Klassifikation gerader unimodularer Gitter in Dimension 24

Seminar Gitter und Codes, 23. Mai 2011

Carmen Stein

Inhaltsverzeichnis

1 Einleitung 2

2 Wurzelsysteme in geraden unimodularen Gittern 2

3 Gitter mit Wurzelsystemen von maximalem Rang 6

4 Die Klassifikation der geraden unimodularen Gitter in Dimension 24 8

§ 1 Einleitung

Wir betrachten hier gerade unimodulare Gitter Γ im $\mathbb{R}^n$. Es ist bekannt, dass es diese Gitter nur für $n = 8k, k \in \mathbb{N}$ gibt. Für $k = 1, 2, 3$ ist eine komplette Klassifikation bekannt, für $k = 4$ hingegen gibt es schon über 80 Millionen Gitter. Für $k = 1$ und 2 ist die Klassifikation sehr einfach (siehe §2).
Die Klassifikation der geraden unimodularen Gitter in Dimension 24 wurde als erstes von Niemeier 1968 durchgeführt. Demnach ist jedes Gitter Γ eindeutig durch sein Wurzelsystem $\Gamma_2 = \{x \in \Gamma : (x, x) = 2\}$ bestimmt, wobei Γ_2 eines der folgenden Wurzelsysteme ist:
$\emptyset$,
$24\mathbb{A}_1, 12\mathbb{A}_2, 8\mathbb{A}_3, 6\mathbb{A}_4, 4\mathbb{A}_6, 3\mathbb{A}_8, 2\mathbb{A}_{12}, \mathbb{A}_{24}$,
$6\mathbb{D}_4, 4\mathbb{D}_6, 3\mathbb{D}_8, 2\mathbb{D}_{12}, \mathbb{D}_{24}$,
$4\mathbb{E}_6, 3\mathbb{E}_8$,
$4\mathbb{A}_5 + \mathbb{D}_4, 2\mathbb{A}_7 + 2\mathbb{D}_5, 2\mathbb{A}_9 + \mathbb{D}_6, \mathbb{A}_{15} + \mathbb{D}_9, \mathbb{E}_8 + \mathbb{D}_{16}, 2\mathbb{E}_7 + \mathbb{D}_{10}, \mathbb{E}_7 + \mathbb{A}_{17}, \mathbb{E}_6 + \mathbb{D}_7 + \mathbb{A}_{11}$

§ 2 Wurzelsysteme in geraden unimodularen Gittern

Vorab eine Definition, da diese hier benötigt wird, in den vorherigen Vorträgen aber nicht vorkam:

(2.1) Definition
Zu einem irreduziblen Wurzelgitter $\Gamma \subset \mathbb{R}^n$ definieren wir die *Coxeter Zahl*

$$h := \frac{|R(\Gamma)|}{n}$$

als die Anzahl der Wurzeln in Γ durch die Dimension n.

Um das erste Lemma zu beweisen, benötigen wir die folgende Bemerkung über die Theta-Reihe eines geraden unimodularen Gitters.

(2.2) Bemerkung
Sei $\Gamma \subset \mathbb{R}^n$ ein gerades unimodulares Gitter und P ein Polynom mit sphärischen Koeffizienten in n Varibalen und $\deg(P) = r$. Dann ist $\vartheta_{\Gamma,P}$ eine Modulform vom Gewicht $\frac{n}{2} + r$ und eine Spitzenform, falls $r > 0$ gilt.

Beweis. Für ein gerades unimodulares Gitter gilt immer, dass Level N und Diskriminante d gleich 1 sind. Dann folgt der erste Teil der Behauptung mit der Gleichung

$$\vartheta_{\Gamma,P}(A\tau)(c\tau + d)^{-\frac{n}{2}+r} = \vartheta_{\Gamma,P},$$

die für alle A in $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ gilt, wobei $(\cdot)$ das Legendre-Symbol bezeichne.
Zum zweiten Teil: Es ist

$$\vartheta_{\Gamma,P} = \sum_{s=0}^{\infty} \left(\sum_{x \in \Gamma : x^2 = 2s} P(x) \right) q^s$$

mit $q := e^{2\pi i \tau}$. Für $r > 0$ gilt $c_0 = P(0) = 0$, also ist $\vartheta_{\Gamma,P}$ eine Spitzenform. □

(2.3) Lemma
Sei $\Gamma \subset \mathbb{R}^n$ ein gerades unimodulares Gitter und $n \in \{8, 16, 24\}$. Dann gilt für ein fixes $y \in \mathbb{R}^n$

$$\sum_{x \in \Gamma : x^2 = 2r} (x \cdot y)^2 - \left(\sum_{x \in \Gamma : x^2 = 2r} x^2 \right) \frac{y^2}{n} = 0.$$

Insbesondere gilt die folgende Gleichung für die Wurzeln in Γ:

$$\sum_{x \in \Gamma_2} (x \cdot y)^2 = \frac{2}{n} |\Gamma_2| \cdot y^2. \tag{1}$$

Beweis. Sei $f(x) := (x \cdot y)^2 - \frac{x^2 y^2}{n}$. f ist harmonisch, denn es ist

$$\Delta f = \Delta(x_1 y_1 + ... + x_n y_n)^2 - \frac{1}{n} \Delta(y^2 (x_1^2 + ... + x_n^2)) = 2(y_1^2 + ... + y_n^2) - \frac{2n}{n} y^2 = 0.$$

Nach (2.2) ist $\vartheta_{\Gamma,f}$ eine Spitzenform des Gewichts $\frac{n}{2} + 2$, für $n = 8, 16, 24$ also vom Gewicht 6, 10, 14. Diese sind bekannterweise identisch 0, folglich sind alle Koeffizienten von $\vartheta_{\Gamma,f}(\tau) = \sum_{r=0}^{\infty} c_r q^r$ gleich 0. □

(2.4) Folgerung
Sei $\Gamma \subset \mathbb{R}^n$ ein gerades unimodulares Gitter und $n \in \{8, 16, 24\}$. Dann gilt für das Wurzelsystem Γ_2 entweder $\Gamma_2 = \emptyset$ oder $\langle \Gamma_2 \rangle = \mathbb{R}^n$.

Beweis. Es gelte $\langle \Gamma_2 \rangle \neq \mathbb{R}^n$. Dann gibt es ein $y \in \mathbb{R}^n - \{0\}$, welches orthogonal zu allen Elementen aus Γ_2 ist. Dann folgt aber mit der Gleichung (1), dass $|\Gamma_2| = 0$ gilt. □

Es bezeichne von nun an $(\Gamma_2)_{\mathbb{Z}}$ das von Γ_2 aufgespannte Wurzelgitter.

(2.5) Folgerung
Sei $\Gamma \subset \mathbb{R}^n$ ein gerades unimodulares Gitter und $n = 8, 16, 24$. Dann haben alle irreduziblen Komponenten des Wurzelgitters $(\Gamma_2)_{\mathbb{Z}}$ dieselbe Coxeter Zahl, nämlich $h = \frac{1}{n} |\Gamma_2|$.

Beweis. Für das Wurzelsystem Γ_2 eines irreduziblen Wurzelgitters und ein fixes $y \in \mathbb{R}^n$ gilt

$$\sum_{x \in \Gamma_2} (x \cdot y)^2 = 2 \cdot h \cdot y^2.$$

Wählt man nun $y \in \mathbb{R}^n$ so, dass es in einer irreduziblen Komponente des Wurzelgitters $(\Gamma_2)_{\mathbb{Z}}$ liegt, folgt die Behauptung mit der Gleichung (1). □

Das folgende Lemma fasst die Eigenschaften eines nicht-leeren Wurzelsystems zusammen.

(2.6) Lemma
Sei $\Gamma \subset \mathbb{R}^{24}$. Ist $\Gamma_2 \neq \emptyset$, so besitzt das Wurzelsystem Γ_2 in $\mathbb{R}^{24}$ die folgenden Eigenschaften:

(i) $\operatorname{rang}(\Gamma_2) = 24$,

(ii) alle irreduziblen Komponenten von Γ_2 haben dieselbe Coxeter Zahl h,

(iii) $|\Gamma_2| = 24h$.

(2.7) Beispiel
Für $n = 8$ gilt $(\Gamma_2)_{\mathbb{Z}} = \mathbb{E}_8$ und $\mathbb{E}_8$ ist das einzige gerade unimodulare Gitter in $\mathbb{R}^8$ (Ebeling Proposition(2.5)).
Für $n = 16$ und $\Gamma \subset \mathbb{R}^{16}$ ist ϑ_Γ eine Modulform vom Gewicht 8. Da $M = \mathbb{C}[E_4, E_6]$ gilt, ist $\vartheta_\Gamma = E_4^2$. Folglich ist $|\Gamma_2| = 480$ und die Coxeter Zahl ist $h = 30$. Es gilt $\langle \Gamma_2 \rangle = \mathbb{R}^{16}$ also

$$(\Gamma_2)_{\mathbb{Z}} = \mathbb{E}_8 + \mathbb{E}_8 \text{ oder } (\Gamma_2)_{\mathbb{Z}} = \mathbb{D}_{16}.$$

Dies sind die beiden einzigen Möglichkeiten in $\mathbb{R}^{16}$.

Mit den Eigenschaften aus (2.6) können wir dann das Hauptergebnis dieses Abschnittes zeigen:

(2.8) Lemma
Sei Γ_2 ein Wurzelsystem in $\mathbb{R}^{24}$. Γ_2 erfülle die Bedingungen (i) - (iii) in (2.5), dann ist Γ_2 isomorph zu einem der folgenden 23 Wurzelsysteme:
$24\mathbb{A}_1, 12\mathbb{A}_2, 8\mathbb{A}_3, 6\mathbb{A}_4, 4\mathbb{A}_6, 3\mathbb{A}_8, 2\mathbb{A}_{12}, \mathbb{A}_{24}$,
$6\mathbb{D}_4, 4\mathbb{D}_6, 3\mathbb{D}_8, 2\mathbb{D}_{12}, \mathbb{D}_{24}$,
$4\mathbb{E}_6, 3\mathbb{E}_8$,
$4\mathbb{A}_5 + \mathbb{D}_4, 2\mathbb{A}_7 + 2\mathbb{D}_5, 2\mathbb{A}_9 + \mathbb{D}_6, \mathbb{A}_{15} + \mathbb{D}_9, \mathbb{E}_8 + \mathbb{D}_{16}, 2\mathbb{E}_7 + \mathbb{D}_{10}, \mathbb{E}_7 + \mathbb{A}_{17}, \mathbb{E}_6 + \mathbb{D}_7 + \mathbb{A}_{11}$

Beweis. Die Komponenten von Γ_2 können $\mathbb{A}_i, \mathbb{D}_j$ und $\mathbb{E}_k$ sein. Sei also

$$\Gamma_2 = \sum_{i=1}^{24} \alpha_i \mathbb{A}_i + \sum_{j=1}^{24} \beta_j \mathbb{D}_j + \sum_{k=6}^{8} \gamma_k \mathbb{E}_k.$$

Die Werte der Coxeter Zahlen dieser Gitter sind: $h(\mathbb{A}_l) = l+1, h(\mathbb{D}_l) = 2l-2, h(\mathbb{E}_6) = 12, h(\mathbb{E}_7) = 18, h(\mathbb{E}_8) = 30$.
Nach (ii) müssen alle irreduziblen Komponenten dieselbe Coxeter Zahl haben, folglich können jeweils höchstens ein α_i, ein β_j und ein γ_k ungleich 0 sein. Gilt $\alpha_i \neq 0$ für ein i und $\beta_j \neq 0$ für ein j, so folgt $i = 2j-3$. Genauso gilt, falls $\alpha_i \neq 0$ für ein i und $\gamma_k \neq 0$ für ein k: $i = 11$ für $k = 6$, $i = 17$ für $k = 7$ und $i = 29$ für $k = 8$. Sind $\beta_j \neq 0$ für ein j und $\gamma_k \neq 0$ für ein k, so folgt: $j = 7$ für $k = 6$, $j = 10$ für $k = 7$ und $j = 16$ für $k = 8$.
Folglich hat Γ_2 eine der folgenden Formen:

(1) $\Gamma_2 = \alpha_i \mathbb{A}_i$ für ein i,

(2) $\Gamma_2 = \beta_j \mathbb{D}_j$ für ein j,

(3) $\Gamma_2 = \gamma_k \mathbb{E}_k$ für ein k,

(4) $\Gamma_2 = \alpha_{2j-3}\mathbb{A}_{2j-3} + \beta_j \mathbb{D}_j$ für gewisse $\alpha_{2j-3} \neq 0, \beta_j \neq 0$,

(5) $\Gamma_2 = \alpha_{11}\mathbb{A}_{11} + \beta_7\mathbb{D}_7 + \gamma_6\mathbb{E}_6, \gamma_6 \neq 0, \alpha_{11}$ oder β_7 positiv,

(6) $\Gamma_2 = \alpha_{17}\mathbb{A}_{17} + \beta_{10}\mathbb{D}_{10} + \gamma_7\mathbb{E}_7, \gamma_7 \neq 0, \alpha_{17}$ oder β_{10} positiv,

(7) $\Gamma_2 = \alpha_{29}\mathbb{A}_{29} + \beta_{16}\mathbb{D}_{16} + \gamma_8\mathbb{E}_8, \gamma_8 \neq 0, \beta_{16}$ positiv.

Bedingung (i) aus (2.5) bedeutet, dass

$$\sum_{i,j,k} i\alpha_i + j\beta_j + k\gamma_k = 24$$

gilt. Insgesamt ergeben sich damit die folgenden Möglichkleiten für Γ_2.

(1) $24\mathbb{A}_1, 12\mathbb{A}_2, 8\mathbb{A}_3, 6\mathbb{A}_4, 4\mathbb{A}_6, 3\mathbb{A}_8, 2\mathbb{A}_{12}, \mathbb{A}_{24}$

(2) $6\mathbb{D}_4, 4\mathbb{D}_6, 3\mathbb{D}_8, 2\mathbb{D}_{12}, \mathbb{D}_{24}$

(3) $4\mathbb{E}_6, 3\mathbb{E}_8$

Im Fall (4) besagt (i): $j\beta_j + (2j-3)\alpha_{2j-3} = 24$ mit $j \geq 4, \beta_j \geq 1$ und $\alpha_{2j-3} \geq 1$ ganzzahlig. Nachrechnen ergibt die folgenden Lösungen: $(j, \alpha, \beta) = (4,4,1), (5,2,2), (6,2,1)$ und $(9,1,1)$. Also erhält man

(4) $4\mathbb{A}_5 + \mathbb{D}_4, 2\mathbb{A}_7 + 2\mathbb{D}_5, 2\mathbb{A}_9 + \mathbb{D}_6, \mathbb{A}_{15} + \mathbb{D}_9$

Im nächsten Fall bedeutet (i), dass $11\alpha_{11} + 7\beta_7 + 6\gamma_6 = 24$ gilt. Dies ergibt die folgende Möglichkeit

(5) $\mathbb{E}_6 + \mathbb{D}_7 + \mathbb{A}_{11}$

Im letzten Fall erhalten wir $16\beta_{16} + 8\gamma_8 = 24$, also

(6) $\mathbb{E}_8 + \mathbb{D}_{16}$

Dies sind alle oben aufgelisteten Gitter. □

(2.9) Folgerung
Sei $\Gamma \subset \mathbb{R}^{24}$ ein gerades unimodulares Gitter. Dann gilt entweder $\Gamma_2 = \emptyset$ oder Γ_2 ist eines der 23 in (2.7) aufgelisteten Wurzelsysteme.

§ 3 Gitter mit Wurzelsystemen von maximalem Rang

Wir wollen nun einige Eigenschaften gerader unimodularer Gitter mit maximalem Wurzelsystem untersuchen. Dabei werden wir nur solche betrachten, wo die Wurzeln alle dieselbe Länge haben, also die irreduziblen Komponenten vom Typ $\mathbb{A}_i, \mathbb{D}_j$ und $\mathbb{E}_k$ sind. Dazu führen wir folgendes ein: Jedem irreduziblen Wurzelsystem $\Gamma_2 \neq \mathbb{E}_8$ ordnen wir ein Tripel $(T(\Gamma_2), G(\Gamma_2), l_{\Gamma_2})$ zu, wobei $T(\Gamma_2) = (\Gamma_2)^{\#}_{\mathbb{Z}}/(\Gamma_2)_{\mathbb{Z}}$ eine endliche abelsche Gruppe, $G(\Gamma_2) = Aut(\Gamma_2)/W(\Gamma_2)$ eine endliche Gruppe, die auf $T(\Gamma_2)$ operiert und $l_{\Gamma_2}(x) = \min\{y^2 : y \in \Gamma_2^{\#}, \overline{y} = x \in T(\Gamma_2)\}$ eine $\mathbb{R}$-wertige, $G(\Gamma_2)$-invariante Längenfunktion auf $T(\Gamma_2)$ ist. Im Einzelnen ist dieses Tripel wie folgt definiert:

(1) Für $\Gamma_2 = \mathbb{A}_i$ ist $T(\mathbb{A}_i) = \mathbb{Z}/(i+1)\mathbb{Z}$ sowie $G(\mathbb{A}_1) = 1$ und $G(\mathbb{A}_i) = C_2$ für $i > 1$. Ein nichttriviales Element $\sigma \in G(\mathbb{A}_i), i > 1$ operiert auf $T(\mathbb{A}_i)$ wie die Multiplikation mit -1, also $\sigma(k) = i + 1 - k$. Ferner ist $l_{\mathbb{A}_i}(k) = \frac{k(i+1-k)}{i+1}$.

(2) Für $\Gamma_2 = \mathbb{D}_j$ mit $j \geq 4$ ist

$$T(\mathbb{D}_j) = \{d_0, d_1, d_2, d_3\} = \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{, falls } j \equiv 0 \pmod 2, \\ \mathbb{Z}/4\mathbb{Z} & \text{, falls } j \equiv 1 \pmod 2. \end{cases}$$

d_0 sei das Nullelement der additiven Gruppe $T(\mathbb{D}_j)$ und es sei $d_i \equiv i \pmod 4$ für ungerade j. Weiter ist $G(\mathbb{D}_4) = S_3 = Aut(T(\mathbb{D}_4))$ und $G(\mathbb{D}_j) = C_2$ für $j \geq 5$. Ein nichttriviales Element $\sigma \in C_2$ fixiert d_0 und d_2 und $\sigma(d_1) = d_3$. $l_{\mathbb{D}_j}$ ist wie folgt definiert: $l(d_0) = 0, l(d_1) = l(d_3) = \frac{j}{4}, l(d_2) = 1$.

(3) Für $\Gamma_2 = \mathbb{E}_6$ ist $T(\mathbb{E}_6) = \mathbb{Z}/3\mathbb{Z}, G(\mathbb{E}_6) = C_2 = \{\sigma\}$ mit $\sigma(1) = 2$ und $l(0) = 0, l(1) = l(2) = \frac{4}{3}$.

(4) Für $\Gamma_2 = \mathbb{E}_7$ ist $T(\mathbb{E}_7) = \mathbb{Z}/2\mathbb{Z}, G(\mathbb{E}_7) = 1$ und $l(0) = 0, l(1) = \frac{3}{2}$.

Für ein Wurzelsystem der Form $n\Gamma_2$ mit $\Gamma_2 \neq \mathbb{E}_8$, setzen wir $T(n\Gamma_2) = T(\Gamma_2)^n$ und $G(n\Gamma_2)$ als das natürliche semidirekte Produkt $G(n\Gamma_2) = G(\Gamma_2)^n \rtimes S_n$ mit der natürlichen monomialen Operation auf $T(n\Gamma_2)$. Ferner definieren wir l durch Additivität als $l(x_1, ..., x_n) = \sum_{i=1}^n l(x_i)$. Offensichtlich ist l dann $G(n\Gamma_2)$ invariant.
Schließlich definieren wir das Tripel für ein gewöhnliches Wurzelsystem $\Gamma_2 = \sum n_i R_i$, wobei R_i die irreduziblen Komponenten seinen, wie folgt: Wir entfernen $\mathbb{E}_8$ und setzen

$$T(\Gamma_2) = \bigoplus_i T(n_i R_i), \ G(\Gamma_2) = \prod_i G(n_i R_i), \ l_{\Gamma_2} = \sum_i l_{n_i R_i},$$

wobei die Summation über alle Typen irreduzibler Wurzelsysteme, die ungleich $\mathbb{E}_8$ sind, geht.

(3.1) Definition
Eine Untergruppe $A < T(\Gamma_2)$ nennen wir *gerade und selbstdual*, falls $|A|^2 = |T(\Gamma_2)|$ gilt und l_{Γ_2} nur gerade ganze Werte > 2 auf $A - \{0\}$ annimmt. Solche Untergruppen nennen wir auch Codes.

(3.2) Lemma
Sei Γ_2 ein Wurzelsystem von Rang n. Dann gibt es eine Bijektion zwischen Klassen gerader unimodularer n-dimensionaler Gitter (bis auf Isomorphie) mit einem zu Γ_2 isomorphen Wurzelsystem und den Bahnen gerader, selbstdualer Untergruppen $A < T(\Gamma_2)$ bezüglich $G(\Gamma_2)$.

Beweis. Sei Γ ein gerades unimodulares Gitter in $\mathbb{R}^n$ und Γ_2 sein Wurzelsystem. Dann ist $(\Gamma_2)_\mathbb{Z} \leq \Gamma = \Gamma^\# \leq (\Gamma_2)_\mathbb{Z}^\#$ und damit $A := \Gamma/(\Gamma_2)_\mathbb{Z} \leq (\Gamma_2)_\mathbb{Z}^\#/(\Gamma_2)_\mathbb{Z} = T(\Gamma_2)$. Es gilt $1 = disc(\Gamma) = [\Gamma : (\Gamma_2)_\mathbb{Z}]^{-2} disc((\Gamma_2)_\mathbb{Z})$ (Ebeling §1.1) und folglich $|A|^2 = |T(\Gamma_2)|$. Ferner ist x^2 gerade und ganzzahlig für $x \in \Gamma$, dementsprechend ist $l(x) > 2$ für $x \in A - \{0\}$. Wir definieren also $\nu : \Gamma \mapsto A$ und erhalten damit nach dem Homomorphiesatz, dass sich Untergruppen $A \leq T(\Gamma_2)$ und Zwischengitter $(\Gamma_2)_\mathbb{Z} \leq \Gamma \leq (\Gamma_2)_\mathbb{Z}^\#$ entsprechen. □

(3.3) Beispiel
Sei $\Gamma_2 = n\mathbb{A}_1$. Dann ist $T(\Gamma_2) = (\mathbb{Z}/2\mathbb{Z})^n = \mathbb{F}_2^n$ und $G(\Gamma_2)$ ist isomorph zu S_n. l ist in diesem Fall gegeben durch $l(x) = l(x_1, ..., x_n) = \frac{1}{2} wt(x)$, wobei $wt(x)$ das Hamminggewicht bezeichne. Eine gerade, selbstduale Untergruppe ist ein binärer, selbstdualer, doppelt gerader Code mit Minimalabstand ≥ 8. Demnach ist das Problem gerade, unimodulare n-dimensionale Gitter mit Wurzelsystem $n\mathbb{A}_1$ zu klassifizieren äquivalent zu dem Problem solche Codes zu klassifizieren.

(3.4) Beispiel
Sei $\Gamma_2 = n\mathbb{A}_2$. In diesem Fall gilt $T(\Gamma_2) = \mathbb{F}_3^n, G(\Gamma_2) = C_2^n \rtimes S_n, l(x) = \frac{2}{3} \cdot |\{x_i : x_i \neq 0\}|$. Wie oben ist das Problem $2n$-dimensionale Gitter mit Wurzelsystem $n\mathbb{A}_2$ zu klassifizieren äquivalent zu dem Problem ternäre, selbstduale Typ III Codes mit Minimalabstand > 3 zu klassifizieren.

Im Allgemeinen kann das Problem gerade, selbstduale Untergruppen $A < T(\Gamma_2)$ zu klassifizieren als Problem der Codierungstheorie angesehen werden. Dies beinhaltet das Problem der Klassifikation selbstdualer Codes über den Ringen $\mathbb{Z}/n\mathbb{Z}$ und dem Körper $\mathbb{F}_4$. Gerade, unimodulare Gitter, die ein Wurzelsystem mit maximalem Rang haben, zu klassifizieren ist ein äquivalentes Problem.

§ 4 Die Klassifikation der geraden unimodularen Gitter in Dimension 24

(4.1) Satz
Bis auf Isomorphie gibt es genau 24 gerade, unimodulare Gitter in $\mathbb{R}^{24}$. Jedes dieser Gitter ist eindeutig durch sein Wurzelsystem bestimmt, wobei die möglichen Wurzelsysteme in (2.8) aufgelistet sind.

Beweis. Es ist bereits bekannt, dass das Wurzelsystem eines geraden unimodularen Gitters Γ eines aus dieser Liste ist. Es reicht also zu zeigen, dass es zu jedem der Wurzelsysteme genau ein Gitter Γ gibt. Alle nicht-leeren Wurzelsysteme haben Rang 24, folglich können wir die Theorie aus §3 anwenden, also zu jedem von ihnen das Tripel $(T(\Gamma_2), G(\Gamma_2), l_{\Gamma_2})$ berechnen und die Existenz und Eindeutigkeit des zugehörigen Codes zeigen.
Da die Konstruktionen immer nach demselben Schema ablaufen, werden wir hier nur einige Beispiele betrachten.

(i) $\Gamma_2 = 24\mathbb{A}_1$. Dann ist $T(\Gamma_2) = \mathbb{F}_2^{24}, G(\Gamma_2) = S_{24}$ und $l(\alpha) = \frac{1}{2}wt(\alpha)$, wobei wt das Hamminggewicht bezeichne. $A < T(\Gamma_2)$ ist dann ein binärer, selbstdualer, doppelt gerader Code mit Minimalabstand 8. Es gibt nur einen solchen Code und das ist der Golay Code $\mathcal{G}_{24}$.

(ii) $\Gamma_2 = 4\mathbb{A}_6$. Dann ist $T(\Gamma_2) = \mathbb{F}_7^4, G(\Gamma_2) = C_2^4 \rtimes S_4, l(0) = 0, l(\pm 1) = \frac{6}{7}, l(\pm 2) = \frac{10}{7}, l(\pm 3) = \frac{12}{7}$. Gesucht ist ein selbstdualer Code A der Dimension 2 erzeugt von Elementen x mit $x^2 \equiv_2 0$. Nach Anwenden von $G(\Gamma_2)$ ist x eines von $(0,1,2,3), (1,1,1,2), (2,2,2,3), (1,3,3,3)$. Wäre $(2,2,2,3)$ in A, dann auch $(4,4,4,6)$, der aber in derselben Bahn wie $(1,3,3,3)$ liegt. Ferner liegt $2(1,3,3,3)$ in der Bahn von $(1,1,1,2)$. Demnach ist OE $(0,1,2,3)$ oder $(1,1,1,2)$ in A. Wir gehen zunächst von ersterem aus. Da A Dimension 2 hat, liegt ein zu $(0,1,2,3)$ linear unabhängiger Vektor (a,b,c,d) in A. Dabei ist OE $b = 0$. Ferner ist $a \neq 0$, denn sonst wäre $(1,0,0,0)$ in $A^\perp$, aber nicht in A, also OE $a = 1$. Für (c,d) bleiben $(-3,2)$ oder $(3,-2)$. Beide Wahlen liefern unter $G(\Gamma_2)$ äquivalente Codes. Damit ist $A = \langle (0,1,2,3), (1,0,3,-2) \rangle$ und A enthält $(1,1,-2,-1)$, welches mit $(1,1,1,2)$ in einer $G(\Gamma_2)$-Bahn liegt.
Gehen wir nun davon aus, dass $(1,1,1,2)$ in A liegt. Durch analoge Rechnungen erhält man, dass dann auch ein Element aus der $G(\Gamma_2)$-Bahn von $(0,1,2,3)$ in A liegt. Folglich ist A eindeutig.

(iii) $\Gamma_2 = \mathbb{D}_{24}$. Dann ist $T(\Gamma_2) = \mathbb{F}_4, G(\Gamma_2) = C_2, l(0) = 0, l(1) = 1, l(\omega) = l(\omega^2) = 6$. Der Code besteht dann aus 0 und ω und das zugehörige Gitter ist $\mathbb{D}_{24}^+ = \mathbb{D}_{24} \cup (v + \mathbb{D}_{24})$, wo $v = \frac{1}{2}(1, ..., 1)$ ist.

(iv) $\Gamma_2 = 3\mathbb{E}_8$. Dann ist $T(\Gamma_2) = 0$ und der Code ist trivial. Das zugehörige Gitter ist $\mathbb{E}_8 \oplus \mathbb{E}_8 \oplus \mathbb{E}_8$.

(v) $\Gamma_2 = 2\mathbb{E}_7 + \mathbb{D}_{10}$. Dann ist $T(\Gamma_2) = \mathbb{F}_2^2 \times \mathbb{F}_4$ und $G(\Gamma_2) = S_2 \times C_2$. Die Funktion l hat auf den ersten zwei Summanden die Form $l(0) = 0, l(1) = \frac{3}{2}$ und auf dem letzten $l(0) = 0, l(1) = 1, l(\omega) = l(\omega^2) = \frac{5}{2}$, wobei ω ein primitives Element von $\mathbb{F}_4$ sei, also $\omega^2 + \omega + 1 = 0$ gilt. Gesucht ist eine Untergruppe der Ordnung 4 erzeugt von Elementen x mit $x^2 \equiv_2 0$. Nach Anwenden von $G(\Gamma_2)$ ist x eines der Elemente $(1, 0, \omega), (1, 1, 1)$. Sei $x = (1, 0, \omega)$, dann ist $(0, 1, \omega^2)$ dazu linear unabhängig und die von den beiden Elementen erzeugte Gruppe hat Ordnung 4 und enthält $(1, 1, 1)$. Beginnt man mit $(1, 1, 1)$, so kommt man auf denselben Code. Folglich ist der Code eindeutig.

Zum leeren Wurzelsystem gehört das Leech-Gitter, welches ebenfalls eindeutig ist. Denn angenommen $\Lambda \subset \mathbb{R}^{24}$ ist ein gerades unimodulares Gitter mit $\Lambda_2 = \emptyset$. Dann muss die Theta-Reihe von Λ gleich der des Leech-Gitters sein und folglich muss es ein Element u der Länge 8 geben. Sei $\Gamma = \Lambda^u = \Lambda' \cup (\frac{u}{2} + \Lambda')$ mit $\Lambda' = \{\lambda \in \Lambda : \lambda \cdot u \equiv_2 0\}$. Dann ist Γ ein Nachbar von Λ, d.h. $\Gamma \cap \Lambda$ hat Index 2 in Γ und Λ, und damit ein gerades unimodulares Gitter in $\mathbb{R}^{24}$. Da $\frac{u}{2} \cdot \frac{u}{2} = \frac{8}{4} = 2$, ist Γ_2 nicht leer. Seien $x, y \in \Gamma_2, x \neq \pm y$, so dass $x, y \in \frac{u}{2} + \Lambda'$ mit $x \cdot y \neq 0$. OE gilt $x \cdot y = 1$ (Sonst Vorzeichen von y ändern), aber dann ist $x - y$ eine Wurzel, denn $(x - y) \cdot (x - y) = x^2 - 2x \cdot y + y^2 = 2 - 2 + 2 = 2$. Dies ist aber nicht möglich, da $x - y \in \Lambda' \subset \Lambda$ und $\Lambda_2 = \emptyset$ gilt. Also ist $\Gamma_2 = k\mathbb{A}_1$ mit $k = 24$. Wir können eine Basis $(e_1, ..., e_{24})$ wählen mit $e_i \cdot e_j = \frac{1}{2}\delta_{ij}$ und $\sum_{i=1}^{24} n_i e_i \in \Gamma$ genau dann, wenn $n_i \in \mathbb{Z}$. Da die Eigenschaft Nachbar zu sein symmetrisch ist, gibt es ein $v \in \Gamma$ mit $\Gamma^v = \Lambda$. Sei $v = \sum_{i=1}^{24} m_i e_i, m_i \in \mathbb{Z}$. Ist ein m_α gerade, so gilt $v \cdot 2e_\alpha = m_\alpha \equiv_2 0$, also $2e_\alpha \in \Gamma^v = \Lambda$, was aber nicht möglich ist, da $\Lambda_2 = \emptyset$. Also sind alle m_i ungerade. Da v mod 2Γ definiert ist, können wir annehmen, dass $m_1 \in \{\pm 1, \pm 3\}$ und $m_i = \pm 1, 2 \leq i \leq 24$, gilt. Wegen der Operation der Weyl-Gruppe $W(\Gamma_2)$ können wir ferner $m_1 \in \{1, 3\}$ und $m_i = 1, 2 \leq i \leq 24$ annehmen. Da $\left(\frac{1}{2} \sum_{i=1}^{24} e_i\right)^2 = \frac{1}{4} \cdot \frac{24}{2} = 3 \notin 2\mathbb{Z}$ gilt, muss $v = 3e_1 + ... + e_{24}$ sein. Für solch ein v ist Γ^v das Leech-Gitter. $\square$

Literatur

(1) Ebeling, Wolfgang: *Lattices and Codes*
Vieweg Wiesbaden Braunschweig, 2002

(2) Conway, J. H., Sloane, N. J. A.: *Sphere Packings, Lattices and Groups*
Springer Berlin, 3. Edition, 1998