

---

## Fehlerkorrigierende Codes, Übungen

Sommersemester 2026

---

### Beispiele für die Übung am 1.6.2026

36. Man zeige, dass der Dualcode eines Reed-Solomon Codes ebenfalls ein Reed-Solomon Code ist.
37. Sei  $\alpha$  ein primitives Element in  $\mathbb{F}_q$ ,  $n = q - 1$  und  $1 \leq k \leq n$ . Wir betrachten folgende Codierung: Einem Nachrichtenwort  $u = (u_0, \dots, u_{k-1}) \in \mathbb{F}_q^k$  entspricht das Polynom  $u(x) = u_0 + u_1x + \dots + u_{k-1}x^{k-1}$ , und diesem ordnen wir das Codewort  $c = (u(1), u(\alpha), \dots, u(\alpha^{n-1}))$  zu.

(a) Man zeige, dass der so konstruierte Code ein Reed-Solomon Code ist.

(b) Man zeige auf direktem Weg, dass dieser Code ein MDS Code ist.

38. (Möbiussche Umkehrformel) Sei  $(G, +)$  eine abelsche Gruppe,  $h, H : \mathbb{N} \rightarrow G$  zwei Funktionen und  $\mu$  die Möbius-Funktion. Dann gilt für alle  $m \in \mathbb{N}$

$$H(m) = \sum_{t|m} h(t)$$

genau dann, wenn für alle  $m \in \mathbb{N}$

$$h(m) = \sum_{t|m} \mu\left(\frac{m}{t}\right) H(t)$$

gilt (die Summen werden jeweils nur über die positiven Teiler gebildet). (Hinweis: Man beachte  $\sum_{t|m} \mu(t) = 0$  für alle  $m > 1$  und  $\sum_{t|m} \mu(t) = 1$  für  $m = 1$ .)

39. Bezeichne  $N_q(t)$  die Anzahl der normierten irreduziblen Polynome in  $\text{GF}(q)$  vom Grad  $t$ . Man beweise die Formel

$$q^m = \sum_{t|m} t \cdot N_q(t)$$

für alle  $m \in \mathbb{N}$  und leite daraus die Formel für  $N_q(m)$  aus der VO her.

40. Man betrachte den zum Reed-Solomon Code über  $\mathbb{F}_8$  mit Generatorpolynom

$$g(x) = (x - 1)(x - T)(x - T^2)(x - T^3)$$

gehörenden Binärcode. Bündelfehler welcher Länge kann dieser Binärcode korrigieren? Man demonstriere dies an einem Beispiel.

41. Man zeige, dass der Dualcode eines MDS Codes ebenfalls ein MDS Code ist.
42. Gegeben seien Codes  $C_i$  mit Parametern  $[n_i, k_i, d_i]$ ,  $i = 1, 2$ . Man bestimme die Parameter  $[n, k, d]$  für den Produktcode  $C = C_1 \otimes C_2$ .
43. Man zeige, dass man beim Produktcode  $C_1 \otimes C_2$  zum gleichen Ergebnis gelangt, wenn man in der Nachrichtenmatrix zuerst die Spalten zu Codewörtern in  $C_1$  ergänzt und anschließend alle Zeilen zu Codewörtern in  $C_2$  bzw. zuerst die Nachrichtenzeilen zu Wörtern in  $C_2$  und anschließend alle Spalten zu Wörtern in  $C_1$ .
44. Man zeige, dass ein Code mit Minimaldistanz  $d$  jede Kombination von  $i$  Auslöschungen und  $j$  Fehlern an unbekanntenen Stellen korrigieren kann, wenn gilt  $i + 2j < d$ . Man gebe für Linearcodes ein Konzept an, wie man solche Fehlerkombinationen korrigiert.
45. Man zeige, dass es genau 267 Binärwörter der Länge 14 gibt mit der Eigenschaft, dass (1) zwischen zwei Einsen mindestens 2 Nullen auftreten und (2) niemals mehr als 10 Nullen aufeinanderfolgen.

(Hinweis: Man betrachte zunächst nur die Eigenschaft (1) und stelle eine Rekursion für die Anzahl  $a(n)$  dieser Wörter mit Länge  $n$  auf; mit Hilfe dieser Rekursion berechne man  $a(14)$  und vermindere um jene, die (2) nicht erfüllen.)