

## 2. Übung Codierungstheorie

### 1. Aufgabe Selbstduale Codes

(5 Punkte)

Zeige folgende Aussagen:

- (i) Ein Code  $C$  mit Prüfmatrix  $H = [A|I]$  über einem beliebigen Körper ist genau dann selbstdual, wenn  $A$  eine quadratische Matrix mit  $AA^t = -I$  ist.
- (ii) Für jede Primzahlpotenz  $q$ , für die  $-1$  ein Quadrat in  $\mathbb{F}_q$  ist, und für jedes  $n \in \mathbb{N}$  existiert ein selbstdualer  $[2n, n]$ -Code über  $\mathbb{F}_q$ .

### 2. Aufgabe Erweiterung von Codes

(5 Punkte)

- (i) Es seien  $C_i \leq \mathbb{F}_q^{n_i}$  zwei  $[n_i, k_i, d_i]_q$ -Codes und es sei

$$C := \{(c_1, c_1 + c_2) \mid c_1 \in C_1, c_2 \in C_2\} \in \mathbb{F}_q^{2n}.$$

Zeige, dass  $C$  ein  $[2n, k_1 + k_2, \min\{2d_1, d_2\}]$ -Code ist.

- (ii) Es seien  $C_i \leq \mathbb{F}_q^{n_i}$  zwei  $[n_i, k_i, d_i]_q$ -Codes. Zeige, dass  $C_1 \otimes C_2 \leq F_q^{n_1} \otimes F_q^{n_2}$  gilt.

### 3. Aufgabe ML-Decodierung

(2 Punkte)

Begründe, warum im Allgemeinen die Hamming-Decodierung und die Maximum-Likelihood-Decodierung (=ML-Decodierung) nicht das selbe sind.

### 4. Aufgabe Programmieraufgabe

(4 Punkte)

Sei  $C$  ein  $[n, k, d]_q$ -Code. Implementiere in KASH3 einen Algorithmus, der zu einem gegebenen linearen Code  $C$  die Parameter  $n$ ,  $k$  und  $d$  berechnet. Der Algorithmus bekommt dazu eine Erzeugermatrix  $G \in \mathbb{F}_q^{l \times n}$  mit  $l \geq k$  als Eingabe.