Angewandte diskrete Mathematik

Wintersemester 2008/2009
Barbara Baumeister
Jürgen Schütz

Freie Universität Berlin
Institut für Mathematik

Aufgabenblatt 9

Ausgabe: 16.12.2008

Abgabe: 6.1.2009

Aufgabe 33. — 4 Punkte

a) Ist die Caesar-Chiffre perfekt geheim?

b) Gegeben sei ein Kryptosystem mit $\mathcal{P} = \{a, b\}$, $\mathcal{C} = \{A, B\}$, $\mathcal{K} = \{0, 1\}$ und Verschlüsselungsfunktionen e_0 und e_1 mit $e_0(a) = A$, $e_0(b) = B$, $e_1(a) = B$ und $e_1(b) = A$. Weiter sei auf $\mathcal{P}$ ein Wahrscheinlichkeitsmaß durch $P(a) = \frac{1}{3}$ und $P(b) = \frac{2}{3}$ definiert.
Gibt es ein Wahrscheinlichkeitsmaß auf $\mathcal{K}$, so dass dieses Kryptosystem perfekt geheim ist?

Aufgabe 34. — 4 Punkte

Betrachte die Blockchiffre mit Blocklänge n über dem Alphabet $\Sigma = GF(q)$, q Primzahlpotenz. Dabei sei sowohl auf dem Klartextraum $\mathcal{P} = \Sigma^n$ als auch auf dem Schlüsselraum $\mathcal{K}$ der $n \times n$-Matrizen über $GF(q)$ mit Determinante ungleich 0 die Gleichverteilung gegeben.

a) Ist die Blockchiffre perfekt geheim?

b) Ändert sich daran etwas, wenn man sowohl im Klar- als auch im Chiffretextraum die 0 entfernt.

Aufgabe 35. — 4 Punkte

Es sei $(\mathcal{P}, \mathcal{C}, \mathcal{K})$ ein perfekt geheimes Kryptosystem. Zeige, dass dann $|\mathcal{P}| \leqslant |\mathcal{K}|$ und $|\mathcal{C}| \leqslant |\mathcal{K}|$ ist.

Aufgabe 36. — 4 Punkte

a) Sei $K = GF(2^n)$ und $a \in K$. Zeige: Hat die Gleichung $x^2 + x = a$ eine Lösung in K, so gilt $a + a^2 + \ldots + a^{2^{n-1}} = 0$.

b) Sei $n \in \mathbb{N}$ ungerade. Beweise, dass $f : GF(2^n) \to GF(2^n)$ mit

$$f(x) = \begin{cases} x^{-1}, & \text{falls } x \neq 0, \\ 0, & \text{falls } x = 0 \end{cases}$$

eine APN-Funktion ist.
Hinweis: Es gilt $f(x) = x^{2^n-2}$. Zeige, dass $f(x+k) + f(x) = b$ für alle $b \in GF(2^n)$ und $0 \neq k \in GF(2^n)$ keine oder genau zwei Lösungen hat. Wir dürfen $k = 1$ annehmen. Sind $x \neq 0 \neq x+1$ Lösungen, so sind es die einzigen. Untersuche nun den Fall, dass $x = 0$ und $x = 1$ Lösungen sind, und benutze Aufgabenteil (a).

Zusatzaufgabe. 4 Punkte

Der Weihnachtsmann ist ja nicht mehr der Jüngste und geht deshalb nie ohne einen Spazierstock vor die Tür. Eines Tages, es war sehr glatt, rutscht er aus und sein Stock zerbricht (zufällig gleichverteilt) in drei Teile. Um nun nicht noch überfahren zu werden möchte er die Bruchstücke zu einem Warndreieck zusammenlegen.

Mit welcher Wahrscheinlichkeit geht das?