RUHR UNIVERSITÄT BOCHUM RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Jun.-Prof. Roberto Avanzi
Enrico Thomae

Hausübungen zur Vorlesung

Diskrete Mathematik II

SoSe 2010

Blatt 4 / 1. Juni 2010 / Abgabe bis spätestens 15. Juni 2010, 10:00 Uhr

AUFGABE 29 (2 Punkte)**:**
Geben Sie eine Parity Check Matrix für den binären Repetitionscode $R(n)$ an.

AUFGABE 30 (5 Punkte)**:**

(a) Konstruieren Sie das Standardarray für den Code mit Generatormatrix

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

(b) Decodieren Sie die empfangenen Worte 1111, 0000, 0001.

(c) Geben Sie ein Codewort und ein empfangenes Wort an, so dass ein Bitfehler vorkommt, aber dennoch korrekt dekodiert wird. Erläutern Sie Ihre Angaben.

(d) Geben Sie ein Codewort und ein empfangenes Wort an, so dass ein Bitfehler vorkommt und falsch dekodiert wird. Erläutern Sie Ihre Angaben.

AUFGABE 31 (4 Punkte)**:**
Bestimmen Sie den Minimalabstand der binären Linearcodes mit Parity Check Matrizen

$$\text{a) } H_1 = \begin{pmatrix} 0111000 \\ 1110100 \\ 1100010 \\ 1010001 \end{pmatrix}, \quad \text{b) } H_2 = \begin{pmatrix} 1101000 \\ 1010100 \\ 0110010 \\ 1100001 \end{pmatrix}.$$

AUFGABE 32 (4 Punkte)**:**
Konstruieren Sie das Standardarray zum binären Code $\mathcal{C} = \{0000, 1001, 0101, 1111\}$. Was läuft schief und warum? Geben Sie den kleinsten Code $\mathcal{C}' \supset \mathcal{C}$ an, für den man das Standardarray konstruieren kann. Welche Parameter (n, M, d) hat $\mathcal{C}'$?

AUFGABE 33 (8 Punkte)**:**
Ein linearer Code $\mathcal{C}$ ist selbst-orthogonal, falls $\mathcal{C} \subseteq \mathcal{C}^\perp$. Falls außerdem $\dim(\mathcal{C}) = \dim(\mathcal{C}^\perp)$, so heißt $\mathcal{C}$ selbst-dual.

(a) Sei $G = \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_k \end{pmatrix}$ die Generatormatrix eines binären linearen Codes. Zeigen Sie, dass $\mathcal{C}$ genau dann selbst-orthogonal ist, falls alle $\mathbf{b}_i, \mathbf{b}_j$ mit $i \neq j$ orthogonal sind und $2|w(\mathbf{b}_i)$ für alle i.

(b) Zeigen Sie, dass die Länge n eines selbst-dualen Codes gerade ist, und bestimmen Sie die Dimension eines selbst-dualen Codes der Länge n.

(c) Zeigen Sie, dass für jedes gerade n ein binärer selbst-dualer Code $\mathcal{C}_n$ existiert. Konstruieren Sie dazu die Generatormatrix von $\mathcal{C}_n$.