Fehlerkorrigierende Codes, Übungen

Sommersemester 2026

Beispiele für die Übung am 11.5.2026

31. Für alle $\alpha \in \mathrm{GF}(q^m)$ (q eine Primzahlpotenz, $m \in \mathbb{N}$) zeige man, dass α und α^q dasselbe Minimalpolynom über $\mathrm{GF}(q)$ haben.

32. Man zeige, dass binäre Hamming-Codes zyklisch sind (d.h., dass man bei der in der VO besprochenen Konstruktion der binären Hamming-Codes über die Kontrollmatrix die Stellen so anordnen kann, dass ein zyklischer Code entsteht). Hinweis: Man wähle als Generatorpolynom ein primitives Polynom.

33. [1] Bezeichne $H_r(q)$ den Hamming-Code über dem Alphabet $A = \mathrm{GF}(q)$ mit r Kontrollstellen (siehe Beispiel 21). Unter der Voraussetzung $\mathrm{ggT}(r, q-1) = 1$ zeige man, dass $H_r(q)$ (bei geeigneter Anordnung der Stellen) zyklisch ist. (Hinweis: Man betrachte das Minimalpolynom von α^{q-1} über $\mathrm{GF}(q)$, wobei α ein primitives Element in $\mathrm{GF}(q^r)$ ist. Weiters beachte man, dass aus $\mathrm{ggT}(r, q-1) = 1$ folgt $\mathrm{ggT}((q^r - 1)/(q-1), q-1) = 1$.)

34. Man begründe für allgemeines $n \in \mathbb{N}$ die Formel (Vandermondesche Determinante)

$$\det \begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \vdots & & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{pmatrix} = \prod_{1 \le i < j \le n} (x_j - x_i).$$

35. Man zeige, dass Reed-Solomon Codes MDS Codes sind. Hinweis: Man benütze die Kontrollmatrix.

[1] Aufgabe 33 ist ein Zusatzbeispiel für Interessierte, kein Pflichtprogramm.