Übungsaufgaben zur Kodierungstheorie

1. *(1+1+1+1+2+2 Punkte)* Der lineare Code in $\mathbb{F}_2^{24}$ mit der folgenden Erzeugermatrix G wird $\mathcal{G}_{24}$ genannt.

	l_∞	l_0	l_1	l_2	l_3	l_4	l_5	l_6	l_7	l_8	l_9	l_{10}	r_∞	r_0	r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8	r_9	r_{10}
1	1	1												1	1		1	1	1				1	
2	1		1												1	1		1	1	1				1
3	1			1										1		1	1		1	1	1			
4	1				1										1		1	1		1	1	1		
5	1					1										1		1	1		1	1	1	
6	1						1										1		1	1		1	1	1
7	1							1						1				1		1	1		1	1
8	1								1					1	1				1		1	1		1
9	1									1				1	1	1				1		1	1	
10	1										1				1	1	1				1		1	1
11	1											1		1		1	1	1				1		1
12													1	1	1	1	1	1	1	1	1	1	1	1

(Die erste Zeile $[l_\infty, \ldots, r_{10}]$ und erste Spalte $[1, \ldots, 12]$ sind nicht Bestandteil der Erzeugermatrix; Auslassungen entsprechen dem Eintrag 0.*)*

Die Zeilen von G werden $z_1, ..., z_{12}$ genannt, die Spalten werden $l_\infty, l_0, ..., l_{10}, r_\infty, r_0, ..., r_{10}$ genannt. Es gelten die folgenden Aussagen:

(i) $\mathcal{G}_{24}$ ist ein $[24, 12, 8]$-Code. $\dim \mathcal{G}_{24} = 12$ folgt aus $\operatorname{rang} G = 12$, was man sofort sieht. Aber der Beweis von $d(\mathcal{G}_{24}) = 8$ ist schwer. Ein Beweis mit (iv) $G = H$ und Aufgabe 4 von Blatt 3 würde erfordern, dass man beweist, dass alle Mengen von 7 Spalten linear unabhängig sind, und es gibt $\binom{24}{7}$ solche Mengen.

(ii) $w(z_1) = ... = w(z_{11}) = 8,\ w(z_{12}) = 12.$

(iii) z_i und z_j haben an 4 Stellen eine 1 gemeinsam, falls $i \neq j$ und $i, j \leq 11$ ist. Und z_i mit $i \leq 11$ und z_{12} haben an 6 Stellen eine 1 gemeinsam.

(iv) $\mathcal{G}_{24}$ ist selbstdual (d.h. $\mathcal{G}_{24} = \mathcal{G}_{24}^\perp$). Und daher ist $G = H$ auch eine Kontrollmatrix.

(v) Enthält $\mathcal{G}_{24}$ das Wort $L|R$ mit $L = \lambda_\infty \lambda_0 \lambda_1 \ldots \lambda_{10}$ und $R = \rho_\infty \rho_0 \rho_1 \ldots \rho_{10}$, denn enthält $\mathcal{G}_{24}$ auch das Wort $\tilde{L}|\tilde{R}$ mit $\tilde{L} = \rho_\infty \rho_0 \rho_{10} \rho_9 \ldots \rho_1$ und $\tilde{R} = \lambda_\infty \lambda_0 \lambda_{10} \lambda_9 \ldots \lambda_1$.

(vi) Es sei G' die Matrix, die man aus G durch Weglassen der Spalte r_{10} bekommt, und $\mathcal{G}'_{23}$ der von ihr erzeugte lineare Code.

(vii) Es ist $\mathcal{G}'_{23} = \mathcal{G}_{23}$ der binäre Golay-Code.

(viii) Bemerkenswerterweise gilt etwas viel stärkeres als (vi): Die Erzeugermatrix des binären Golaycode $\mathcal{G}_{23}$ bekommt man durch das Auslassen einer *beliebigen* Spalte in der obigen Erzeugermatrix. (Aber das wird gleich nicht benutzt.)

(ii) und (iii) sind leichte Beobachtungen, (iii) ist etwas länglich. (i) und (v) und (viii) sind schwer zu beweisende Aussagen. Sie sollen hier nicht alles beweisen, sondern nur etwas vertraut werden mit der Erzeugermatrix G und den Golay-Codes $\mathcal{G}_{24}$ und $\mathcal{G}_{23}$. Dazu sollen Sie folgende Teile ausführen.

(a) Zeigen Sie mit Hilfe von (ii) und (vi), dass $\mathcal{G}_{24}$ der (durch Paritätsregel) erweiterte Code $\overline{\mathcal{G}'_{23}}$ ist.

(b) Zeigen Sie mit Hilfe von $d(\mathcal{G}_{24}) = 8$ und (a), dass $d(\mathcal{G}'_{23}) = 7$ ist.

Bitte wenden!

(c) Zeigen Sie mit Hilfe von (b) und den Bemerkungen 3.2 der Vorlesung, dass $\mathcal{G}'_{23}$ ein perfekter Code ist.

(d) Zeigen Sie mit Hilfe von (iii), dass (iv) gilt, d.h. dass G selbstdual ist.

(e) Zeigen Sie mit Hilfe von $d(\mathcal{G}_{24}) = 8$, $G = H$ Kontrollmatrix und Aufgabe 4 von Blatt 3, dass die Spalten $r_0, ..., r_{10}$ von G je 7 Einsen haben müssen und eine davon in der 12. Zeile liegen muss (was ja auch erfüllt ist), wenn die Spalten $l_\infty, l_0, ..., l_{10}, r_\infty$ so sind wie angegeben.

(f) Zeigen Sie (v) für die letzten beiden Zeilen z_{11} und z_{12} der Erzeugermatrix.
(Hinweis: Zeigen Sie, dass $(11\dots11)$ *in* $\mathcal{G}_{24}$ *liegt.)*

2. *(4 Punkte)* Zeigen Sie, dass das Tensorprodukt (vgl. Bemerkung 4.2 (iii) der Vorlesung)

   (i) nicht symmetrisch,

   (ii) assoziativ (d.h. $(A \otimes B) \otimes C = A \otimes (B \otimes C)$),

   (iii) und multiplikativ (d.h. $(A \otimes B) \cdot (C \otimes D) = (A \cdot C) \otimes (B \cdot D)$) ist.

3. *(4 Punkte)* Für einen Code $C \subset \mathbb{F}_q^n$ sei

$$A_i := A_i(C) := |\{x \in C \mid w(x) = i\}|$$

als die Anzahl der Worte im Code mit Gewicht i definiert. (Trivialerweise ist $A_i = 0$ für $i > n$.) Diese A_i werden zu einer *erzeugenden Funktion* $A(C, t)$ des Codes C zusammengefasst:

$$A(C, t) := A_0 + A_1 t + A_2 t^2 + A_3 t^3 + \ldots + A_n t^n \in \mathbb{Z}[t].$$

Für den dualen Code gilt die **MacWilliams-Identität**: Es sei C ein [n,k]-Code über $\mathbb{F}_q$ mit erzeugender Funktion $A(C, t)$. Dann hat der duale Code die erzeugende Funktion

$$A(C^\perp, t) = \frac{1}{q^k} \cdot (1 + (q-1)t)^n \cdot A\left(\frac{1-t}{1+(q-1)t}\right).$$

(a) Die zu den Hamming-Codes dualen Codes heißen *Simplex-Codes*. Wählen Sie einen $[7, 4]$-Hamming-Code C über $\mathbb{F}_2$, geben Sie eine Erzeugermatrix und alle 16 Elemente von C an. Und geben Sie eine Erzeugermatrix des dualen [7,3]-Simplex-Codes $C^\perp$ und alle 8 Elemente von $C^\perp$ an.

(b) Schreiben Sie für C und $C^\perp$ wie in (a) die erzeugenden Funktionen $A(C, t)$ und $A(C^\perp, t)$ hin und zeigen Sie, dass hier die MacWilliams-Identität erfüllt ist.

Alle Informationen zur Vorlesung (Termine, Übungsblätter, Skript etc.) sind unter `http://hilbert.math.uni-mannheim.de/cod10.html` zu finden.

Abgabe bis Donnerstag, 18. März 2007, 17 Uhr (Kasten im Eingangsbereich A5 oder Beginn der Übung)