Informationstheorie, FS 2017 Dr. Luis Haug
ETH Zürich, Dept. Informatik Nico Gorbach

Lösungen zu Übungsblatt 12

12.1

a) Die folgende Tabelle gibt für jedes Syndrom das Fehlermuster mit geringstem Hamming-Gewicht an.

Syndrom	Fehlermuster
000	00000
001	00001
010	00010
011	00011
100	00100
101	01000
110	00110
111	10000

b) Für ein Wort $y \in \mathbb{F}_2^N$ mit Syndrom $\sigma = Hy$ lässt sich die Menge der Codewörter schreiben als $\mathcal{C} = \{y - e | e \in \mathbb{F}_2^N, He = \sigma\}$. Es gilt

$$P(y|y-e) = \varepsilon^{w(e)}(1-\varepsilon)^{N-w(e)},$$

für jedes $e \in \mathbb{F}_2^N$ mit $He = \sigma$, und wegen $\varepsilon < \frac{1}{2}$ wird diese Ausdruck genau dann maximal, wenn $w(e)$ minimal wird. Damit folgt für den Syndromdecodierer g_S:

$$\begin{aligned} G \cdot g_S(y) &= y - \operatorname*{arg\,min}_{e,\, He=\sigma} w(e) \\ &= y - \operatorname*{arg\,max}_{e, He=\sigma} P(y|y-e) \\ &= \operatorname*{arg\,max}_{c \in \mathcal{C}} P(y|c) \\ &= G \cdot g_{ML}(y) \end{aligned}$$

wobei G eine Generatormatrix des Codes ist; also ist der Syndromdecodierer ist ein ML-Decodierer. Da die Informationsvektoren nach Annahme gleichverteilt sind, ist dieser wiederum ein MAP-Decodierer.

12.2

a) Dass $\mathcal{C}$ die Korrektur von bis zu e Fehlern erlaubt, bedeutet, dass die M Mengen $B_e(c) = \{w \in \mathbb{F}_q^N \mid d_H(w,c) \leq e\}$, $c \in \mathcal{C}$, paarweise diskunkt sind. Da diese Mengen jeweils die Kardinalität $\sum_{j=0}^{e} \binom{N}{j}(q-1)^j$ haben und $\mathbb{F}_q^N$ die Kardinalität q^N hat, muss

dafür $M \sum_{j=0}^{e} \binom{N}{j}(q-1)^j \leq q^N$ gelten; durch Umformen erhält man die zu zeigende Ungleichung.

b) Für $q = 2$, $e = 1$ wird die Ungleichung in (a) zu

$$M \leq \frac{2^N}{1+N},$$

und für $N = 2^r - 1$ weiter zu

$$M \leq \frac{2^{2^r-1}}{2^r}.$$

Für den Hamming-Code mit Codewörtern der Länge $N = 2^r - 1$ ist $M = 2^{N-r} = 2^{2^r-1-r}$, und damit wird die Ungleichung zu einer Gleichung. Also hat der Hamming-Code unter allen Codes mit $e = 1$ und $N = 2^r - 1$ die maximale Anzahl an Codewörtern, und damit auch die maximale Rate.

12.3

Wir starten mit $\mathcal{P}^0 = \mathbb{F}_q^N$ als Menge potentieller Codewörter und $\mathcal{C}^0 = \{\}$ als Menge ausgewählter Codewörter. Im i-ten Schritt wählen wir aus ein beliebiges Wort $w \in \mathcal{P}^{i-1}$ als i-tes Codewort aus, d.h. wir definieren $\mathcal{C}^i := \mathcal{C}^{i-1} \cup \{w\}$; dann definieren wir $\mathcal{P}^i$, indem wir aus $\mathcal{P}^{i-1}$ alle Wörter entfernen, die Hammingdistanz $\leq d-1$ von w besitzen. Damit ist sichergestellt, dass nach jedem Schritt die Minimaldistanz der Wörter in $\mathcal{C}^i$ mindestens d ist (das sieht man leicht durch Induktion). In jedem Schritt werden maximal $\sum_{j=0}^{d-1} \binom{N}{j}(q-1)^j$ der noch in Frage kommenden Wörter entfernt; daher können wir mindestens

$$\left\lceil \frac{q^N}{\sum_{j=0}^{d-1} \binom{N}{j}(q-1)^j} \right\rceil$$

Schritte ausführen, bevor die Menge der potentiellen Codewörter leer ist. Da wir in jedem Schritt ein Codewort hinzufügen, ist diese Zahl eine untere Schranke für die Anzahl der Codewörter am Ende.

12.4

Nach Definition ist ein RS-Code $\mathcal{C}_{RS}$ über $\mathbb{F}_q$ mit Parametern $\alpha \in \mathbb{F}_q$ und $t \in \mathbb{N}$ gegeben durch

$$\{\mathcal{F}_\alpha^{-1}(0, \ldots, 0, w_{2t}, \ldots, w_{N-1}) \mid (w_{2t}, \ldots, w_{N-1}) \in \mathbb{F}_q^{N-2t}\}.$$

Wir fassen nun Vektoren $w = (w_{2t}, \ldots, w_{N-1}) \in \mathbb{F}_q^{N-2t}$ als Polynome

$$\begin{aligned} p_w(x) &= w_{2t}x^{2t} + \cdots + w_{N-1}x^{N-1} \\ &= x^{2t}(w_{2t} + \cdots + w_{N-1}x^{N-1-2t}) \\ &= x^{2t}\tilde{p}_w(x) \end{aligned}$$

auf, wobei $\tilde{p}_w(x) = w_{2t} + \cdots + w_{N-1}x^{N-1-2t}$. Aus der Definition der (inversen) Fouriertransformation folgt dann, dass die Einträge c_i von $\mathcal{F}_\alpha^{-1}(w)$ gegeben sind durch Evaluation von $-p_w$ an den Stellen $\alpha^{-i} \in \mathbb{F}_q$, $i = 0, \ldots, N-1$:

$$c_i = -\sum_{j=2t}^{N-1} w_j \alpha^{-ij} = -p_w(\alpha^i) = -\alpha^{2ti}\tilde{p}_w(\alpha^i)$$

Die Polynome $\tilde{p}_w$ sind vom Grad $N-2t-1$, und daher sind ihre Koeffizienten durch die Werte an $N-2t$ Stellen eindeutig bestimmt; wegen $p_w(x) = x^{2t}\tilde{p}_w$ sind damit auch die Polynome p_w (unter allen Polynomen dieser Form) eindeutig durch $N-2t$ Werte bestimmt, die nicht Nullstellen von x^{2t} sind. Da wir schon wissen, dass $\mathcal{F}_\alpha^{-1}$ injektiv ist, knnen wir schliessen, dass sich für verschiedene $w_0 \neq w_1$ die Polynome p_{w_0} und p_{w_1} an mindestens $2t+1$ der Stellen α^i, $i = 0, \ldots, N-1$, unterscheiden, d.h. dass die Minimaldistanz $\geq 2t+1$ ist. Da allgemein die Minimaldistanz eines linearen (q^K, N)-Codes $\geq N-K+1 = 2t+1$ ist (siehe Vorlesung), folgt $d_{min}(\mathcal{C}_{RS}) = 2t+1$.