Fehlerkorrigierende Codes, Übungen

Sommersemester 2014

Beispiele für die Übung am 15.5.2014

31. Man konstruiere GF(16) mit Hilfe eines primitiven Polynoms vom Grad 4 über $\mathbb{Z}_2$. Weiters zerlege man $T^{16} - T$ in irreduzible Faktoren über $\mathbb{Z}_2$ und bestimme das Minimalpolynom aller Elemente aus GF(16).

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).

33. 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. (Möbiussche Umkehrformel) Sei $(G, +)$ eine abelsche Gruppe, $h, H : \mathbb{N} \to G$ zwei Funktionen und μ 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 $m = 1$.)

35. Bezeichne $N_q(t)$ die Anzahl der normierten irreduziblen Polynome in $\mathrm{GF}(q)$ 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.

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

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

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

38. Man gebe die Generatormatrix eines Reed-Solomon Codes über dem Alphabet $\mathbb{F}_7$ mit der Dimension 2 an. Man berechne die Minimaldistanz d dieses Codes mit Hilfe der Formel aus der VO und überprüfe dies an Hand der Codewörter.