G. Nebe, M. Kirschmer

Gitter und Codes, WS 08/09

Lösung 4

Aufgabe 1. Es sei $(b_1, \dots, b_4)$ eine Orthogonalbasis von $\mathbb{R}^{1\times 4}$ mit $(b_i, b_i) = \frac{1}{3}$. Weiter seien $M := \langle b_1, \dots, b_4\rangle_{\mathbb{Z}}$ und $\pi\colon M \to C$, $\sum_{i=1}^4 a_i b_i \mapsto (\bar{a}_1, \dots, \bar{a}_4)$. Wir setzen $x := b_1 + b_2 - b_3$ und $y := b_2 + b_3 + b_4$. Dann ist $\langle \pi(x), \pi(y)\rangle_{\mathbb{F}_3} = C$ und es gilt $\ker(\pi) = 3M$. Daher ist $L_C = \pi^{-1}(C) = \langle x, y, 3M\rangle_{\mathbb{Z}}$. Eine Basis von L_C ist damit z.B. gegeben durch $B := (x, y, 3b_3, 3b_4)$.
Nun ist $\mathcal{G}(B) = \begin{pmatrix} 1 & 0 & -1 & 0\\ 0 & 1 & 1 & 1\\ -1 & 1 & 3 & 0\\ 0 & 1 & 0 & 3\end{pmatrix}$. D.h. bezüglich der Basis $(x, y, x - y + 3b_3, 3b_4 - y)$ ergibt sich die Grammatrix $\begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & -1\\ 0 & 0 & -1 & 2\end{pmatrix}$. Daher ergibts sich bezüglich Basis $(x, y, x - y + 3b_3, x - 2y + 3b_3 + 3b_4)$ von L_C die GramMatrix I_4. Also ist L_C isometrisch zum Standardgitter und damit ist $\min(L_C) = 1$.

Aufgabe 2 Nach dem Elementarteilersatz existiert eine Basis $B = (b_1, \dots, b_n)$ von L und ganze Zahlen $a_1, \dots, a_n$ so, daß $B' := (a_1 b_1, \dots, a_n b_n)$ eine Basis von L' ist. Also ist

$$\mathcal{G}(B') = \mathrm{Diag}(a_1, \dots, a_n) \cdot \mathcal{G}(B) \cdot \mathrm{Diag}(a_1, \dots, a_n)\,.$$

Bilden wir auf beiden Seiten die Determinanten, so erhalten wir $\det(L') = \det(L) \cdot \prod_{i=1}^n a_i^2$. Wegen $[L : L'] = |L/L'| = |\mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}| = \prod_{i=1}^n a_i$ folgt daraus die Behauptung.

Aufgabe 3. Eine Prüfmatrix von $H(\mathbb{F}_2, 3)$ ist z.B. gegeben durch

$$P := \begin{pmatrix} 0&0&1\\ 0&1&0\\ 0&1&1\\ 1&0&0\\ 1&0&1\\ 1&1&0\\ 1&1&1\end{pmatrix}\,.$$

Eine Erzeugermatrix ist dann z.B. (in Stufenform)

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

Also bilden die Zeilen von

$$T := \begin{pmatrix} 1&0&0&0&0&1&1\\ 0&1&0&0&1&0&1\\ 0&0&1&0&1&1&0\\ 0&0&0&1&1&1&1\\ 0&0&0&0&2&0&0\\ 0&0&0&0&0&2&0\\ 0&0&0&0&0&0&2\end{pmatrix}$$

eine Basis B' von $L_{H(\mathbb{F}_2,3)}$ bezüglich B.
Die Grammatrix $G := \mathcal{G}(B')$ ist dann $\frac{1}{2}TT^{\mathrm{tr}}$. Also bilden die Zeilen von $G^{-1} \cdot T = 2T^{\text{-tr}}$ eine Basis von $L^{\#}_{H(\mathbb{F}_2,3)} = L_{H(\mathbb{F}_2,3)^\perp}$ bezüglich B.
Sei nun $S := \begin{pmatrix} 0&0&0&0&0&-2&0\\ -1&0&1&-1&0&1&0\\ 1&0&-1&0&-1&0&1\\ 0&1&1&1&1&0&0\\ 0&-2&0&0&0&0&0\\ 0&1&-1&-1&1&0&0\\ 0&0&0&0&0&0&-2\end{pmatrix}$ wie im Hinweis. Wegen $S \cdot (2T^{\text{-tr}})^{-1} = S \cdot \frac{1}{2}T^{\mathrm{tr}} \in \mathrm{GL}_7(\mathbb{Z})$ (nachrechnen) bilden daher auch die Zeilen von S eine Basis B'' von $L_{H(\mathbb{F}_2,3)^\perp}$. Als letzten Schritt überprüft man nun, daß $\mathcal{G}(B'') = \frac{1}{2}SS^{\mathrm{tr}}$ die Gestalt aus Bem. 1.16 besitzt.

Aufgabe 4.

(a) Wir zeigen zunächst:

Lemma: Sei K ein endlicher Körper oder ein Körper der Charakteristik 0. Dann ist $f' \neq 0$ für jedes irreduzible Polynom $f \in K[X]$ mit $\deg(f) > 0$.

Beweis: Sei p die Charakteristik von K. Im Fall $p = 0$ ist nichts zu zeigen. Sei nun K endlich. Weiter sei $f' = 0$ angenommen. Dann existiert ein Polynom $g(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ mit $f(X) = g(X^p)$. Es ist $K = \{x^p \mid x \in K\}$, da der Frobeniusmonomorphismus auf endlichen Körpern bijektiv ist. Also ist $a_i = b_i^p$ für geeignete $b_i \in K$. Damit wird $g(X^p) = \sum_{i=1}^{n} b_i^p X^{pi} = h(X)^p$ mit $h(X) = \sum_{i=0}^{n} b_i X^i$. Dann aber ist $f(X) = g(X^p) = h(X)^p$ reduzibel.

Nun zur eigentlichen Aufgabe:

Sei $f = cf_1 \cdot \cdots \cdot f_s$ mit $c \in K$ und $f_i \in K[X] \setminus K$ irreduzibel und normiert. Angenommen die f_i sind nicht paarweise verschieden, sagen wir $f_1 = f_2$. Dann ist $f = f_1^2 \cdot h$ mit $h = c \cdot \prod_{i \geq 3} f_i$ und $f' = 2f_1 h + f_1^2 h'$. Also ist f_1 ein nichtkonstantes Polynom welches f und f' teilt.

Seien umgekehrt alle f_i paarweise verschieden. Dann ist $f = \gcd(f, f') \cdot g$ für $g \in K[X]$ geeignet. Da die Zerlegung in normierte irreduzible Faktoren eindeutig ist, folgt $\gcd(f, f')$ ist das Produkt einiger f_i. Angenommen f_i teilt f', so setze $g_i := \prod_{j \neq i} f_j$. Dann wird $f' = f_i' g_i + f_i g_i'$ aber nicht von f' geteilt, denn nach Voraussetzung teilt f_i weder g_i noch f_i'. (Beachte: Es ist $f_i' \neq 0$ nach obigem Lemma.) Also wird f' von keinem der f_i geteilt. Daher ist $\gcd(f, f')$ konstant.

(b) Sei $q = p^e$ und $f = X^N - 1$. Ist $\gcd(N, q) \neq 1$ so gilt $p \mid N$. Also ist $\gcd(f, f') = \gcd(f, NX^{N-1}) = \gcd(f, 0) = f$ nicht konstant. Ist $\gcd(N, q) \neq 1$, so ist $\gcd(f, NX^{N-1}) = 1$, denn es ist $X^N - 1 = (NX^{N-1})(N^{-1}X) - 1$. Die Behauptung folgt nun mit Teil (a).

(c) Es faktorisiert $X^4 - 1 \in \mathbb{F}_7[X]$ in die irreduziblen Faktoren $X - 1, X + 1$ und $X^2 + 1$. Der letzte Faktor ist irreduzibel da er vom Grad ≤ 3 ist und keine Nullstelle in $\mathbb{F}_7$ besitzt.

Es ergeben sich also die folgenden 8 Prüfpolynome:

$$g_1 := 1 \qquad g_2 := X + 1$$
$$g_3 := X - 1 \qquad g_4 := X^2 + 1$$
$$g_5 := (X + 1)(X - 1) = X^2 - 1 \qquad g_6 := (X + 1)(X^2 + 1) = X^3 + X^2 + X + 1$$
$$g_7 := (X - 1)(X^2 + 1) = X^3 - X^2 + X - 1 \qquad g_8 := X^4 - 1$$

Bezeichne G_i die zu g_i gehörende Erzeugermatrix, so erhalten wir:

$$G_1 = I_4 \qquad G_8 = 0 \in \mathbb{F}_7^{0 \times 4}$$
$$G_2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \qquad G_3 = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$
$$G_4 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \qquad G_5 = \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$
$$G_6 = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \qquad G_7 = \begin{pmatrix} 1 & -1 & 1 & -1 \end{pmatrix}$$

Ferner ist $g_i g_{9-i} = X^4 - 1$ für alle $1 \leq i \leq 8$. Also ist g_{9-i} ein Prüfpolynom von g_i. Bezeichne H_i die zugehörige Prüfmatrix, so erhalten wir:

$$H_1 = 0 \in \mathbb{F}_7^{4 \times 0} \qquad H_8 = I_4$$
$$H_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}^{\mathrm{tr}} \qquad H_3 = \begin{pmatrix} -1 & 1 & -1 & 1 \end{pmatrix}^{\mathrm{tr}}$$
$$H_4 = \begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}^{\mathrm{tr}} \qquad H_5 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}^{\mathrm{tr}}$$
$$H_6 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}^{\mathrm{tr}} \qquad H_7 = \begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix}^{\mathrm{tr}}$$