



Prüfung WS 2016/17

Studiengang: INF-B

Fach: Grundlagen der Informatik 1

Prüfer: Prof. Dr. J. Schmidt

Prüfung: 26.1.2017

90 Minuten. Hilfsmittel: alle schriftlichen Unterlagen, Taschenrechner, **kein** Laptop, Smartphone, 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	ges.
Punkte							

Note:

Name: _____

Matrikelnr.: _____

Aufgabe 1: Codierung (16 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
A	0,09		
B	0,17		
C	0,33		
D	0,06		
E	0,21		
F	0,02		
G	0,01		
H	0,11		

- 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.
- Bilden Sie den einen Binärcode für das Alphabet mit Hilfe des Huffman-Verfahrens und tragen Sie die sich ergebenden Wortlängen l_i in die obige Tabelle ein.
- Berechnen Sie nun die mittlere Wortlänge und die Redundanz für den in (b) ermittelten Code.
- 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?

Aufgabe 2: Zahlendarstellung (15 Punkte)

- Geben Sie die Zahl 5849_{10} im Stellenwertsystem zur Basis 13 an.
- Zeigen Sie: Der Bruch $\frac{42}{70}$ (im Dezimalsystem) ist im Hexadezimalsystem nicht exakt als gebrochene Zahl darstellbar.
- Führen Sie die Rechenoperation $-9 - 47$ in binärer Arithmetik unter Verwendung des Zweierkomplements (mit 8 Stellen) aus.
Geben Sie Ihr Ergebnis (d.h. die Summe im Zweierkomplement interpretiert als vorzeichenlose Binärzahl) in dezimaler, oktaler und hexadezimaler Form an!
- Gegeben sei die der Speicherinhalt von 4 Byte in hexadezimaler Darstellung: 46 1C A1 80. Dieser soll als binäre 32-Bit Gleitpunktzahl nach IEEE-Format interpretiert werden. Geben Sie die Gleitpunktzahl in der üblichen dezimalen Schreibweise an.
- Wie sieht die Gleitpunktzahl aus der vorhergehenden Teilaufgabe in hexadezimaler Form aus, wenn sie mit 16 multipliziert wird?

Aufgabe 3: Hamming-Code (12 Punkte)

Zur Absicherung während der Übertragung sollen Daten mit einem fehlerkorrigierenden (15, 11) Hamming-Code gesichert werden.

- Codieren Sie die Zahl 999_{10} mit diesem Code. Geben Sie das zu sendende Codewort in binärer Form an.
- Bei der Übertragung kippen die Bits Nummer 1 und 3 (gezählt von rechts, beginnend bei 1). Wie lauten die decodierten Daten?
- Welche Hamming-Distanz hat dieser Code?

Aufgabe 4: Verschlüsselung – RSA (15 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 $p = 29$ und $q = 17$. Berechnen Sie daraus n und den Wert der eulerschen Funktion $\phi(n)$.
- b) Zeigen Sie, dass $c = 13$ als Teil des öffentlichen Schlüssels geeignet ist.
- c) Alice verwendet $c = 13$ als Teil des öffentlichen Schlüssels. Bestimmen Sie den geheimen Schlüssel d .
- d) Ist $q = 17$ eine sichere Primzahl?
- e) Verschlüsseln Sie den Klartext gegeben durch die Zahl 2.
- f) Als Angreifer haben Sie eine mit RSA verschlüsselte Botschaft abgefangen, nämlich die Zahl 3. Der öffentliche Schlüssel des rechtmäßigen Empfängers lautet $(5, 35)$. Bestimmen Sie den Klartext, indem Sie den Wiederherstellungsexponenten berechnen.

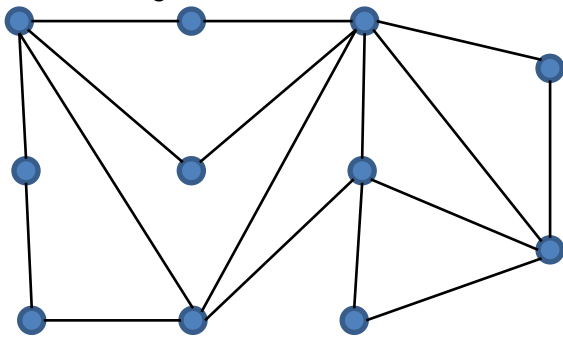
Aufgabe 5: Reed-Solomon Code (16 Punkte)

Zur Reed-Solomon Codierung in dieser Aufgabe wird ein endlicher Körper mit 5 Elementen verwendet, die Länge der (uncodierten) Nachricht sei 2, die Codewortlänge 4.

- a) Kodieren Sie die Nachricht $(3, 2)$.
- b) Wie viele fehlerhafte Stellen sind mit diesem Code korrigierbar?
- c) Empfangen wurde das Codewort $(3, 0, 0, 4)$.
Stellen Sie das zur Decodierung erforderliche Gleichungssystem auf; reduzieren Sie dabei die auftretenden Koeffizienten so weit wie möglich. Das System muss **nicht** gelöst werden!
- d) Nach dem Lösen des Gleichungssystems entstehen folgende Polynome:
 $f(x) = 1 + 2x$
 $g(x) = 2 + 2x + x^2$
Wie lautet die empfangene und decodierte Nachricht?

Aufgabe 6: Verschiedenes (16 Punkte)

Welche der folgenden Aussagen sind richtig bzw. falsch? Kreuzen Sie das entsprechende Feld an. Falsche Antworten geben Punktabzug (wird nicht auf andere Aufgaben übertragen).

Aussage	richtig	falsch
Der ASCII-Code hat eine Hamming-Distanz von 2		
Die Breite des Datenbusses einer CPU legt fest, wie viele Bits parallel ins RAM übertragen werden können		
Mit dem CRC-Generatorpolynom $x^3 + x + 1$ lassen sich alle Bündelfehler der Länge kleiner 3 erkennen		
AES ist ein fehlerkorrigierender Code		
Die Zahl $0,1_{10}$ ist als BCD-Zahl exakt darstellbar, sie lautet $0,0001_{\text{BCD}}$		
<p>Im folgenden Graphen gibt es einen Rundweg, so dass jede Kante genau einmal besucht wird:</p> 		
<p>Die beiden durch die folgenden Adjazenzmatrizen definierten Graphen sind isomorph:</p> $\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$		
<p>Der Knoten C des folgenden Graphen ist ein trennender Knoten:</p> 