G. Nebe, M. Kirschmer

Gitter und Codes, WS 08/09

Lösung 7

Aufgabe 1.

(a) Nach Aufgabe 3 auf Blatt 4 ist $\mathbb{D}_4$ isometrisch zum Codegitter des Codes d_4 und es gilt $p_{d_4}(X,Y) = X^4 + Y^4$.
Wir rechnen in $\mathbb{C}[[q^{1/2}]]$. Nach Satz 6.3 wird

$$\begin{aligned}\Theta_{\mathbb{D}_4} = \Theta_{L_{d_4}} &= p_{d_4}(\theta_{0,2}, \theta_{1,2}) = \theta_{0,2}^4 + \theta_{1,2}^4 \\ &\equiv_{q^9} (1 + 2q^2 + 2q^8)^4 + (2q^{1/2} + 2q^{9/2})^4 \\ &\equiv_{q^9} 1 + 24q^2 + 24q^4 + 96q^6 + 24q^8 \ .\end{aligned}$$

Insbesondere besteht $\{x \in \mathbb{D}_4 \mid (x,x) = 8\}$ aus 24 Elementen. Ausserdem sehen wir, daß die Koeffizienten im allgemeinen nicht monoton wachsen.

(b) Nach Aufgabe 3 auf Blatt 4 ist $\mathbb{E}_7$ isometrisch zum Codegitter von $H(\mathbb{F}_2, 3)^\perp$. Bestimmen wir nun zuerst den Hamminggewichtszähler von $H(\mathbb{F}_2, 3)$. Dort haben wir gezeigt, daß

$$\begin{pmatrix} 1&0&0&0&0&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&1&1&1 \end{pmatrix}$$

eine Erzeugermatrix von $H(\mathbb{F}_2, 3)$ ist. Also ist z.B.

$$\begin{pmatrix} 1&0&1&0&1&0&1 \\ 0&1&1&0&0&1&1 \\ 0&0&0&1&1&1&1 \end{pmatrix}$$

eine Erzeugermatrix von $H(\mathbb{F}_2, 3)^\perp$. Der Code hat 8 Codewörter und alle Wörter ungleich Null haben Gewicht 4. Damit ist $p_{\mathbb{E}_7}(X,Y) = p_{H(\mathbb{F}_2,3)^\perp}(X,Y) = X^7 + 7X^3Y^4$.
Nach Satz 6.3 ist dann

$$\begin{aligned}\Theta_{\mathbb{E}_7} &= \theta_{0,2}^7 + 7\theta_{0,2}^3\theta_{1,2}^4 \\ &\equiv_{q^9} (1 + 2q^2 + 2q^8)^7 + 7(1 + 2q^2 + 2q^8)^3(2q^{1/2} + 2q^{9/2})^4 \\ &\equiv_{q^9} 1 + (7 \cdot 2 + 7 \cdot 16) \cdot q^2 + (\binom{7}{2} \cdot 4 + 7 \cdot 2 \cdot 3 \cdot 16) \cdot q^4 + (\binom{7}{3} \cdot 8 + 7(4 \cdot 2^4 + 3 \cdot 2^6)) \cdot q^6 \\ &\quad + (7 \cdot 2 + 16 \cdot \binom{7}{4} + 7(2^7 + 2 \cdot 3 \cdot 4 \cdot 16)) \cdot q^8 \\ &\equiv_{q^9} 1 + 126q^2 + 756q^4 + 2072 \cdot q^6 + 4158q^8\end{aligned}$$

Insbesondere besteht $\{x \in \mathbb{E}_7 \mid (x,x) = 8\}$ aus 4158 Elementen.

Aufgabe 2.
Es wird

$$\begin{aligned}\Theta_{\sum_{i=1}^N a_i b_i + pM}(q) &= \sum_{d_1 \in \mathbb{Z}} \cdots \sum_{d_N \in \mathbb{Z}} q^{\left(\sum_{i=1}^N (a_i + pd_i)b_i,\ \sum_{i=1}^N (a_i + pd_i)b_i\right)} \\ &= \sum_{d_1 \in \mathbb{Z}} \cdots \sum_{d_N \in \mathbb{Z}} q^{\sum_{i=1}^N (a_i + pd_i)^2/p} \\ &= \sum_{d_1 \in \mathbb{Z}} \cdots \sum_{d_N \in \mathbb{Z}} \prod_{i=1}^N q^{(a_i + pd_i)^2/p} \\ &= \prod_{i=1}^N \underbrace{\sum_{d_i \in \mathbb{Z}} q^{(a_i + pd_i)^2/p}}_{\theta_{a_i,p}(q)}\end{aligned}$$

Aufgabe 3.
Im Fall $p = 2$ ist ℓ ungerade, $Q = \{1\}$, $\zeta = -1$ und somit $p_Q(X) = X + 1 \in \mathbb{F}_\ell[X]$. Also hat $QR(\mathbb{F}_\ell, 2)$ die Erzeugermatrix $(1, 1)$ und damit Minimum 2.
Sei nun p ungerade. Fassen wir Q als Teilmenge von $\mathbb{F}_p$ auf, so ist Q eine Untergruppe von $\mathbb{F}_p^*$ von Ordnung $\frac{p-1}{2}$.

(a) Die Nullstellenmenge von $p_Q(X)$ ist gerade $M := \{\zeta^q \mid q \in Q\}$. Wegen $\ell \in Q$ ist $M = \{(\zeta^\ell)^q \mid q \in Q\}$. Also ist M invariant unter dem Frobeniusautomorphismus $x \mapsto x^\ell$. Damit ist $M \subseteq \mathbb{F}_\ell$. Daraus folgt die Behauptung, da die Koeffizienten von $p_Q(X)$ Linearkombinationen von Produkten von Elementen aus M sind. Insbesondere ist $p_Q(X) \in \mathbb{F}_\ell[X]$.

(b) Sei $N = \{i \in \{1, \ldots, p-1\} \mid i \notin Q\}$ die Menge der Nichtquadrate modulo p. Fixieren wir nun ein $n \in N$ beliebig so ist $N = nQ$. Wegen (a) ist

$$(X^p - 1) = (X - 1) \cdot p_Q(X) \cdot p_N(X)$$

mit $p_N(X) = \prod_{q \in Q}(X - \zeta^{nq}) \in \mathbb{F}_\ell[X]$ da alle anderen Polynome der Gleichung in $\mathbb{F}_\ell[X]$ sind.
Sei nun $a(x)$ ein Codewort in $QR(\mathbb{F}_\ell, 2)$ von minimalem Gewicht d. Dann ist $a(\zeta^q) = 0$ für alle $q \in Q$. Damit hat $a(X)a(X^n) \in \mathbb{F}_\ell[X]$ die Nullstellenmenge $Q \cup N$. D.h. $\sum_{i=1}^{p} X^i \equiv p_Q(X)p_N(X) \mod (X^p - 1)$. Insbesondere hat das Wort $a(X)a(X^n)$ Gewicht p. Andererseits zeigt Ausmultiplizieren, daß $a(X)a(X^n)$ höchstens d^2 Koeffizienten ungleich Null haben kann. Also gilt $d^2 \geq p$.

(c) Ist $p \equiv_4 -1$, so dürfen wir $n = -1$ (bzw. $p - 1$) wählen. Ist $a(X) = \sum_{i=0}^{p-1} a_i X^i$, so ist $a_i X^i a_i X^{-i} = 1$ für genau d Koeffizienten $a_i \neq 0$. Also liefern d Summanden von $a(X)a(X^{-1})$ den Beitrag 1. Damit ist das Gewicht von $a(X)a(X^{-1})$ maximal $d^2 - d + 1$.

Aufgabe 4.
Per Definition ist $\hat{f}(y) = \int_{\mathbb{R}^n} \exp(-\frac{\pi}{t} x x^{\mathrm{tr}}) \cdot \exp(-2\pi \mathrm{i} x y^{\mathrm{tr}}) \mathrm{d}x$. Wir haben also

$$\int_{\mathbb{R}^n} \exp(-\frac{\pi}{t} x x^{\mathrm{tr}}) \cdot \exp(-2\pi \mathrm{i} x y^{\mathrm{tr}}) \mathrm{d}x = t^{n/2} \cdot \exp(-\pi t y y^{\mathrm{tr}})$$

für alle $y \in \mathbb{R}^n$ und $t \in \mathbb{R}_{>0}$ zu zeigen.

Wenden wir auf die linke Seite Fubini an, so erhalten wir $\prod_{j=1}^{n} \int_{\mathbb{R}} \exp(-\frac{\pi}{t} x^2) \cdot \exp(-2\pi \mathrm{i} x_j y_j) \mathrm{d}x$. Die rechte Seite läßt sich umformen zu $\prod_{j=1}^{n} t^{1/2} \cdot \exp(-\pi t y_j^2)$.

Daher genügt es die Behauptung nur für $n = 1$ zu zeigen. Also ist zu zeigen:

$$\int_{\mathbb{R}} \exp(-\frac{\pi}{t} x^2) \cdot \exp(-2\pi \mathrm{i} x y) \mathrm{d}x = t^{1/2} \cdot \exp(-\pi t y^2)$$

für alle $y \in \mathbb{R}$ und $t \in \mathbb{R}_{>0}$. Ersetzen wir y durch $t^{-1/2} y$ und substituieren links $x \mapsto t^{1/2} x$, so dürfen wir annehmen, daß $t = 1$ ist.

Wir beweisen zunächst den bekannten Spezialfall $y = 0$, aus dem der allgemeine Fall folgen wird. Die linke Seite ist im Fall $y = 0$ gerade $I := \int_{\mathbb{R}} \exp(-\pi x^2) \mathrm{d}x$. Mittels dem üblichen Trick bestehend aus Quadrieren und Übergang zu Polarkoordinaten folgt

$$\begin{aligned} I^2 &= \int_{\mathbb{R}^2} \exp(-\pi(u^2 + v^2)) \mathrm{d}(u, v) = \int_0^{2\pi} \int_0^{\infty} \exp(-\pi r^2) r \mathrm{d}r \, \mathrm{d}\alpha \\ &\overset{z=\pi r^2}{=} 2\pi \cdot \frac{1}{2\pi} \int_0^{\infty} \exp(-z) \mathrm{d}z = 1 \end{aligned}$$

Wegen $I > 0$ ist damit $I = 1$ wie behauptet.

Nun zum Fall $y \neq 0$. Partielle Integration zeigt (mit $u(x) = \exp(-\pi x^2), v(x) = (-2\pi \mathrm{i} y)^{-1} \exp(-2\pi \mathrm{i} x y)$):

$$\hat{f}(y) = u(x)v(x)|_{-\infty}^{+\infty} - \int_{\mathbb{R}} u'(x)v(x) \mathrm{d}x = 0 - \int_{\mathbb{R}} \frac{-2\pi x}{-2\pi \mathrm{i} y} \exp(-\pi x^2) \exp(-2\pi \mathrm{i} x y) \mathrm{d}x$$

Andererseits ist

$$\hat{f}'(y) = \int_{\mathbb{R}} \exp(-\pi x^2) \exp(-2\pi \mathrm{i} x y)(-2\pi \mathrm{i} x) \mathrm{d}x$$

und somit $\hat{f}'(y) = (-2\pi y)\hat{f}(y)$. Damit hat dann $\frac{\hat{f}(y)}{\exp(-\pi y^2)}$ die Ableitung Null.
Also ist $\hat{f}(y) = c \cdot \exp(-\pi y^2)$ für ein $c \in \mathbb{R}$. Setzt man auf beiden Seiten $y = 0$ ein, so folgt $c = \hat{f}(0) = 1$ wie wir bereits gezeigt haben. Damit ist der Beweis beendet.