Prof. C. P. Schnorr Sommersemester 2006

Diskrete Mathematik

Blatt 11, 30.06.2006, Abgabe 07.07.2006

Aufgabe 1. (Reed–Solomon–Codes) Sei $\mathbf{F}_q^* = \langle \alpha \rangle, n = q - 1$.
Der Code $C \subset \mathbf{F}_q^n$ bestehe aus den Codepolynomen $a(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in \mathbf{F}_q[x]$ mit $a(\alpha) = a(\alpha^2) = \cdots = a(\alpha^{d-1}) = 0$. Zeige

1. C ist zyklisch mit
   Generatorpolynom $g(x) = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{d-1}) \in \mathbf{F}_q[x]$,
2. $d(C) \geq d - 1$,
3. $\dim_{\mathbf{F}_q} C = n - d + 1$.

Aufgabe 2. Sei $C, \alpha, \mathbf{F}_q$ wie in Aufgabe 1. Zeige

1. C liefert einen $[kn, k(n - d + 1)]$ Blockcode $\bar{C}$ über $\mathbf{Z}_2$ mit $d(\bar{C}) \geq d$.
2. Wie erhält man die Generator– und PCH–Matrix von $\bar{C}$?
3. $\bar{C}$ kann man erweitern zu $\bar{\bar{C}} \subset \mathbf{F}_q^n$ mit $d(\bar{\bar{C}}) \geq d$ und
   $\dim_{\mathbf{Z}_2}(\bar{\bar{C}}) = kn - k\#\{2j + 1 \mid 1 \leq 2j + 1 \leq d\}$.

Aufgabe 3. Zu $a_1, \ldots, a_k \in \mathbf{R}^n$ ist die Dimension des Polytops $P = \mathrm{conv}(a_1, \ldots, a_k)$ erklärt als die Dimension des Vektorraums $\sum_{i=2}^k (a_i - a_1)\mathbf{R}$. Zeige, dass $\dim(P)$ von der Reihenfolge der $a_1, \ldots, a_k$ nicht abhängt.

Aufgabe 4. $P = (-3, 9)$ und $Q = (-2, 8)$ sind Punkte der elliptischen Kurve $y^2 = x^3 - 36x$ über $\mathbf{Q}$. Bestimme $P + Q$ und $2P$.

6 Punkte pro Aufgabe.