Übungsblatt 8

Kryptographie und Kodierungstheorie
WiSe 16/17

Aufgabe 8.1. Für ein gegebenes Wort w in $\mathbb{F}_2^3$ berechne man den Erwartungswert der Zufallsvariable $X_w : C \mapsto \chi_C(w)$ auf der Menge aller zweidimensionalen Untervektorräume, wobei vorausgesetzt wird, dass jeder Unterraum mit gleicher Wahrscheinlichkeit auftritt. Geben Sie anschließend den Erwartungswert für $Y_w : C \mapsto \chi_C(w)$ auf der Menge der dreidimensionalen Unterräume an, wobei $w \in \mathbb{F}_2^4$ ist.
Hinweis: Hier sind *nicht* die Unterräume bis auf Isomorphie gemeint, sondern wirklich alle.

Aufgabe 8.2. Beweisen Sie für $d, i \in \mathbb{Z}_{\geq 0}$ und $q \in \mathbb{Z}_{\geq 2}$ die Gleichung

$$\left\lceil \frac{\lceil d/q^i \rceil}{q} \right\rceil = \left\lceil \frac{d}{q^{i+1}} \right\rceil .$$

Aufgabe 8.3. Bestimmen Sie die lexikographischen Codes $L_{n,k}$ für die (n, k)-Paare (3,2), (4,2) und (4,3).

Aufgabe 8.4. Was passiert, wenn Sie die lexikographische Ordnung durch eine andere Ordnungsrelation ersetzen? Bleibt die Anforderung an das Minimalgewicht stets erhalten? Sind die Codes immer linear?

Aufgabe 8.5. Zeigen Sie, dass $L_{8,4}$ dem erweiterten Hamming-Code entspricht.

Aufgabe 8.6. Berechnen Sie das Minimalgewicht des ISBN-13 Codes.

Aufgabe 8.7. Zeigen Sie: Der (binäre) Wiederholungscode ungerader Länge ist perfekt. Gilt das auch für den erweiterten Hamming- bzw. Golay-Code?