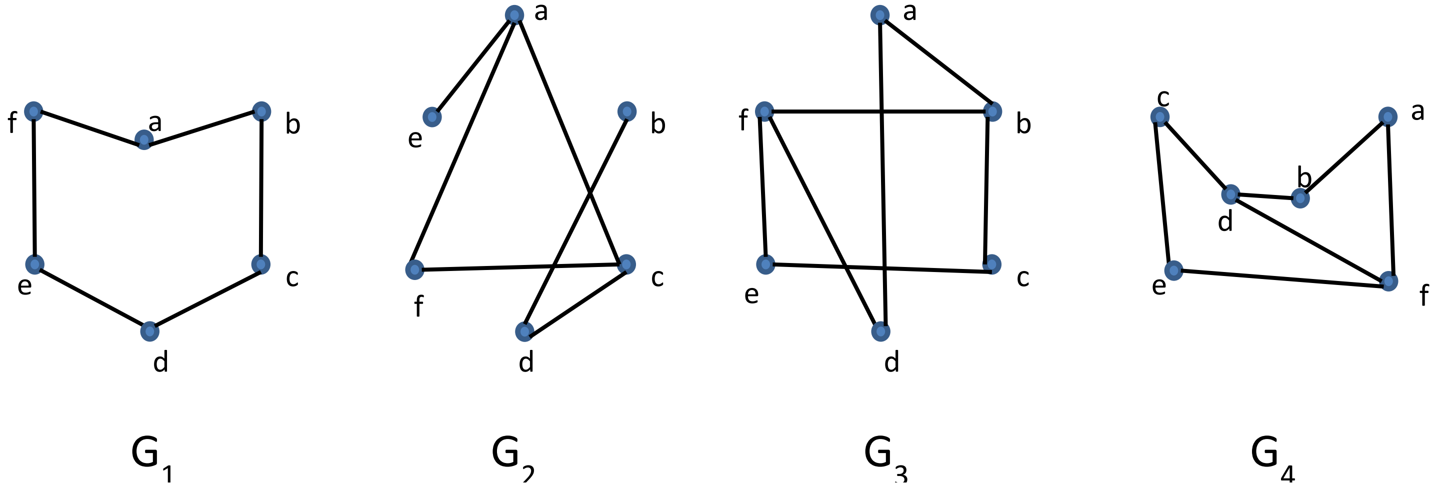
Aufgabe 7: Graphen (9 Punkte)

a) Gegeben ist die Adjazenzmatrix eines gewichteten gerichteten Graphen:

$$A = \begin{pmatrix} 0 & -1 & 2 & 1 \\ 0 & 4 & 0 & 3 \\ -5 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

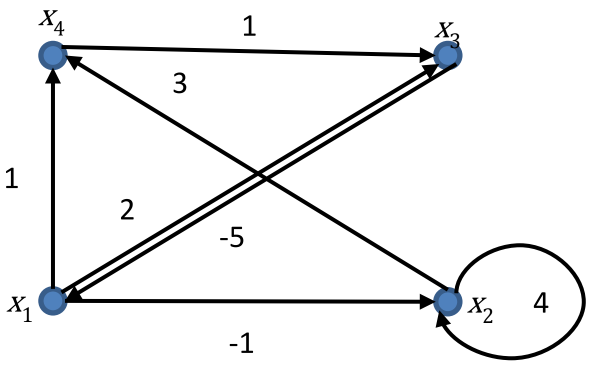
Zeichnen Sie den Graphen!

b) Bestimmen Sie die Gradfolge von jedem der nachfolgend dargestellten Graphen:



c) Sind von den Graphen welche zueinander isomorph? Falls ja: Welche sind dies? Geben Sie die Isomorphieabbildung an!

a)



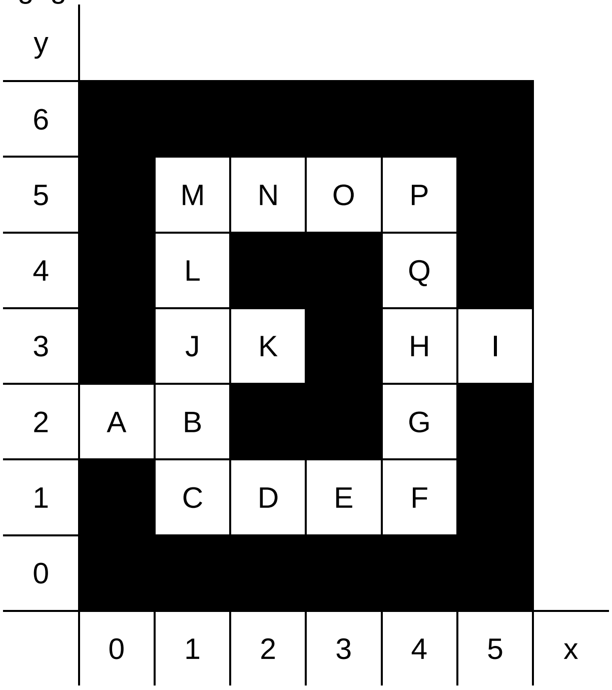
b) Gradfolgen
(2, 2, 2, 2, 2, 2), (1, 1, 2, 2, 3, 3), (2, 2, 2, 2, 3, 3), (2, 2, 2, 2, 3, 3)

c) G3 und G4 sind isomorph: ergibt 2 Rechtecke, mehrere Möglichkeiten zur Isomorphieabb., z.B.:

G3	a b c d e f
G4	a d f b e c

Aufgabe 8: Graphsuche (12 Punkte)

Gegeben ist das folgende Labyrinth. Start ist bei A, Ende bei I. Die freien Felder, auf denen man sich bewegen kann, sind von A bis Q beschriftet. Zusätzlich sind die x- und y-Achsen zur Bestimmung der Koordinaten eines Feldes angegeben.



a) Zeichnen Sie einen Graphen, der das Labyrinth repräsentiert. Jedes Feld ist ein Knoten. Beachten Sie, dass ein Zug von einem Feld zum nächsten nur horizontal bzw. vertikal möglich ist, diagonale Bewegungen sind ausgeschlossen.

b) Mit Hilfe des A*-Algorithmus soll nun ein Weg vom Start A zum Ziel I gefunden werden. Als Heuristik wird der euklidische Abstand d eines Knotens zum Zielknoten I verwendet, also:

$$d = \sqrt{(x_\mathrm{I} - x)^2 + (y_\mathrm{I} - y)^2}$$

Hierbei sind $(x_\mathrm{I}, y_\mathrm{I})$ die Koordinaten des Zielknotens I und (x, y) die Koordinaten des zu bewertenden Knotens.
Die nachfolgende Tabelle enthält für einen Teil der Knoten die bereits berechnete Heuristik. Ergänzen Sie die fehlenden Einträge:

Knoten	***d***	**Knoten**	***d***	**Knoten**	***d***	**Knoten**	***d***
A	5,10	F	2,24	K	3	P	2,24
B	4,12	G		L	4,12	Q	1,41
C	4,47	H		M	4,47		
D		I	0	N			
E	2,83	J		O			

c) Berechnen Sie nun den optimalen Weg vom Start A zum Ziel I mit dem A*-Algorithmus. Geben Sie die sich ergebende Knotenfolge an. Zu beachten ist:

- die Kosten eines Zuges von einem Feld zu einem benachbarten betragen 1
- die Entstehung des Suchbaumes sowie die einzelnen Berechnungsschritte müssen klar erkennbar sein

- geben Sie in jedem Schritt die Bewertung der expandierten Knoten an, diejenigen Knoten, die noch offen sind (also bewertet, aber noch nicht zur Expansion ausgewählt) und den Knoten, der als nächstes zur Expansion ausgewählt wird

a)

```
          K
         /
A – B – J – L – M – N – O – P – Q
    |                           |
    C                           H – I
    |                           |
    D – E – F – G ------------------|
```

b)

Knoten	d	Knoten	d	Knoten	d	Knoten	d
A	5,10	F	2,24	K	3	P	2,24
B	4,12	G	1,41	L	4,12	Q	1,41
C	4,47	H	1	M	4,47		
D	3,61	I	0	N	3,61		
E	2,83	J	4	O	2,83		

c) Werte in Klammer geben die Gesamtkosten an

Puffer (offen)	**bearbeitet**
A (0 + 5,10 = 5,10)	-
B (1 + 4,12 = 5,12)	A
J (2 + 4 = 6), C (2 + 4,47 = 6,47)	B
K (3 + 3 = 6), C (6,47), L (3 + 4,12 = 7,12)	J
C (6,47), L (7,12)	K
D (3 + 3,61 = 6,61), L (7,12)	C
E (4 + 2,83 = 6,83), L (7,12)	D
L (7,12), F (5 + 2,24 = 7,24)	E
F (7,24), M (4 + 4,47 = 8,47)	L
G (6 + 1,41 = 7,41), M (8,47)	F
H (7 + 1 = 8), M (8,47)	G
I (8 + 0 = 8), M (8,47), Q (8 + 1,41 = 9,41)	H
	I → Zielknoten würde expandiert, fertig

Knotenfolge: A, B, C, D, E, F, G, H, I

voraussichtlicher Notenschlüssel:

0-36: 5,0	37 – 45: 4,0	46 – 50: 3,7	51 - 54: 3,3	55 - 59: 3,0	60 - 63: 2,7
	64 – 68: 2,3	69 – 72: 2,0	73 – 77: 1,7	78 – 81: 1,3	82 - 90: 1,0