Übungen zur Kursvorlesung Algebraische Codierungstheorie
Wintersemester 2009/10 Blatt 5

W.Knapp Tübingen, den 14. November 2009

17. Eine endliche Gruppe G wirke (von rechts) auf eine endliche Menge Ω. Für $g \in G$ setze $f_\Omega(g) := \#\{\alpha \mid \alpha \in \Omega \text{ und } \alpha g = \alpha\}$; $r := |\Omega : G|$ bezeichne die Anzahl der G-Bahnen auf Ω. Beweisen Sie das *Lemma von Cauchy-Frobenius* (fälschlicherweise in der Literatur auch als das *Lemma von Burnside* bezeichnet):
$$\frac{1}{|G|}\sum_{g\in G} f_\Omega(g) = r\ .$$
Hinweis: Verwenden Sie doppelte Abzählung einer geeigneten Menge geordneter Paare (α, g). (5 Punkte)

18. Es sei A ein Alphabet mit $q \geq 2$ Elementen und $1 \leq n \in \mathbb{N}$. Ist $C \subseteq A^n$ ein n-Code über A, so setze für ganzzahlige $0 \leq i \leq n$
$d_i(C) := \frac{1}{|C|}\#\{(x,y) \mid (x,y) \in C \times C \text{ und } d_H(x,y) = i\}$.
Das $(n+1)$-Tupel $(d_i(C))_{i\in n+1}$ heiße die *Abstandsverteilung* von C und das homogene Polynom $d_H(C) := \sum_{i=0}^{n} d_i(C)\xi^i\eta^{n-i} \in \mathbb{Q}[\xi,\eta]$ heiße der *Abstandsenumerator* von C.
   (a) Was ist $\sum_{i\in n+1} d_i(C)$? Beweisen Sie, dass äquivalente Codes dieselbe Abstandsverteilung besitzen.
   (b) Berechnen Sie im Fall $C = \{x \mid x \in A^n \text{ und } d_H(x,a) = k\}$ mit $1 \leq k \leq n$ die Abstandsverteilung. Dabei bezeichne a ein beliebig gewähltes (konstantes) Wort in A^n.
   (c) Was lässt sich über die Abstandsverteilung sagen, falls $A = \mathbb{F}_q$ ist und C ein linearer Code, d.h. ein Unterraum von ${\mathbb{F}_q}^n$? (8 Punkte)

19. Es sei (V, B) ein Hamming-Paar über $\mathbb{F}_q$ mit $B = (e_i)_{i\in n}$ und α ein Automorphismus von $\mathbb{F}_q$.
Mit $\varphi(B,\alpha)$ bezeichnen wir die Abbildung $V \to V : x = \sum_{i\in n} x_i e_i \mapsto \sum_{i\in n} x_i^\alpha e_i$.
   (a) Beweisen Sie, dass $\varphi(B,\alpha)$ eine bijektive semilineare Abbildung mit Begleitautomorphismus α ist, welche die Hamming-Metrik d_B invariant lässt, d.h. $\forall_{x,y\in V}\ d_B(x\varphi(B,\alpha), y\varphi(B,\alpha)) = d_B(x,y)$.
   (b) Bestimmen Sie im Fall $q = 4$, $\alpha = (t \mapsto t^2)$ und $(V,B) = ({\mathbb{F}_4}^4, (e_i)_{i\in 4})$ einen linearen $(4,2)$-Code $C_1 = (V,B,C_1)$, welcher von $\varphi(B,\alpha)$ (als Ganzes) invariant gelassen wird und einen linearen $(4,2)$-Code $C_2 = (V,B,C_2)$, welcher von $\varphi(B,\alpha)$ nicht invariant gelassen wird. (7 Punkte)

Die Übungsaufgaben und sind schriftlich zu bearbeiten und am Mittwoch, dem 25. November 2009, in der Vorlesungspause abzugeben.