G. Nebe, M. Kirschmer

Gitter und Codes, WS 08/09

Lösung 3

Aufgabe 1.

(a) Für $1 \leq i \leq 8$ sei $b_i := e_i - e_{i+1}$ und setze $X := \langle b_1, \ldots, b_8, v\rangle_{\mathbb{Z}}$. In Aufgabe 1 auf Blatt 2 wurden $\mathbb{A}_8 = \langle b_1, \ldots, b_8\rangle_{\mathbb{Z}}$ und $\mathbb{A}_8^{\#} = \langle b_1, \ldots, b_8, u\rangle_{\mathbb{Z}}$ gezeigt, wobei $u = \frac{1}{9}(8e_1 - \sum_{i=2}^{9} e_i)$. Es ist

$$-3v = 2b_1 + 4b_2 + 6b_3 + 5b_4 + 4b_5 + 3b_6 + 2b_7 + b_8$$

Damit ist $b_8 \in \langle b_1, \ldots, b_7, v\rangle_{\mathbb{Z}}$ und daher ist $B_1 := (b_1, \ldots, b_7, v)$ eine $\mathbb{Z}$-Basis von X. Bezüglich dieser ergibt sich die Grammatrix

$$\begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

wie behauptet. Also sind X und $\mathbb{E}_8$ isometrisch und wir identifizieren nun X mit $\mathbb{E}_8$.

Es ist $3u + v = 2e_1 - e_2 - e_3 = 2b_1 + b_2 \in \mathbb{A}_8$, also $\mathbb{E}_8 \leq \mathbb{A}_8^{\#}$ und $v + \mathbb{A}_8 = 3u + \mathbb{A}_8$. Insbesondere folgt wegen $\mathbb{A}_8^{\#}/\mathbb{A}_8 \cong \mathbb{Z}/9\mathbb{Z}$ damit $[\mathbb{A}_8^{\#} : \mathbb{E}_8] = [\mathbb{E}_8 : \mathbb{A}_8^{\#}] = 3$. Da X ganz ist, folgt $\mathbb{A}_8 \lneq \mathbb{E}_8 \leq \mathbb{E}_8^{\#} \lneq \mathbb{A}_8^{\#}$ und also $\mathbb{E}_8 = \mathbb{E}_8^{\#}$.

(b) Es ist z.B. $B_2 := (e_1 - e_2, e_2 - e_3, \ldots, e_6 - e_7, v)$ eine Basis von $\langle w\rangle_{\mathbb{Z}}^{\perp, \mathbb{E}_8}$. Die Grammatrix bezüglich dieser Basis ist gegeben durch

$$\begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 2 \end{pmatrix}$$

wie behauptet. Also sind $\mathbb{E}_7$ und $\langle w\rangle_{\mathbb{Z}}^{\perp, \mathbb{E}_8}$ isometrisch.

Es ist $\langle w\rangle_{\mathbb{Z}} < \mathbb{E}_8$ ein reines Teilgitter, denn bezüglich der Basis B_1 hat w die Koordinaten

$$\begin{pmatrix} 2 & 4 & 6 & 5 & 4 & 3 & 2 & 3 \end{pmatrix}$$

und diese 1×8-Matrix hat Elementarteiler 1.

Mit Satz 1.29 folgt nun $\det(\mathbb{E}_7) = \det(\langle w\rangle^{\perp, \mathbb{E}_8}) = \det(\langle w\rangle) = (w, w) = 2$.

(c) Es ist z.B. $B_3 := (e_1 - e_2, e_2 - e_3, \ldots, e_5 - e_6, v)$ eine Basis von $\langle w, w'\rangle_{\mathbb{Z}}^{\perp, \mathbb{E}_8}$. Die Grammatrix bezüglich dieser Basis ist gegeben durch

$$\begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 \end{pmatrix}$$

wie behauptet. Also sind $\mathbb{E}_6$ und $\langle w, w'\rangle_{\mathbb{Z}}^{\perp, \mathbb{E}_8}$ isometrisch.

Es ist $\langle w, w'\rangle_{\mathbb{Z}} < \mathbb{E}_8$ ein reines Teilgitter, denn bezüglich der Basis B_1 hat die Basis (w, w') die Koordinaten

$$\begin{pmatrix} 2 & 4 & 6 & 5 & 4 & 3 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \end{pmatrix}$$

und diese Matrix hat Elementarteiler 1.

Mit Satz 1.29 folgt nun $\det(\mathbb{E}_6) = \det(\langle w, w'\rangle^{\perp, \mathbb{E}_8}) = \det(\langle w, w'\rangle_{\mathbb{Z}}) = \det \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} = 3$.

Aufgabe 2.

(a) Seien $S = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & -2 \\ 2 & 1 & 1 \end{pmatrix}$ und $T := \begin{pmatrix} 1 & 4 & -3 \\ 3 & -2 & 3 \\ 2 & -2 & 2 \end{pmatrix}$. Dann sind π_1 und π_2 bezüglich der Standardbasis von $V = \mathbb{R}^3$ gegeben durch $S_1 := S^{-1}\operatorname{Diag}(1,0,0)S = \frac{1}{2}\begin{pmatrix} -2 & -2 & -2 \\ 5 & 5 & 5 \\ -1 & -1 & -1 \end{pmatrix}$ bzw. $S_2 := S^{-1}\operatorname{Diag}(0,1,1)S = \frac{1}{2}\begin{pmatrix} 4 & 2 & 2 \\ -5 & -3 & -5 \\ 1 & 1 & 3 \end{pmatrix}$.

Daher bilden die Zeilen von TS_i ein Erzeugendensystem von $L'_i = L\pi_i$. Wegen $TS_1 = \frac{1}{2}\begin{pmatrix} 21 & 21 & 21 \\ -19 & -19 & -19 \\ -16 & -16 & -16 \end{pmatrix}$ ist also $B_1 = (\frac{1}{2}(1,1,1))$ eine $\mathbb{Z}$-Basis von L'_1.

Weiter ist $TS_2 = \frac{1}{2}\begin{pmatrix} -19 & -13 & -27 \\ 25 & 15 & 25 \\ 20 & 12 & 20 \end{pmatrix}$. Durch elementare Zeilenumformungen findet man nun ein $x \in \mathrm{GL}_3(\mathbb{Z})$ mit $xTS_2 = \frac{1}{2}\begin{pmatrix} 1 & -1 & -7 \\ 0 & 8 & 40 \\ 0 & 0 & 0 \end{pmatrix}$. Daher ist $B_2 = (\frac{1}{2}(1,-1,-7),(0,4,20))$ eine $\mathbb{Z}$-Basis von L'_2.

Es ist $L \cap U_1$ der Kern von $L \stackrel{\pi_2}{\to} L'_2$. Mit dem Elementarteilersatz findet man

$$\begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & -1 \\ 0 & -4 & 5 \end{pmatrix} \cdot T \cdot S_2 \cdot \begin{pmatrix} 0 & 5 & 2 \\ 2 & 1 & -5 \\ -1 & -4 & 1 \end{pmatrix} = \operatorname{Diag}(1/2, 4, 0)\,.$$

Also erzeugt $(0,4,-5)\cdot T = (2,2,2)$ das Gitter $L_1 = L \cap U_1$.

Analog ist $L \cap U_2$ der Kern von $L \stackrel{\pi_1}{\to} L'_1$. Mit dem Elementarteilersatz findet man

$$\begin{pmatrix} -1 & -2 & 1 \\ 2 & -2 & 5 \\ 3 & 5 & -2 \end{pmatrix} \cdot T \cdot S_1 \cdot \begin{pmatrix} 1 & -1 & -1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \operatorname{Diag}(1/2, 0, 0)\,.$$

Also bilden $(2,-2,5)\cdot T = (6,2,-2)$ und $(3,5,-2)\cdot T = (14,6,2)$ eine $\mathbb{Z}$-Basis von L'_2.

(b) Sicher ist $L'_1/L_1 \cong \mathbb{Z}/4\mathbb{Z}$.

Bezüglich der in (a) gefundenen Basen wird die Inklusion $L_2 \to L'_2$ beschrieben durch $\begin{pmatrix} 12 & 2 \\ 28 & 5 \end{pmatrix}$ und diese Matrix hat Elementarteiler $(1,4)$. Also ist $L'_2/L_2 \cong \mathbb{Z}/4\mathbb{Z}$.

Die Einbettung $L \to L'_1 \oplus L'_2$ wird bezüglich der der in (a) gefundenen Basen beschrieben durch $\begin{pmatrix} 21 & -19 & -4 \\ -19 & 25 & 5 \\ -16 & 20 & 4 \end{pmatrix}$. Diese Matrix hat Elementarteiler $(1,1,4)$. Also ist $L'_1 \oplus L'_2/L \cong \mathbb{Z}/4\mathbb{Z}$.

Die Einbettung $L_1 \oplus L_2 \to L$ wird bezüglich der der in (a) gefundenen Basen beschrieben durch $\begin{pmatrix} 0 & 4 & -5 \\ 2 & -2 & 5 \\ 3 & 5 & -2 \end{pmatrix}$. Diese Matrix hat Elementarteiler $(1,1,4)$. Also ist ebenfalls $L/L_1 \oplus L_2 \cong \mathbb{Z}/4\mathbb{Z}$.

Aufgabe 3.

(a) Eine Erzeugermatrix in strikter Zeilenstufenform ist z.B. gegeben durch

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

Damit wird

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

eine Prüfmatrix von C.

In dieser sind alle Zeilentupel der Länge 1 linear unabhängig (d.h. es gibt keine Nullzeile). Wohl aber ist das Zeilentupel der Länge 2, welches aus der 3ten und der 4ten Zeile besteht, linear abhängig. Es folgt $d(C) = 2$.

(b) Angenommen, es gibt eine (ohne Einschränkung) nicht-negative ganze Zahl e so, daß es zu jedem $a \in \mathbb{F}_4^{1\times 6}$ genau ein $c \in C$ mit $d(c,a) \leq e$ gibt. Wegen $C \neq \mathbb{F}_4^{1\times 6}$ ist $e \geq 1$. Aber für $a = (0,0,1,0,0,0)$ ist dann $d(0,a) = d((0,0,1,1,0,0),a) = 1 \leq e$ ein Widerspruch. Also ist C nicht perfekt.

(c) Für einen MDD haben wir in jeder Nebenklasse in $\mathbb{F}_4^{1\times 6}/C$ ein Element minimaler Länge zu bestimmen. Es genügt, dies bis auf $\mathbb{F}_4^*$-Vielfache durchzuführen. Betrachtet man nun sukzessive Linearkombinationen von $0,1,2,3,\ldots$ Zeilen von P, so ergibt sich z.B.

Syndrom s bzgl. P	Vertreter minimalen Gewichts in $\{x \in \mathbb{F}_4^{1\times 6} \mid xP = s\}$
$(0,0,0)$	$(0,0,0,0,0,0)$
$(0,0,1)$	$(0,0,0,0,0,1)$
$(0,1,0)$	$(0,0,1,0,0,0)$
$(0,1,1)$	$(0,0,1,0,0,1)$
$(0,1,\omega)$	$(0,0,0,1,1,0)$
$(0,1,\omega^2)$	$(0,0,0,1,\omega,0)$
$(1,0,0)$	$(0,1,0,0,0,0)$
$(1,0,1)$	$(0,1,0,0,0,1)$
$(1,0,\omega)$	$(0,1,0,0,0,\omega)$
$(1,0,\omega^2)$	$(0,1,0,0,0,\omega^2)$
$(1,1,0)$	$(0,1,1,0,0,0)$
$(1,1,1)$	$(\omega^2,0,0,0,1,0)$
$(1,1,\omega)$	$(\omega^2,0,0,0,\omega^2,0)$
$(1,1,\omega^2)$	$(\omega^2,0,0,0,0,0)$
$(1,\omega,0)$	$(0,1,\omega,0,0,0)$
$(1,\omega,1)$	$(1,\omega^2,0,0,0,0)$
$(1,\omega,\omega)$	$(0,1,\omega,0,1,0)$
$(1,\omega,\omega^2)$	$(\omega^2,0,\omega^2,0,0,0)$
$(1,\omega^2,0)$	$(0,1,\omega^2,0,0,0)$
$(1,\omega^2,1)$	$(0,1,\omega^2,0,0,1)$
$(1,\omega^2,\omega)$	$(\omega,\omega,0,0,0,0)$
$(1,\omega^2,\omega^2)$	$(\omega^2,0,\omega,0,0,0)$

(d) Das Syndrom von $x = (1,\omega^2,1,1,\omega,0)$ ist $xP = (1,\omega,\omega)$. Folglich decodiert x bzgl. unseres MDD aus (c) zu

$$x - (0,1,\omega,0,1,0) = (1,\omega,\omega^2,1,\omega^2,0)\,.$$