

11. Übung Codierungstheorie

1. Aufgabe Golay-Code

(4 Punkte)

Sei C der $[23, 12]_2$ -Golay-Code. Zeige, dass für C dann $d(C) \geq 5$ gilt.

2. Aufgabe Klassifizierung von Codes

(4 Punkte)

Sei K ein Körper mit q Elementen. Sei $k \geq 2$ und $n = \frac{q^k - 1}{q - 1}$. Zeige folgende Aussagen:

- (1) Ein $[n, n - k, 3]_q$ -Code über K ist bis auf Äquivalenz ein Hamming-Code.
- (2) Ein $[n, k, q^{k-1}]_q$ -Code über K ist bis auf Äquivalenz ein Simplex-Code.

Hinweis: Sei H Kontrollmatrix zum Code in (2). Zeige, dass der Code mit H als Erzeugermatrix die Minimaldistanz $d = 3$ hat, also nach (1) ein Hamming-Code ist. Wäre $d = 1$ bzw. $d = 2$, so streiche in H eine bzw. zwei geeignete Spalten und eine geeignete Zeile und betrachte den Code, der diese Matrix als Kontrollmatrix hat. Verwende die Griesmer-Schranke: Ist C ein $[n, k, d]$ -Code über einen Körper mit q Elementen, so gilt

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil.$$

3. Aufgabe

(3 Punkte)

Sei $C = \text{RM}(1, m)$ ein binärer Reed-Muller-Code erster Ordnung. Zeige, dass $d_r(C) = 2^{m-1} + 2^{m-2} + \dots + 2^{m-r}$ für $1 \leq r \leq m$ und $d_{m+1}(C) = 2^m$ ist.

Hinweis: Beachte, dass die Verkürzung von $\text{RM}(1, m)$ ein Simplex-Code ist.

4. Aufgabe Praktische Aufgabe

(5 Punkte)

Implementiere die Ver- und Entschlüsselung nach McEliece.

Hinweis: Die praktische Aufgabe kann bis zum 11.7.06 bearbeitet werden.