Codierungstheorie (Sommersemester 2014)

Irene Bouw, Michel Börner

Blatt: 13
Punkte: +25

Abgabe (zu zweit oder alleine) vor der Vorlesung am Di., **22.07.14** um 10:15 Uhr im Raum E 20. Besprechung von Aufgabe 28 am Freitag, 25.7. **12:15** Uhr in He18, E 20. Alle Punkte sind Bonuspunkte.

Aufgabe 28 (BCH-Codes)

Wir konstruieren einen 3-fehlerkorrigierenden Code der Länge 8 über $\mathbb{F}_3$. Bezeichne mit α eine Nullstelle von $x^2 + x - 1$ sowie $\mathbb{F}_9 := \mathbb{F}_3[x]/(x^2 + x - 1)$. Wir haben gezeigt, dass $\text{ord}(\alpha) = 8$.

a) Finde ein $s > 0$ minimal, sodass $8 \mid (3^s - 1)$.

b) Zerlege $x^8 - 1 \in \mathbb{F}_3[x]$ (ohne Ergebnisse aus alten Übungsblättern oder dem Skript) in irreduzible Faktoren.
Vorgehen: 1. Wie groß kann der Grad dieser Faktoren maximal sein?
2. Wie überprüft man schnell, ob ein Polynom über $\mathbb{F}_3$ irreduzibel ist?

c) Bestimme alle zyklotomischen Nebenklassen C_a von $a \in \mathbb{Z}/8\mathbb{Z}$ und die zugehörigen Polynome $M^{(a)}$ bezüglich des Elements α.

d) Konstruiere ein Erzeugerpolynom g, sodass der von g erzeugte Code ein 3-fehlerkorrigierender Code der Länge 8 über $\mathbb{F}_3$ ist.

e) Zeige, dass für den in d) konstruierten Code tatsächlich $d_{\min}(\mathcal{C}) = 8$ gilt und berechne die Dimension k. Welchen großen Nachteil hat dieser Code in der Praxis? (1+2,5+2,5+2+2 = **+10 P**)

Hinweis: Die folgende Aufgabe wird nur bei denjenigen korrigiert, die die noch Punkte für die Vorleistung brauchen. Für die Vorleistung werden **60 Punkte** benötigt.

Aufgabe 29 (Wiederholungsaufgabe: Körper, Faktorisierung, zyklotomische Nebenklassen)

Betrachte $g(x) = x^{64} + x \in \mathbb{F}_2[x]$. Löse diese Aufgabe unter Klausurbedingungen, d.h. begründe alle Behauptungen (ggf. mit Skriptstellen) und verwende alte Übungsaufgaben nur mit Rechenweg.

a) Zeige, dass g über $\mathbb{F}_2$ keine mehrfachen Nullstellen besitzt.

b) Gib die Charakteristik p von $\mathbb{F}_{64}$, sowie den Grad der Körpererweiterung $\mathbb{F}_{64}/\mathbb{F}_p$ (bzw. den Index $[\mathbb{F}_{64} : \mathbb{F}_p]$) an.

c) Beschreibe, wie man den Körper $\mathbb{F}_{64}$ konstruiert.

d) Zeige, dass die Nullstellen von g genau die Elemente aus $\mathbb{F}_{64}$ sind.

e) Welche Teilkörper enthält der Körper $\mathbb{F}_{64}$?

f) Zeige: $\text{Grad}(\min_{\mathbb{F}_2}(b)) \in \{1, 2, 3, 6\}$ $\forall\, b \in \mathbb{F}_{64}$ und schließe, dass $h(x) = x^{63} + 1$ nur irreduzible Faktoren vom Grad $1, 2, 3$ und 6 hat.

g) Bestimme alle irreduziblen Polynome vom Grad ≤ 3 über $\mathbb{F}_2$ (mit Begründung!).

h) Gib alle irreduziblen Faktoren von h vom Grad ≤ 5 an. (1+2+1+2+3+2+3+1 = **+15 P**)
Tipp: Verwende f) und g).