Codierungstheorie (Sommersemester 2014)

Irene Bouw, Michel Börner

Blatt: 11
Punkte: 10

Abgabe zu zweit vor der Vorlesung am Di., **08.07.14** um 10:15 Uhr im Raum E 20.

Aufgabe 24 (Wiederholungsaufgabe: Ordnung)

Dies ist eine Fortsetzung von Aufgabe 20 a (Blatt 9). Wie wir gesehen haben gilt über $\mathbb{F}_3$ folgende Zerlegung in irreduzible Faktoren:

$$x^9 - x = x(x-1)(x+1)(x^2+1)(x^2+x-1)(x^2-x-1) \qquad (*)$$

Wir betrachten ein Element $\gamma \in \mathbb{F}_9 := \mathbb{F}_3[x]/(x^2+x-1)$ mit $\min_{\mathbb{F}_3}(\gamma) = x^2+x-1$. Nach Aufgabe 20 a hat γ Ordnung 8 und für die Potenzen von γ gilt: $\operatorname{ord}(\gamma^k) = 8/\operatorname{ggT}(8,k)$.

a) Bestimme das Minimalpolynom der Elemente der Ordnung 4 in $\mathbb{F}_9$.

b) Zeige, dass γ^2 auch ein primitives Element von $\mathbb{F}_9$ ist.

c) Faktorisiere $\min_{\mathbb{F}_3}(\gamma)$ über $\mathbb{F}_9$ und schreibe die Nullstellen in der Form γ^k.

d) Vervollständige die folgende Tabelle. Schreibe die Nullstellen in der Form $a + b\gamma$ sowie als Potenz von γ. Wir werden auf den kommenden Übungsblättern auf diese Tabelle zurückgreifen.

irred. Faktor	Ordnung d. Nullstellen	Nullstellen
$x-1$		
$x+1$		
x^2+1		
x^2+x-1		
x^2-x-1		

Wir haben damit insbesondere gezeigt, dass ein primitives Element α mit $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ nicht notwendigerweise Ordnung $q-1$ hat. (1+1+1+2,5 = **5,5 P**)

Aufgabe 25 (Zyklische selbstduale Codes)

Sei $\mathcal{C}$ ein zyklischer selbstdualer (n,k)-Code über $\mathbb{F}_q$ mit Erzeugerpolynom g und Prüfpolynom h, wobei $f(x) := x^n - 1 = g(x)h(x)$.

a) Zeige, dass $n = 2k$ und $g(x) = x^k h(\frac{1}{x})$ sowie $h(x) = x^k g(\frac{1}{x})$ gilt.

b) Schließe daraus, dass $x^n g(\frac{1}{x})h(\frac{1}{x}) = x^n - 1$.

c) Zeige, dass $\mathbb{F}_q$ ein Körper der Charakteristik 2 ist.
Hinweis: Zeige zunächst beispielweise $x^n g(\frac{1}{x})h(\frac{1}{x}) = -x^n + 1$.

d) Bestimme alle selbstdualen Codes der Länge 6 über $\mathbb{F}_2$.

e) Zeige, dass $g(x) := x^7 + x^6 + x^5 + x^4 + x + 1$ einen selbstdualen $(14,7)$-Code über $\mathbb{F}_2$ definiert.
Hinweis: Dies ist ein Beispiel für einen selbstdualen Code dessen Erzeugerpolynom nicht die Form $g(x) = x^{n/2} + 1$ hat.

(1+0,5+1+1+1 = **4,5 P**)