Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold

Hausübungen zur Vorlesung

Diskrete Mathematik II

SS 2011

Blatt 6 / 7. Juni 2011 / Abgabe **bis spätestens Dienstag 28. Juni, 09:00 Uhr**

AUFGABE 1:

(a) Bestimmen Sie jeweils die Menge aller Suffixe der folgenden beiden Codes: [6P]
$C_1 = \{11, 001, 101, 110, 0010, 1010, 1100, 1001, 00100, 01000, 10001, 11000, 10100\}$
$C_2 = \{11, 001, 101, 110, 0010, 1010, 1100, 0001, 00100, 01000, 10001, 11000, 10100\}$

(b) Sind die beiden Codes jeweils eindeutig entschlüsselbar?
Falls nein, konstruieren Sie jeweils ein $x \in \{0,1\}^*$, so dass x auf mind. 2 verschiedene Arten als Folge von Codeworten dekodiert werden kann. [4P]

Bemerkungen: In Teil (a) sollte erkennbar sein, wie Sie die Menge der Suffixe bestimmt haben. Insbesondere empfiehlt sich dabei, dem Algorithmus aus der Vorlesung zu folgen und bei jedem gefundenen Suffix hinzuschreiben, welche anderen Codewörter/Suffixe gerade benutzt wurden.
In Teil (b) sollte erkennbar sein, wie Sie das nicht eindeutig dekodierbare x und die Darstellungen als Folge von Codeworten gefunden haben.

AUFGABE 2:

Bestimmen Sie einen Huffman-Code zu einer erinnerungslosen Quelle Q über dem Alphabet $A = \{a_1, a_2, a_3, a_4, a_5, a_6\}$ mit jeweiligen Wahrscheinlichkeiten p_i für a_i, wobei

$$p_1 = \frac{3}{10}, p_2 = \frac{1}{4}, p_3 = \frac{3}{20}, p_4 = \frac{3}{20}, p_5 = \frac{1}{10}, p_6 = \frac{1}{20}$$

Was ist die erwartete Codewortänge für Ihren Code? [4P]

Bitte wenden!

AUFGABE 3:

Sei C ein eindeutig entschlüsselbarer Code, dessen Codewörter allesamt höchstens Länge n haben. Was ist die maximale Anzahl c_{max} an Codewörtern, die C besitzen kann?
Die Richtigkeit der Aussage ist selbstverständlich zu beweisen.[4.5P]

Hinweis: Beachten Sie, dass hier 2 Dinge zu zeigen sind: Zum einen ist die Existenz eines Codes mit c_{max} Codewörtern zu zeigen, zum anderen, dass es keinen solchen Code mit mehr als c_{max} Codewörtern gibt.

AUFGABE 4:

Konstruieren Sie jeweils einen Präfixcode $C = \{C_1, \dots C_n\}$ oder zeigen Sie, dass kein solcher existiert für

(a) $n = 5, |C_1| = 1, |C_2| = 3, |C_3| = 3, |C_4| = 3, |C_5| = 5$. [2.5P]

(b) $n = 6, |C_1| = 1, |C_2| = 3, |C_3| = 3, |c_4| = 3, |C_5| = 3, |C_6| = 6$. [2P]