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

**Präsenzübungen zur Vorlesung**

# Diskrete Mathematik II

**SoSe 2010**

Blatt 4 / 1. Juni 2010

**AUFGABE 24:**
Berechnen Sie die Übertragungsrate und die Fehlerrate folgender Codes. Welchen würden Sie benutzen?

1. $(32, 2, 32)$ Repetitionscode,
2. $(31, 2^{26}, 3)$ Hamming Code,
3. $(24, 2^{12}, 8)$ Golay Code,
4. $(32, 2^{6}, 16)$ Reed-Muller Code,
5. $(32, 2^{16}, 17)$ Reed-Solomon Code.

**AUFGABE 25:**
In den USA gibt es zur Zeit rund 115.000.000 Telefonanschlüsse. Jede Telefonnummer besteht aus 10 Ziffern. Ist es möglich, die Telefonnummern so zu vergeben, dass ein Fehler beim Wählen der Nummer korrigiert werden kann? Wie lang müsste die Telefonnummern mindestens sein, dass dies auf jeden Fall möglich ist?

Hinweis: Zeigen Sie, dass $A_{10}(10, 3) < 115.000.000$ ist.

**AUFGABE 26:**
Sei $C = \langle 111 \rangle$.

(a) Bestimmen Sie die Generatormatrix des dualen Codes $C^{\perp}$.

(b) Geben Sie eine Parity Check Matrix von $C$ an und konstruieren Sie das Standardarray.

(c) Dekodieren Sie die Strings $100, 110, 111$ mit Hilfe von (b).

**AUFGABE 27:**
Sind folgende Codes $\mathcal{C} \subset \mathbb{F}_2^n$ Linearcodes? Geben sie eine Basis der Linearcodes an.

1. $\mathcal{C} = \{00, 11\}$,
2. $\mathcal{C} = \{000, 001, 011, 111\}$,
3. $\mathcal{C} = \{0000, 0011, 1100, 1010, 0101, 0110, 1001, 1111\}$,
4. $\mathcal{C} = \{001, 010, 101, 100\}$.

Kann es einen binären $(n, M)$ Linearcode mit $n = 4$ und $M = 12$ geben?

**AUFGABE 28:**
Gegeben ist folgende Generatormatrix des $(7, 16, 3)$ Hamming Codes $\mathcal{H}_2(3)$.

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

Geben Sie die dazugehörige Parity Check Matrix an. Ist 0101011 ein Codewort?