Übungsaufgaben zur Kodierungstheorie

1. *(8 Punkte)* In dieser Aufgabe sollen Sie die Dekodierung von Reed-Muller-Codes nach Satz 5.7 an einem Beispiel durchführen. Dabei sollen die Elemente von $\mathrm{Abb}\,(\mathbb{F}_2^4, \mathbb{F}_2)$ wieder wie in Aufgabe 4 von Blatt 5 dargestellt werden, nämlich durch Ausfüllen von den Kreisen im Bild von Aufgabe 4 von Blatt 5, Wert 0 $\sim$ leerer Kreis, Wert 1 $\sim$ ausgefüllter Kreis.

   Die Abbildung $g \in \mathrm{Abb}\,(\mathbb{F}_2^4, \mathbb{F}_2)$ sei gegeben durch das Diagramm

   ○ ● ● ●
   ○ ○ ● ●
   ○ ○ ● ○
   ○ ○ ● ○

   Es ist $g = f + e$ für ein $f \in \mathcal{R}(2,4)$ und ein e mit $w(e) = 1$. Also ist Satz 5.7 mit $m = 4$ und $r = 2$ anwendbar.

   (a) $M = \{1,2,3,4\}$ hat die 6 Teilmengen mit 2 Elementen $I = \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}$. Es ist jeweils $|S_I| = 4$. Skizzieren Sie für jede dieser 6 Mengen in einem Diagramm mit 16 Kreisen wie in Aufgabe 2 die 4 (natürlich disjunkten) Träger $S_{I^C} + t$, $t \in S_I$.

   (b) Berechnen Sie für jedes I wie in (a) die 4 Werte $< g, P_{I^C,t} > \in \mathbb{F}_2$ mit $t \in S_I$ und bestimmen Sie so nach Satz 5.7 die m_I mit $|I| = 2$ in

   $$f = \sum_{I \subset M, |I| \leq 2} m_I P_{I,(1,1,1,1)}.$$

   (c) Wie (a), aber für $I = \{1\}, \{2\}, \{3\}, \{4\}$. Nun ist $|S_I| = 8$.

   (d) Nun arbeitet man mit $r - 1 = 1$ statt $r = 2$ und mit

   $$\widetilde{g} := g + \sum_{I \subset M, |I| = 2} m_I P_{I,(1,1,1,1)}$$

   anstelle von g: es erfüllt $\widetilde{g} = \widetilde{f} + e$ mit

   $$\widetilde{f} = f + \sum_{I \subset M, |I|=2} m_I P_{I,(1,1,1,1)} = \sum_{I \subset M, |I| \leq 1} m_I P_{I,(1,1,1,1)} \in \mathcal{R}(1,4).$$

   Malen Sie in einem Diagramm mit 16 Kreisen wie oben den Träger von $\widetilde{g}$ ein. Berechnen Sie für jedes I wie in (c) die 8 Werte $< g, P_{I^C,t} > \in \mathbb{F}_2$ und bestimmen Sie so nach Satz 5.7 (mit $t \in S_I$) die m_I mit $|I| = 1$.

   (e) Es bleibt der konstante Term $m_\emptyset$ zu bestimmen. Gehen Sie analog zu (a)+(b) und (c)+(d) vor.

Bitte wenden!

Die restlichen 3 Aufgaben betreffen Kapitel 6. Ihre Punkte sind für das Erreichen der 50 % für einen Schein irrelevant.

In Kapitel 6 ist für p eine Primzahl und $n \in \mathbb{N}$ folgende Menge definiert,

$$J_{n,p} := \{f(t) \in \mathbb{F}_p[t] \mid \deg f(t) = n,\ f(t) \text{ unitär und irreduzibel}\}.$$

In Satz 6.14 werden folgende Formeln bewiesen (die zweite verfeinert die erste),

$$\begin{aligned} p^n &= \sum_{r \text{ teilt } n} r \cdot |J_{r,p}| \\ t^{p^n} - t &= \prod_{r \text{ teilt } n} \prod_{f(t) \in J_{r,p}} f(t) \quad \text{in } \mathbb{F}_p[t] \\ &= \prod_{a \in \mathbb{F}_{p^n}} (t-a). \end{aligned}$$

Aus der ersten wird die Formel

$$|J_{n,p}| = \frac{1}{n} \sum_{r \text{ teilt } n} \mu(r) \cdot p^{\frac{n}{r}}$$

gefolgert, und aus dieser $|J_{n,p}| > 0$ und damit $J_{n,p} \neq \emptyset$. Die zweite und dritte Formel zeigen, welche irreduziblen Polynome als Minimalpolynome der Elemente von $\mathbb{F}_{p^n}$ als Körpererweiterung von $\mathbb{F}_p$ auftreten, nämlich alle in $J_{r,p}$ mit r Teiler von n.

Andererseits zeigt Satz 6.18, dass alle Minimalpolynome (von Elementen α von $\mathbb{F}_{p^n}$ als Körpererweiterung von $\mathbb{F}_p$) die spezielle Gestalt $m_{\alpha,p}$ von Satz 6.18 c) haben. Schliesslich folgt aus Satz 6.17 der Gruppenisomorphismus

$$(\mathbb{F}_{p^n} - \{0\}, \cdot) \cong (\mathbb{Z}/(p^n-1)\mathbb{Z}, +).$$

Aus der Struktur der Gruppe $(\mathbb{Z}/(p^n-1)\mathbb{Z}, +)$ kann man wie im Beispiel 6.21 relativ leicht ablesen, welche Grade die Minimalpolynome der Elemente von $\mathbb{F}_{p^n} - \{0\}$ haben und welche von ihnen primitiv (Definition 6.20) sind.

2. *(2 Punkte)* Bestimmen Sie mit der Formel

$$|J_{n,p}| = \frac{1}{n} \sum_{r \text{ teilt } n} \mu(r) \cdot p^{\frac{n}{r}}$$

explizitere Formeln für $|J_{n,p}|$ für $1 \leq n \leq 6$, und werten Sie diese 6 Formeln in den Fällen $p = 2$ und $p = 3$ aus.

3. *(4 Punkte)* Für $d \in \mathbb{N} \cup \{0\}$ gibt es 2^d unitäre Polynome vom Grad d in $\mathbb{F}_2[t]$. Jedes mit $d \geq 1$ lässt sich eindeutig als Produkt von unitären und irreduziblen Polynome schreiben. Listen Sie alle $30 = 2+4+8+16$ unitären Polynome der Grade $d \in \{1,2,3,4\}$ und ihre Produkt-Zerlegungen in unitäre und irreduzible Polynome auf.

4. *(2 Punkte)* Die Lösung von Aufgabe 2 zeigt $|J_{6,2}| = 9$, d.h. es gibt 9 unitäre und irreduzible Polynome vom Grad 6 in $\mathbb{F}_2[t]$. Wieviele von ihnen sind primitiv (Definition 6.20)?

   Hinweise: Die Lösung ist ähnlich zu Beispiel 6.21 und benutzt die Struktur der Gruppe $(\mathbb{F}_{p^n} - \{0\}, \cdot) \cong (\mathbb{Z}/(p^n-1)\mathbb{Z}, +)$. Wieviele Einheiten hat diese Gruppe?
   (Diese Aufgabe erfordert *nicht* die Bestimmung der 9 Elemente von $J_{6,2}$, sondern ist viel einfacher.)

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

Abgabe bis Donnerstag, 22. April 2010, 17 Uhr (Kasten im Eingangsbereich A5 oder Beginn der Übung)