Übungsblatt 11

Aufgabe 1. (a) Sei $\Gamma = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n \mid \sum_{i=1}^n x_i \equiv 0 \mod 2\}$. Bestimmen Sie eine Basis von Γ und überprüfen Sie, ob Γ ganzzahlig bzw. unimodular ist.

(b) Sei $\Gamma' = \Gamma + \mathbb{Z}\, u$, wobei $u = \frac{1}{2}(e_1 + \ldots + e_n)$ ist. Bestimmen Sie eine Basis von Γ' und wann Γ' ganzzahlig bzw. unimodular ist.

(a) Zunächst betrachten wir $\widetilde{\Gamma} = \langle v_1, \ldots, v_n \rangle_{\mathbb{Z}}$ mit $v_1 = 2e_1$ und $v_i := e_1 - e_i$ für $2 \le i \le n$. Da $\langle v_1, \ldots, v_n \rangle_{\mathbb{R}} = \mathbb{R}^n$ gilt, ist $\widetilde{\Gamma}$ ein volles Gitter in $\mathbb{R}^n$.

Im Folgenden wollen wir zeigen, dass $\Gamma = \widetilde{\Gamma}$. Offensichtlich gilt $\widetilde{\Gamma} \subseteq \Gamma$ und $\mathbb{Z}^n/\widetilde{\Gamma} = \{0, \overline{e_1}\}$. Also liefert die Vorlesung

$$2 = |\mathbb{Z}^n/\widetilde{\Gamma}| = |\mathbb{Z}^n/\Gamma| \cdot |\Gamma/\widetilde{\Gamma}|.$$

Da $\mathbb{Z}^n \neq \Gamma$ ist, erhalten wir $|\Gamma/\widetilde{\Gamma}| = 1$, d.h. $\Gamma = \widetilde{\Gamma}$.

Es gilt $\langle x, y \rangle \in \mathbb{Z}$ für alle $x, y \in \Gamma$, d.h. Γ ist ganzzahlig.

Es gilt $\mathrm{vol}(\mathbb{Z}^n/\Gamma) = |\det(v_1^t, \ldots, v_n^t)| = 2$ und wegen

$$\mathrm{vol}(\mathbb{R}^n/\Gamma^\star) = 1/\mathrm{vol}(\mathbb{R}^n/\Gamma)$$

ist Γ ist nicht unimodular.

(b) Sei n zunächst gerade, so bilden die linear unabhängigen Vektoren $v_1, \ldots, v_{n-1}, u$ eine Basis von Γ', denn

$$v_n = \begin{cases} e_1 - e_2 = -2u + v_1 & , n = 2 \\ 2u - \frac{n-2}{2} v_1 + \sum_{i=2}^{n-1} v_i & , \text{sonst.} \end{cases}$$

Ist n ungerade betrachte die linear unabhängigen Vektoren $u, \widetilde{v_i} := (-1)^i e_1 - e_i$ für $2 \le i \le n$. Analog zum ersten Aufgabenteil kann man nachrechnen, dass $v_1 = 2e_1, \widetilde{v_i}$ für $2 \le i \le n$ eine Basis von Γ ist. Nun ist wegen

$$v_1 = 2e_1 = 2u + \sum_{i=2}^{n} \widetilde{v_i}$$

das lineare unabhängige System $u, \widetilde{v_i}$ für $2 \le i \le n$ eine Basis von Γ'.

Das Gitter Γ' ist genau dann ganzzahlig, wenn $4 \mid n$. Dies kann man wie folgt elementar nachrechnen. Seien $x, y \in \Gamma$ und $l, m \in \mathbb{Z}$, so gilt

$$\begin{aligned} \langle x + lu, y + mu \rangle &= \langle x, y \rangle + m\langle x, u \rangle + l\langle u, y \rangle + lm\langle u, u \rangle \\ &= \langle x, y \rangle + \frac{m}{2}\langle x, (1, \ldots, 1) \rangle + \frac{l}{2}\langle (1, \ldots, 1), y \rangle + \frac{lm}{4} n. \end{aligned}$$

Die ersten drei Summanden sind wegen der Definition von Γ ganze Zahlen, wobei der letzte eine ganze Zahl für beliebige $l, m \in \mathbb{Z}$ ist, wenn $4 \mid n$.

Das Gitter Γ' ist genau dann unimodular, wenn $4 \mid n$. Wegen der Ganzzahligkeit für $4 \mid n$ besitzt jede Grammatrix von Γ' ganzzahlige Koeffizienten. Des Weiteren gilt für die Matrix

$$A = \begin{pmatrix} & \cdots & & \frac{1}{2} \\ v_1^t & \ldots & v_{n-1}^t & \vdots \\ & \cdots & & \frac{1}{2} \end{pmatrix}$$

$$\mathrm{vol}(\mathbb{R}^n/\Gamma') = |\det(A)| = 1.$$

So folgt aus Proposition 14.5, dass Γ' unimodular ist.

Aufgabe 2. Sei C der binäre Code mit Erzeugermatrix

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

Bestimmen Sie das Codegitter Γ_C. Ist Γ_C isometrisch zu dem Standardgitter?

Es gilt $C = \{(0,0,0,0),(1,1,1,0),(0,1,1,1),(1,0,0,1)\}$. Es sei $\rho : \mathbb{Z}^4 \longrightarrow \mathbb{F}_2^4$ der in der Vorlesung definierte Gruppenhomomorphismus, so gilt für alle $c \in C$ offensichtlich $\rho^{-1}(c) = c + (2\mathbb{Z})^4$. Wir zeigen im Folgenden, dass

$$\rho^{-1}(C) = \mathbb{Z}(1,1,1,0) \oplus \mathbb{Z}(0,1,1,1) \oplus \mathbb{Z}(2,2,0,0) \oplus \mathbb{Z}(0,0,2,2).$$

Es gilt

$$\begin{aligned} -2(1,1,1,0) + (2,2,0,0) + (0,0,2,2) &= (0,0,0,2) \\ 2(1,1,1,0) - (2,2,0,0) &= (0,0,2,0) \\ 2(0,1,1,1) - (0,0,2,2) &= (0,2,0,0) \\ -2(0,1,1,1) + (2,2,0,0) + (0,0,2,2) &= (2,0,0,0). \end{aligned}$$

Aus letzterem folgt, dass $\rho^{-1}(C) = \bigcup_{c\in C} \rho^{-1}(c) = \mathbb{Z}(1,1,1,0) \oplus \mathbb{Z}(0,1,1,1) \oplus \mathbb{Z}(2,2,0,0) \oplus \mathbb{Z}(0,0,2,2)$. Somit ist das Wurzelgitter

$$\Gamma_C = \frac{1}{\sqrt{2}}\rho^{-1}(C) = \frac{1}{\sqrt{2}}\mathbb{Z}(1,1,1,0) \oplus \frac{1}{\sqrt{2}}\mathbb{Z}(0,1,1,1) \oplus \frac{1}{\sqrt{2}}\mathbb{Z}(2,2,0,0) \oplus \frac{1}{\sqrt{2}}\mathbb{Z}(0,0,2,2).$$

Angenommen es existiert eine Isometrie und sie ist durch $\phi : \Gamma_C \longrightarrow \mathbb{Z}^4$ gegeben. So erhalten wir

$$\frac{3}{2} = \left\langle \frac{1}{\sqrt{2}}(1,1,1,0), \frac{1}{\sqrt{2}}(1,1,1,0) \right\rangle = \left\langle \phi\left(\frac{1}{\sqrt{2}}(1,1,1,0)\right), \phi\left(\frac{1}{\sqrt{2}}(1,1,1,0)\right) \right\rangle.$$

Allerdings ist $\mathbb{Z}^4$ ganzzahlig und somit erhalten wir einen Widerspruch.
Alternativ, gilt wegen $C \nsubseteq C^\perp$ und Lemma 14.7, dass Γ_C nicht ganzzahlig ist. Da $\mathbb{Z}^4$ allerdings ganzzahlig ist, können Γ_c und $\mathbb{Z}^4$ nicht isometrisch sein.

Lemma. *Sei C der binäre $[n = 2^k - 1, n - k, 3]$ Hamming-Code, so gilt*

$$A_C(x) = \frac{1}{n+1}\left((1+x)^n + n(1-x)(1-x^2)^{\frac{n-1}{2}}\right).$$

Beweis. Da der duale Code $C^\perp$ ein Simplex-Code mit Parametern $[n, k, 2^{k-1}]$ ist und alle von Null verschiedenen Codewörter Gewicht 2^{k-1} haben, gilt

$$A_{C^\perp}(x) = 1 + (2^k - 1)x^{2^{k-1}}.$$

Der Dualitätssatz von MacWilliams liefert nun

$$\begin{aligned} A_C(x) = A_{(C^\perp)^\perp} &= 2^{-k}(1+x)^n A_{C^\perp}\left(\frac{1-x}{1+x}\right) \\ &= 2^{-k}(1+x)^n\left(1 + (2^k - 1)\left(\frac{1-x}{1+x}\right)^n\right). \end{aligned}$$

Letzteres liefert nun (mit einer kleinen Rechnung)

$$A_i = \begin{cases} \frac{1}{n+1}\left(\binom{n}{i} + n(-1)^{\frac{i}{2}}\binom{\frac{n-1}{2}}{\frac{i}{2}}\right) & \text{, für i gerade} \\ \frac{1}{n+1}\left(\binom{n}{i} + n(-1)^{\frac{i+1}{2}}\binom{\frac{n-1}{2}}{\frac{i-1}{2}}\right) & \text{, sonst.} \end{cases}$$

□

Aufgabe 3. Es sei $C = \mathrm{Ham}_2(3)$ der binäre $[7,4,3]$-Hamming-Code.

(a) Zeigen Sie, dass C das Gewichtspolynom $A(x) = 1 + 7x^3 + 7x^4 + x^7$ hat.

Berechnen Sie für C

(b) die Wahrscheinlichkeit für einen unentdeckten Fehler.

(c) die Decodierfehlerwahrscheinlichkeit bei Korrektur eines Fehlers, wenn zur Übertragung ein binär symmetrischer Kanal mit der Symbolfehlerwahrscheinlichkeit $p = 0,01$ benutzt wird.

(a) *Beweis.* Die Formel aus dem obigen Lemma liefert das entsprechende Gewichtspolynom. □

(b) Die Wahrscheinlichkeit eines unentdeckten Fehlers lautet

$$\sum_{i=1}^{n} A_i \left(\frac{p}{q-1}\right)^i (1-p)^{n-i} = p^7 - 7p^6 + 21p^5 - 21p^4 + 7p^3.$$

(c) Die Decodierfehlerwahrscheinlichkeit lautet nach Vorlesung für $t = 1$ und $p = 0,01$

$$\sum_{i=1}^{n} A_i \sum_{j=0}^{t} \sum_{s=0}^{j} \left(\binom{i}{s} \left(\frac{p}{q-1}\right)^{i-s} \left(1 - \frac{p}{q-1}\right) \binom{n-i}{j-s} p^{j-s} (1-p)^{n-i-j+s} \right) \approx 0,2\%$$

Aufgabe 4. Sei $C \neq 0$ ein perfekter $[n,k,d]$-Code über $\mathbb{F}_2$, wobei $d = 2e+1$ ist. Zeigen Sie, dass

$$A_d = \frac{\binom{n}{e+1}}{\binom{d}{e}}.$$

Beweis. Wir zählen analog zu Blatt 10 Aufgabe 1 alle Vektoren des $\mathbb{F}_2^n$ vom Gewicht $e+1$. Einerseits gibt es genau $\binom{n}{e+1}$ viele Vektoren vom Gewicht $e+1$. Andererseits verteilen sie sich auf e-Sphären um Codewörter vom Gewicht d, denn sei $v \in B_e(c) \subseteq \mathbb{F}_2^n$ vom Gewicht $e+1$ und $c \in C$ mit $\mathrm{wt}(c) > d$. Somit gilt

$$e \geq d(v,c) = \mathrm{wt}(v+c) = \mathrm{wt}(c) + \mathrm{wt}(v) - 2|\mathrm{Tr}(c) \cap \mathrm{Tr}(v)| \geq d + 1 + (e+1) - 2(e+1) = e+1,$$

ein Widerspruch. In jeder e-Sphäre befinden sich genau $\binom{d}{e}$ Vektoren vom Gewicht $e+1$. Insgesamt erhalten wir

$$\binom{n}{e+1} = A_d \binom{d}{e}.$$

□