Gitter und Codes

SS 2007
Prof. Dr. G. Nebe, Dr. M. Künzer

In dieser Vorlesung werden Grundlagen, schöne Beispiele und Ergebnisse der kombinatorischen und geometrischen Theorie von Gittern und einige Analoga für Codes vorgestellt. Nicht behandelt werden arithmetische und algebraische Theorie quadratischer Formen, siehe z.B. Scharlau oder Kneser.

Inhaltsverzeichnis

Literatur:

W. Ebeling, Lattices and Codes, Vieweg
J. Martinet, Perfect lattices in euclidean spaces, Springer
Conway, Sloane, Sphere packings, lattices and groups, Springer
H. Cohen, A course in computational algebraic number theory, Springer
W. Scharlau, Quadratic and Hermitian forms, Springer
M, Kneser, Quadratische Formen, Springer
B. Venkov, Réseaux et designs sphériques, L'enseignement mathématique. Monographie 37, Genève 2001, S. 10-86.

I Grundlagen

1 Gitter.

Wir betrachten einen euklidischen Vektorraum $E = (V, (,))$ meist $E = (\mathbb{R}^{1\times n}, (,))$. Unsere Vektoren sind Zeilenvektoren.

Definition 1.1 *(i) Eine Teilmenge $L \subset V$ heißt* Gitter *, falls es ein linear unabhängiges Tupel $B = (b_1, \ldots, b_m) \in V^m$ gibt, mit*

$$L = \langle b_1, \ldots, b_m\rangle_{\mathbb{Z}} = \{\sum_{i=1}^{m} a_i b_i \mid a_i \in \mathbb{Z}\}.$$

B heißt dann auch eine Gitterbasis *von L und $m = dim(L)$ die* Dimension *von L. L heißt* volles Gitter in *E, falls $\dim(L) = \dim(V)$, also B eine Basis von V ist.*
(ii) Ist $B \in V^m$ eine Gitterbasis von L und $\mathcal{G}(B) := ((b_i, b_j)) \in \mathbb{R}^{m\times m}$ die Grammatrix *von B, so heißt*

$$\det(L) := \det(\mathcal{G}(B))$$

die Determinante *des Gitters L. $\mathcal{G}(B)$ nennt man auch eine Grammatrix von L.*

Beispiele auf Folie: hexagonales und quadratisches Gitter, Gitterbasen und Grammatrizen. Zugehörige Kugelpackung. Keplerpackung und kubisch flächenzentriertes Gitter.

Bemerkung 1.2 *Sei L ein Gitter in V und $B \in V^m$ eine Gitterbasis.*
(a) L ist ein volles Gitter in dem von ihm erzeugten Vektorraum $\mathbb{R}L := \langle B\rangle_{\mathbb{R}}$.
(b) $C \in V^m$ ist Gitterbasis von L genau dann wenn $\langle C\rangle_{\mathbb{R}} = \langle B\rangle_{\mathbb{R}}$ und die Basiswechselmatrix $T := {}_C\mathrm{id}_B \in \mathrm{GL}_m(\mathbb{Z})$ ist. Dann gilt $\mathcal{G}(C) = T\mathcal{G}(B)T^{tr}$. Insbesondere ist $\det(\mathcal{G}(C)) = \det(\mathcal{G}(B))$ und die Determinante von L ist wohldefiniert.
(c) Ist L ein volles Gitter, so ist $\sqrt{\det(L)} = vol(V/L)$ das Volumen des von einer Gitterbasis B aufgespannten Parallelepipeds $P(B) := \{\sum a_i b_i \mid 0 \le i \le 1\}$.
(d) Ist L ein volles Gitter, so ist $P(B)$ ein Fundamentalbereich *der Operation von L auf V, d.h.*
(i) $P(B)$ ist abgeschlossen.
(ii) Für alle $v \in V$ gibt es ein $\ell \in L$ mit $\ell + v \in P(B)$. (iii) Sind $v \neq w \in P(B)$ so dass $v - w \in L$ liegt, dann liegen v und w auf dem Rand von $P(B)$.

Bemerkung 1.3 *Sei L ein volles Gitter in $E = (V, (,))$ mit Gitterbasis B. Dann ist*

$$L^{\#} := \{v \in V \mid (v, \ell) \in \mathbb{Z} \text{ für alle } \ell \in L\}$$

ebenfalls ein volles Gitter in E, das zu L duale Gitter*. Die Dualbasis $B^* = (b_1^*, \ldots, b_n^*)$ von B ist eine Gitterbasis von $L^{\#}$.*

Es gilt $\mathcal{G}(B)\mathcal{G}(B^*) = I_n$, $\det(L^\#)\det(L) = 1$.
Ist $L \subset L^\#$, *so nennt man das Gitter* L *auch* ganz. *Dann ist die Faktorgruppe* $L^\#/L$ *eine endliche abelsche Gruppe der Ordnung* $\det(L)$. *Es gilt* $B^*\mathcal{G}(B) \in L^n$ *und* $\mathcal{G}(B)$ *ist eine Relationenmatrix von* $L^\#/L$. *Sind* $(d_1, \ldots, d_n)$ *die Invariantenteiler von* $\mathcal{G}(B)$, *so ist* $L^\#/L \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_n\mathbb{Z}$.

Beweis. Sei $v \in V$. Dann ist

$$(\ell, v) \in \mathbb{Z} \text{ für alle } \ell \in L \Leftrightarrow a_i := (b_i, v) \in \mathbb{Z} \text{ für alle } 1 \le i \le n \Leftrightarrow v = \sum a_i b_i^* \in \langle b_1^*, \ldots, b_n^* \rangle_{\mathbb{Z}}.$$

Also ist das duale Gitter $L^\#$ genau das von der dualen Basis erzeugte Gitter. Weiter ist ${}_{B^*}\mathrm{id}_B = \mathcal{G}(B)$ die Basiswechselmatrix, d.h. $B^*\mathcal{G}(B) = B$. Damit ist $\mathcal{G}(B)$ die Relationenmatrix von $L^\#/L$ und $\det(\mathcal{G}(B)) = |L^\#/L|$. Die Elementarteiler von $\mathcal{G}(B) \in \mathbb{Z}^{n\times n}$ geben uns die Struktur der endlichen abelschen Gruppe $L^\#/L$ an. □

Definition 1.4 *Seien* L *und* L' *volle Gitter in* E.
(a) L *und* L' *heißen* isometrisch, *falls es ein* $g \in O(E)$ *gibt, mit* $Lg = L'$.
(b) $\mathrm{Aut}(L) := \{g \in O(E) \mid Lg = L\}$ *heißt die* Automorphismengruppe *von* L.

Bemerkung 1.5 *(a) Zwei Gitter* L *und* L' *sind isometrisch, genau dann wenn es Gitterbasen* B *und* B' *gibt, mit* $\mathcal{G}(B) = \mathcal{G}(B')$. *"Sie haben gleiche Grammatrizen". Ein Gitter* L *ist also bis auf Isometrie bestimme durch jede seiner Grammatrizen. Umgekehrt bestimmt ein Gitter* L *eine* $\mathrm{GL}_n(\mathbb{Z})$*-Bahn* $\{g\mathcal{G}(B)g^{tr} \mid g \in \mathrm{GL}_n(\mathbb{Z})\}$ *von Grammatrizen.*
(b) Ist B *eine Gitterbasis von* L, *so ist* ${}_B\mathrm{Aut}(L)_B = \{g \in \mathrm{GL}_n(\mathbb{Z}) \mid g\mathcal{G}(B)g^{tr} = \mathcal{G}(B)\}$.

Beispiel: $\mathrm{Aut}(\mathbb{A}_2)$. Das hexagonale Gitter hat Grammatrix $\mathcal{G}((b_1, b_2)) = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$.

$${}_B\mathrm{Aut}(\mathbb{A}_2)_B = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^{2\times 2} \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{tr} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\}.$$

Die Bilder $(b_1 g = ab_1 + bb_2, b_2 g = cb_1 + db_2)$ unter den Automorphismen g durchlaufen genau die 12 Paare (c_1, c_2) von Gittervektoren, mit $(c_1, c_1) = 2, (c_1, c_2) = 1, (c_2, c_2) = 2$.

Algorithmus 1.6 *Das Gram-Schmidt-Orthogonalisierungsverfahren:*
Eingabe: *Eine Basis* $(b_1, \ldots, b_n)$ *von* V.
Ausgabe: *Eine Orthogonalbasis* $B' := (b'_1, \ldots, b'_n)$ *von* E *mit* $\langle b_1, \ldots, b_i\rangle_{\mathbb{R}} = \langle b'_1, \ldots, b'_i\rangle_{\mathbb{R}}$ *für alle* i.
Algorithmus: *Für* $i = 1, \ldots, n$ *berechne sukzessive*

$$b'_i := b_i - \sum_{j=1}^{i-1} \mu_{ij} b'_j$$

wo $\mu_{ij} = \frac{(b_i, b'_j)}{(b'_j, b'_j)}$.

Bemerkung 1.7 *b'_i ist die Projektion von b_i auf $\langle b_1, \ldots, b_{i-1}\rangle^\perp$.*
Die von B und B' erzeugten Gitter haben die gleiche Determinante, nämlich $\prod_{j=1}^n (b'_j, b'_j)$.
Da $(b'_j, b'_j) \leq (b_j, b_j)$ ist, ergibt sich die folgende Hadamard Ungleichung.

Ende am 3.4.07

Folgerung 1.8 *Die Hadamard Ungleichung:*
Ist $B := (b_1, \ldots, b_n)$ eine Gitterbasis von L, so ist $\det(L) \leq \prod_{j=1}^n (b_j, b_j)$.

Beweis. Sei B' die in Algorithmus 1.6 berechnete Orthogonalbasis und

$$M := \begin{pmatrix} 1 & 0 & \ldots & 0 \\ \mu_{21} & 1 & \ldots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ \mu_{n1} & \ldots & \mu_{n,n-1} & 1 \end{pmatrix}$$

Dann ist $\det(M) = 1$ und $MB' = B$. Also ist $\mathcal{G}(B) = M\mathcal{G}(B')M^{tr}$ und daher

$$\det(L) = \det(\mathcal{G}(B)) = \det(\mathcal{G}(B')) = \prod_{i=1}^n (b'_i, b'_i) \leq \prod_{i=1}^n (b_i, b_i).$$

□

Satz 1.9 *$L_{\leq S} := \{v \in L \mid (v, v) \leq S\}$ ist endlich.*

Beweis. Sei B eine Gitterbasis von L und B', μ_{ij} wie in 1.6.
Ist $v = \sum_{j=1}^n a_j b_j \in L$, so ist $v = \sum_{j=1}^n \alpha_j b'_j$ mit $\alpha_j \in \mathbb{R}$,
$\alpha_n = a_n$, $\alpha_{n-1} = a_{n-1} - \mu_{n,n-1} a_n$, $\ldots$
Aus

$$(v, v) = \sum_{j=1}^n \alpha_j^2 (b'_j, b'_j) \leq S$$

folgt insbesondere $a_n^2 (b'_n, b'_n) \leq S$. Also hat man nur endlich viele Möglichkeiten für $a_n \in \mathbb{Z}$. Allgemein gilt

$$\alpha_j^2 (b'_j, b'_j) = (a_j - \sum_{i=j+1}^n \mu_{i,j} a_i)^2 (b'_j, b'_j) \leq S - \sum_{i=j+1}^n \alpha_i^2 (b'_i, b'_i)$$

woraus man sukzessiv nur endlich viele Möglichkeiten für $a_j \in \mathbb{Z}$, $j = n, n-1, \ldots, 1$ erhält.
□

Folgerung 1.10 $\mathrm{Aut}(L)$ *ist eine endliche Gruppe.*

Beweis. Sei $B = (b_1, \ldots, b_n)$ eine Gitterbasis von L und $S := \max\{(b_i, b_i) \mid 1 \leq i \leq n\}$. Ist $g \in \mathrm{Aut}(L)$, so ist g eindeutig bestimmt durch die Bilder der Basisvektoren $(b_1 g, \ldots, b_n g) \in L^n_{\leq S}$. Also gilt $|\mathrm{Aut}(L)| \leq |L_{\leq S}|^n$. □

1.1 Wurzelgitter

Definition 1.11 *Ein ganzes Gitter L heißt* Wurzelgitter*, falls $L = \langle \{\ell \in L \mid (\ell,\ell) = 2\} \rangle_{\mathbb{Z}}$. $L_{=2} = R(L) := \{\ell \in L \mid (\ell,\ell) = 2\}$ heißt die Menge der* Wurzeln *in L.*

Bemerkung 1.12 *Ist L ein ganzes Gitter und $\ell \in L$ mit $(\ell,\ell) = 2$, so ist die* Spiegelung σ_ℓ *entlang ℓ definiert durch*

$$v\sigma_\ell := v - 2\frac{(v,\ell)}{(\ell,\ell)}\ell = v - (v,\ell)\ell$$

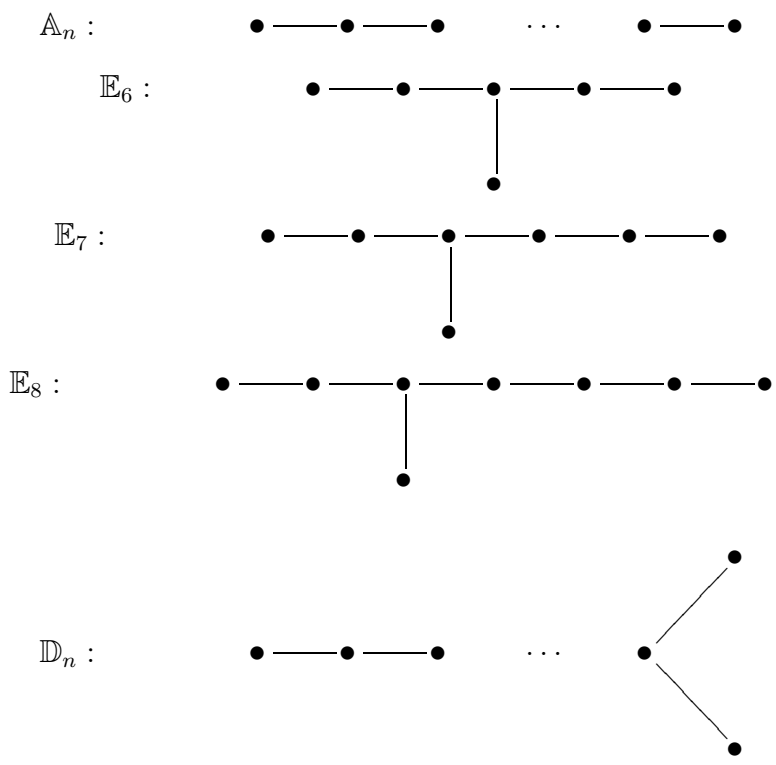
für alle $v \in V$ eine orthogonale Abbildung die L festlässt, also $\sigma_\ell \in \mathrm{Aut}(L)$.
Ist L ein Wurzelgitter, so heißt

$$W(L) := \langle \sigma_\ell \mid \ell \in R(L) \rangle \leq \mathrm{Aut}(L)$$

die Weyl-Gruppe *von L. Da Konjugierte von Spiegelungen wieder Spiegelungen sind ($g^{-1}\sigma_\ell g = \sigma_{\ell g}$), ist die Weyl-Gruppe ein Normalteiler in $\mathrm{Aut}(L)$.*

Satz 1.13 *(Witt, für einen Beweis vgl. Ebeling) Ist L ein Wurzelgitter, so hat L eine Gitterbasis $B = (b_1, \ldots, b_n)$ mit $(b_i, b_i) = 2$ und $(b_i, b_j) \in \{0, -1\}$ für $1 \leq i \neq j \leq n$.*

Beispiel 1.14 *Die Grammatrix einer solchen Basis wird durch einen Graphen kodiert. Die Knoten entsprechen dabei den Basisvektoren. Zwei Knoten b_i, b_j sind durch eine Kante verbunden, genau dann wenn $(b_i, b_j) = -1$. Diese Graphen nennt man* Dynkin-Diagram.



Die zugehörigen Grammatrizen ergeben sich als

$$\mathcal{G}(\mathbb{A}_n) := \begin{pmatrix} 2 & -1 & 0 & \dots & \dots & 0 \\ -1 & 2 & -1 & 0 & \dots & 0 \\ 0 & -1 & 2 & -1 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & -1 & 2 & -1 \\ 0 & \dots & \dots & 0 & -1 & 2 \end{pmatrix}, \quad \mathcal{G}(\mathbb{D}_n) := \begin{pmatrix} 2 & -1 & 0 & \dots & \dots & 0 & 0 \\ -1 & 2 & -1 & 0 & \dots & 0 & 0 \\ 0 & -1 & 2 & -1 & \dots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & -1 & 2 & -1 & -1 \\ 0 & \dots & \dots & 0 & -1 & 2 & 0 \\ 0 & \dots & \dots & 0 & -1 & 0 & 2 \end{pmatrix}$$

$$\mathcal{G}(\mathbb{E}_6) = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 \end{pmatrix}, \quad \mathcal{G}(\mathbb{E}_7) = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 2 \end{pmatrix}$$

$$\mathcal{G}(\mathbb{E}_8) = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

Es gilt $\det(\mathbb{E}_6) = 3$, $\det(\mathbb{E}_7) = 2$, $\det(\mathbb{E}_8) = 1$.
Ist $(e_1, \dots, e_n)$ *eine Orthonormalbasis von* E, *so ist*

$$\mathbb{D}_n = \langle e_1 - e_2, e_2 - e_3, \dots, e_{n-1} - e_n, e_{n-1} + e_n \rangle_{\mathbb{Z}}.$$

Insbesondere ist $\det(\mathbb{D}_n) = 4$. *Weiter ist* $v := \frac{1}{2}(e_1 + \dots + e_n) \in \mathbb{D}_n^{\#}$ *und* $e_1 \in \mathbb{D}_n^{\#}$. *Es gilt immer* $2e_1 \in \mathbb{D}_n$. *Es ist* $2v \in \mathbb{D}_n$ *genau dann, wenn* n *gerade ist. Dann ist* $\mathbb{D}_n^{\#}/\mathbb{D}_n \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, *ansonsten ist* $\mathbb{D}_n^{\#}/\mathbb{D}_n \cong \mathbb{Z}/4\mathbb{Z}$.
Für $\mathbb{A}_n$ *gilt:* $\det(\mathbb{A}_n) = n + 1$ *und* $\mathbb{A}_n^{\#}/\mathbb{A}_n \cong \mathbb{Z}/(n+1)\mathbb{Z}$.
$\mathbb{A}_n$ *ist ein Teilgitter (kein volles Teilgitter) von* $\mathbb{Z}^{n+1}$: *Ist* $(e_1, \dots, e_{n+1})$ *eine ON-Basis von* $\mathbb{R}^{n+1}$, *so ist* $(e_1 - e_2, e_2 - e_3, \dots, e_n - e_{n+1})$ *eine Gitterbasis von* $\mathbb{A}_n$. *Das Gitter* $\mathbb{A}_n$ *erhält man als*

$$\mathbb{A}_n = \{\sum_{i=1}^{n+1} a_i e_i \in \mathbb{R}^{n+1} \mid a_i \in \mathbb{Z}, \sum a_i = 0\}$$

als $(e_1 + \dots + e_{n+1})^{\perp}$ *in* $\mathbb{Z}^{n+1}$. *Der Vektor* $v := \frac{1}{n+1}(ne_1 - e_2 - \dots - e_{n+1}) \in \mathbb{A}_n^{\#}$ *erfüllt* $(n+1)v \in \mathbb{A}_n$.

Gitter L	$\lvert R(L)\rvert$	$\det(L)$	$L^\#/L$	Dimension n
$\mathbb{A}_n$	$n(n+1)$	$n+1$	$\mathbb{Z}/(n+1)\mathbb{Z}$	≥ 1
$\mathbb{D}_n$	$2n(n-1)$	4	$\mathbb{Z}/4\mathbb{Z}$	≥ 4, ungerade
$\mathbb{D}_n$	$2n(n-1)$	4	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	≥ 4, gerade
$\mathbb{E}_6$	72	3	$\mathbb{Z}/3\mathbb{Z}$	6
$\mathbb{E}_7$	126	2	$\mathbb{Z}/2\mathbb{Z}$	7
$\mathbb{E}_8$	240	1	1	8

Ohne Beweis möchte ich angeben:

Satz 1.15 *(vgl. Ebeling) Jedes Wurzelgitter ist orthogonale Summe von Wurzelgittern der Form $\mathbb{A}_n$, $\mathbb{D}_m$ $(m \geq 4)$, $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$.*

Definition 1.16 *(i) Ein Gitter L heißt* gerade*, falls $(\ell, \ell) \in 2\mathbb{Z}$ für alle $\ell \in L$.*
(ii) Ein Gitter L heißt unimodular*, falls $L = L^\#$.*

Bemerkung 1.17 *(i) Ein gerades Gitter ist ganz.*
(ii) Ein ganzes Gitter ist gerade, genau dann wenn für alle Basisvektoren b_i in einer Gitterbasis gilt, dass $(b_i, b_i) \in 2\mathbb{Z}$.

Folgerung 1.18 *Wurzelgitter sind gerade Gitter.*
Das Gitter $\mathbb{E}_8$ ist ein gerades unimodulares Gitter.

Definition 1.19 *(i) Für 2 Gitter L_1, L_2 in V_1 bzw. V_2 bezeichnet $L_1 \perp L_2$ die* orthogonale Summe *. Dies ist ein Gitter in $V_1 \oplus V_2$ der Dimension $\dim(L_1) + \dim(L_2)$. Sind B bzw. C Gitterbasen von L_1 bzw. L_2, so ist $((b_1, 0), \ldots, (b_{n_1}, 0), (0, c_1), \ldots, (0, c_{n_2}))$ eine Gitterbasis von $L_1 \perp L_2$ mit Grammatrix*

$$\begin{pmatrix} \mathcal{G}(B) & 0 \\ 0 & \mathcal{G}(C) \end{pmatrix}$$

(ii) Ist $L \leq M$ ein Teilgitter, so heißt

$$L^{\perp,M} := L^\perp := \{m \in M \mid (\ell, m) = 0 \text{ für alle } \ell \in L\}$$

das Orthogonalgitter *von L in M.*
(iii) Ein Teilgitter $L \leq M$ heißt rein *, falls*

$$L = \{m \in M \mid m \in \langle L \rangle_{\mathbb{R}}\} = M \cap \mathbb{R}L.$$

Bemerkung 1.20 *Sei $L \leq M$ ein Teilgitter, $B = (b_1, \ldots, b_n)$ eine Gitterbasis von M, $C = (c_1, \ldots, c_k)$ eine Gitterbasis von L und $T = {}_C\,\mathrm{id}_B \in \mathbb{Z}^{k \times n}$ die Basiswechselmatrix.*
Dann ist L rein in $M \Leftrightarrow$ die Invariantenteiler von T sind alle gleich $1 \Leftrightarrow M/L$ ist torsionsfrei $\Leftrightarrow C$ kann zu einer Gitterbasis von M ergänzt werden.

Ende am 10.4.2007

Beweis. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen gibt es eine Gitterbasis $B' = (b'_1, \ldots, b'_n)$ von M und Zahlen $d_1, \ldots, d_k \in \mathbb{Z}$ (die Invariantenteiler von T) so daß $C' = (d_1 b'_1, \ldots, d_k b'_k)$ eine Gitterbasis von L ist. Da $\mathbb{R}L \cap M$ aus der Menge aller ganzen Linearkombinationen der $(b'_1, \ldots, b'_k)$ besteht, gilt $\mathbb{R}L \cap M = L$ genau dann, wenn alle d_i gleich 1 sind. □

Satz 1.21 *Sei $V = U_1 \oplus U_2$, $\pi_i \in \mathrm{End}(V)$ die Projektionen auf U_i. Sei L ein volles Gitter in V, so dass $L_i := L \cap U_i$ ein volles Gitter in U_i ist ($i = 1, 2$). (dann ist $U_i = \mathbb{R}L_i$ und L_i ist reines Teilgitter in L.) Setze $L'_i := L\pi_i$. Dann ist $L_i \leq L'_i$ ($i = 1, 2$) und es gilt:*

$$L'_1/L_1 \cong L'_2/L_2 \cong L/(L_1 \oplus L_2) \cong L'_1 \oplus L'_2/L.$$

Beweis. Klar ist $L'_1/L_1 \cong L'_1 \oplus L_2/L_1 \oplus L_2 \cong L'_1 \oplus L'_2/L_1 \oplus L'_2$.
Wir betrachten zunächst die Projektion $\pi_1 : L \to L'_1$. Gefolgt vom natürlichen Epimorphismus $L'_1 \to L'_1/L_1$ liefert sie eine surjektive Abbildung $\overline{\pi_1} : L \to L'_1/L_1$. Sei

$$K_1 := \ker(\overline{\pi_1}) = \{\ell \in L \mid \ell\pi_1 \in L_1\}.$$

Für $\ell = x_1 + x_2 \in L$ mit $x_i \in U_i$ ist $\ell\pi_1 = x_1 \in L_1 = U_1 \cap L$ genau dann wenn $x_1 \in L$ und somit $x_2 = \ell - x_1 \in L \cap U_2 = L_2$ liegt. Also ist $K_1 = L_1 \oplus L_2$ und nach dem Homomorphiesatz gilt

$$L'_1/L_1 = \mathrm{Bild}(\overline{\pi_1}) \cong L/\ker(\overline{\pi_1}) = L/(L_1 \oplus L_2).$$

Ebenso erhält man $L'_2/L_2 \cong L/(L_1 \oplus L_2)$. Für die letzte Isomorphie zeigen wir, dass $L'_1 + L = L'_1 \oplus L'_2$. Denn dann ist nach dem Noetherschen Isomorphiesatz

$$(L'_1 \oplus L'_2)/L = (L'_1 + L)/L \cong L'_1/(L'_1 \cap L) = L'_1/L_1.$$

Nach Definition ist $L'_1 + L = \langle L'_1, L\rangle$. Es ist $x_1 \in L'_1$ genau dann wenn $x_1 \in U_1$ und es gibt ein $\ell \in L$, $x_2 \in U_2$ mit $\ell = x_1 + x_2$ (dann notwendigerweise $x_2 \in L'_2$). Also ist $L'_1 + L \subseteq L'_1 \oplus L'_2$. Umgekehrt liegt natürlich $L'_1 \subset L'_1 + L$ und obige Rechnung zeigt auch $L'_2 \subset L'_1 + L$ und damit $L'_1 + L = L'_1 \oplus L'_2$. □

Satz 1.22 *Sei M ein unimodulares Gitter und $L \leq M$ ein reines Teilgitter. Dann ist* $\det(L) = \det(L^\perp)$, *sogar $L^\# / L \cong (L^\perp)^\# / L^\perp$.*

Beweis. Wir wenden Satz 1.21 an auf $U_1 := \mathbb{R}L$, $U_2 = U_1^\perp = \mathbb{R}L^\perp$, $L_1 = L = U_1 \cap M$, $L_2 = L^\perp = U_2 \cap M$ und müssen nur noch zeigen, dass

$$L'_1 = M\pi_1 = L^\#,\ L'_2 = M\pi_2 = (L^\perp)^\#.$$

Ist nun $\ell \in L$ und $m \in M$, so ist $(\ell, m) = (\ell, m\pi_1) \in \mathbb{Z}$ und daher $M\pi_1 \subset L^\#$. Sei $(b_1, \ldots, b_k)$ eine Gitterbasis von L und ergänze diese zu Basis $B := (b_1, \ldots, b_k, b_{k+1}, \ldots, b_n)$ von M. Da $M = M^\#$ ist auch die duale Basis $B^* = (b_1^*, \ldots, b_k^*, b_{k+1}^*, \ldots, b_n^*)$ eine Gitterbasis von M. (Dabei ist $(b_{k+1}^*, \ldots, b_n^*)$ eine Gitterbasis von $L^\perp$.) Und $L^\# = \langle b_1^*\pi_1, \ldots, b_k^*\pi_1\rangle \subset M\pi_1$. □

Bemerkung 1.23 *Als Anwendung zeigen wir, dass* $\mathbb{A}_n^\#/\mathbb{A}_n \cong \mathbb{Z}/(n+1)\mathbb{Z}$. *Setzt man* $L = \langle \ell := e_1 + \ldots + e_{n+1} \rangle \leq \mathbb{Z}^{n+1} = \langle e_1, \ldots, e_{n+1} \rangle_{\mathbb{Z}}$, *so ist* L *ein reines Teilgitter in dem Gitter* $M := \mathbb{Z}^{n+1}$ *mit* $\det(M) = 1$. *Weiter ist* $\mathbb{A}_n = L^\perp$. $\mathcal{G}(\ell) = (n+1) = ((\ell, \ell))$ *liefert* $L^\#/L \cong \mathbb{Z}/(n+1)\mathbb{Z}$, $L^\# = \langle \frac{1}{n+1}\ell \rangle$. *Mit Satz 1.22 findet man also auch* $\mathbb{A}_n^\#/\mathbb{A}_n \cong \mathbb{Z}/(n+1)\mathbb{Z}$.

Als Übung konstruieren Sie $\mathbb{E}_7 = \langle b_7 \rangle^\perp$ und $\mathbb{E}_6 = \langle b_6, b_7 \rangle^\perp$ als Teilgitter von $\mathbb{E}_8$ und folgern so aus $\det(E_8) = 1$, dass $\det(\mathbb{E}_7) = 2$ und $\det(\mathbb{E}_6) = 3$. $\mathbb{E}_8$ kann man z.B. als Teilgitter von $\mathbb{A}_8^\# = \langle v, \mathbb{A}_8 \rangle$ erhalten, $\mathbb{E}_8 = \langle \mathbb{A}_8, 3v \rangle$.

2 Codes.

Definition 2.1 *(i) Ein* linearer Code C *über* $\mathbb{F}_q$ *der Länge* n *ist ein linearer Teilraum* $C \leq \mathbb{F}_q^n$.
(ii) Auf $\mathbb{F}_q^n$ *definieren wir die nicht ausgeartete symmetrische Bilinearform* $x \cdot y := \sum_{i=1}^n x_i y_i$. *Dann ist für einen Code* $C \leq \mathbb{F}_q^n$ *der* duale Code *definiert als der Orthogonalraum* $C^\perp$ *von* C,

$$C^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot c = 0 \text{ für alle } c \in C\}.$$

(iii) C *heißt* selbstdual , *falls* $C = C^\perp$ *und* selbstorthogonal , *falls* $C \subseteq C^\perp$.

Bemerkung 2.2 *Sei* $C \leq \mathbb{F}_q^n$ *ein Code der Dimension* k *und* $B = (b_1, \ldots, b_k)$ *eine Basis von* C, $H = (h_1, \ldots, h_{n-k})$ *eine Basis von* $C^\perp$. *Dann hat* C *zwei verschiedene Beschreibungen:*
(i) Die Matrix $G \in \mathbb{F}_q^{k \times n}$, *deren Zeilen genau die Zeilenvektoren* b_i *sind, nennt man eine* Erzeugermatrix *von* C. *Interpretiert man* G *als Matrix einer linearen Abbildung* $\mathrm{cod} : \mathbb{F}_q^k \to \mathbb{F}_q^n, x \mapsto xG$, *so ist* C *genau das Bild von* cod. *Diese Beschreibung eignet sich sehr gut zum* Codieren *der* q^k *Informationsworte.*
(ii) Die Matrix $P \in \mathbb{F}_q^{n \times (n-k)}$, *deren Spalten genau die Zeilenvektoren* h_i *sind, nennt man eine* Prüfmatrix *von* C. *Interpretiert man* P *als Matrix einer linearen Abbildung* $\mathrm{decod} : \mathbb{F}_q^n \to \mathbb{F}_q^{n-k}, x \mapsto xP$, *so ist* C *genau der Kern von* decod. *Diese Beschreibung eignet sich sehr gut zum Testen, ob ein empfangenes Wort zum Code gehört.*
(iii) Ist P *eine Prüfmatrix für* C *und* $x \in \mathbb{F}_q^n$ *so nennt man* $xP \in \mathbb{F}_q^{n-k}$ *das* Syndrom *von* x *(unter* H*). Es ist* $x \in C$ *genau dann wenn sein Syndrom gleich 0 ist.*

Definition 2.3 *(i) Auf* $\mathbb{F}_q^n$ *definiert der* Hamming-Abstand

$$d : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{Z}, d(x, y) := |\{i \in \{1, \ldots, n\} \mid x_i \neq y_i\}|$$

eine Metrik, *d.h. für alle* $x, y, z \in \mathbb{F}_q^n$ *gilt*
$d(x, y) \geq 0$ *und* $d(x, y) = 0 \Leftrightarrow x = y$,
$d(x, y) = d(y, x)$,
$d(x, y) + d(y, z) \geq d(x, z)$.
(ii) Das Gewicht *eines Wortes* $x \in \mathbb{F}_q^n$ *ist* $w(x) := d(x, 0) = |\{i \in \{1, \ldots, n\} \mid x_i \neq 0\}|$.
(iii) Das Minimalgewicht $d(C)$ *eines Codes* C *ist* $d(C) := \min\{d(c) \mid 0 \neq c \in C\}$.

Bemerkung 2.4 *Interpretiert man ein Codewort als lineare Abhängigkeit der Zeilen der Prüfmatrix, so sieht man, dass das Minimalgewicht des Codes $d(C)$ gleich der minmalen Anzahl linear abhängiger Zeilen einer jeden Prüfmatrix von C ist.*

Definition 2.5 *Sei $C \subseteq \mathbb{F}_q^n$ ein Code. Ein* minimal distance decoder *MDD ist eine Funktion $f : \mathbb{F}_q^n \to C$ mit*

$$d(f(a), a) = \min\{d(c, a) \mid c \in C\} \text{ für alle } a \in \mathbb{F}_q^n.$$

Bemerkung 2.6 *Sei $C \subseteq \mathbb{F}_q^n$ ein Code, $d := d(C)$, f ein MDD für C.*
(i) Ist $e < \frac{d}{2}$ und $v \in \mathbb{F}_q^n$ so gibt es höchstens ein Codewort $c \in C$ mit $d(v, c) \leq e$. Für jeden MDD f gilt also $f(v) = c$. (Der MDD kann e Übertragungsfehler korrigieren.)
(ii) Ist $e < d$ und $v \in \mathbb{F}_q^n$ für das es ein $c \in C$ gibt mit $d(v, c) = e$, so ist $v \notin C$. (Der MDD erkennt, daß die Übertragung fehlerhaft ist (decodiert aber nicht notwendig zum richtigen Codewort).)

Bemerkung 2.7 *Sei $C \leq \mathbb{F}_q^n$ ein linearer Code und $P \in \mathbb{F}_q^{n \times (n-k)}$ eine Prüfmatrix für C und $S := \{xP \mid x \in \mathbb{F}_q^n\} = \text{Bild}(P)$ die Menge der Syndrome von P.*
Dann gilt $\mathbb{F}_q^n = \dot{\cup}_{s \in S} (\{s\})\,\text{decod} = \dot{\cup}_{s \in S} V_s$.
Für $s \in S$ heißt $a_s \in V_s = a_s + C$ ein minimaler Vertreter, *falls $w(a_s) = \min\{w(x) \mid x \in V_s\}$. Wählt man für jedes $s \in S$ einen minimalen Vertreter a_s, so ist die Funktion $f : \mathbb{F}_q^n \to C$ definiert durch $f(a) := a - a_s$, falls $aP = s$ ist, ein MDD für C.*

Beispiel: $C \leq \mathbb{F}_5^5$ habe Erzeugermatrix

$$G := \begin{pmatrix} 1 & 0 & 0 & 2 & 3 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 4 & 1 \end{pmatrix}$$

Dann ist

$$P := \begin{pmatrix} -2 & -3 \\ -1 & -1 \\ -4 & -1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} =: \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix}$$

eine Prüfmatrix für C. P enthält keine Nullzeile, jedoch gilt $x_1 + 2x_3 = 0$, d.h. es gibt 2 l.a. Zeilen in P. Daher ist $(1, 0, 2, 0, 0) \in C$ und $d(C) = 2$. Zum MDD: Die Menge der Syndrome ist

$$S = \mathbb{F}_5^2 = \{(0, 0)\} \cup \{as \mid s \in \{(1, 0), (0, 1), (1, 1), (1, 2), (1, 3), (1, 4)\}, a \in \mathbb{F}_5^*\}$$

Minimale Vertreter $v_{as} = av_s$ in V_{as} sind z.B. gegeben durch $v_{1,0} = (0, 0, 0, 1, 0), v_{0,1} = (0, 0, 0, 0, 1), v_{1,1} = (0, 4, 0, 0, 0), v_{1,2} = (0, 0, 0, 1, 2), v_{1,3} = (0, 0, 0, 1, 3), v_{1,4} = (0, 0, 1, 0, 0)$.

Ende am 13.4.2007

Definition 2.8 *Zwei Codes $C, C' \leq \mathbb{F}_q^n$ heißen* äquivalent, *falls es eine Umordnung σ von $\{1, \ldots, n\}$ gibt sowie $a := (a_1, \ldots, a_n) \in (\mathbb{F}_q^*)^n$, mit*

$$C' = C(\sigma, a) := \{(a_1 c_{\sigma(1)}, a_2 c_{\sigma(2)}, \ldots, a_n c_{\sigma(n)}) \mid (c_1, \ldots, c_n) \in C\}.$$

Sie heißen permutationsäquivalent *falls*

$$C' = C\sigma := \{(c_{\sigma(1)}, c_{\sigma(2)}, \ldots, c_{\sigma(n)}) \mid (c_1, \ldots, c_n) \in C\}$$

für ein $\sigma \in S_n$. $\mathrm{Aut}(C) := \{\sigma \in S_n \mid C\sigma = C\}$ *heißt die* Automorphismengruppe *von C.*

Beachten Sie: Permutationsäquivalenz erhält Orthogonalität, Äquivalenz jedoch i.a. nicht. Es ist

$$C(\sigma, a)^\perp = C^\perp(\sigma, a^{-1}).$$

2.1 Hamming Codes.

Definition 2.9 *Sei $n = \frac{q^r - 1}{q - 1}$ für ein $r \in \mathbb{N}$. Sei $P \in \mathbb{F}_q^{n \times r}$ eine Matrix, in deren Zeilen gerade alle Erzeuger x_i aller eindimensionalen Teilräume von $\mathbb{F}_q^r$ stehen:*

$$P = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

Jeder Code C mit Prüfmatrix P heißt Hamming Code *der Länge n, $C = H(\mathbb{F}_q, r)$.*

Bemerkung 2.10 *$H(\mathbb{F}_q, r)$ ist bis auf Äquivalenz eindeutig bestimmt, also unabhängig von der Wahl der n Erzeuger der 1-dimensionalen Teilräume von $\mathbb{F}_q^r$ und deren Reihenfolge.*
$d(H(\mathbb{F}_q, r)) = 3$.

Beweis. Je 2 Zeilen der Prüfmatrix von $H(\mathbb{F}_q, r)$ sind linear unabhängig. □

Beispiel: $r = 2 \Rightarrow n = 3$ und

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

Der Hamming-Code hat Dimension 1 und Erzeugermatrix $G = (1, 1, 1)$.
$r = 3 \Rightarrow n = 7$ und

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

Der Hamming Code hat Dimension 4 = 7-3 und Erzeugermatrix

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

Definition 2.11 *Ein Code $C \leq \mathbb{F}_q^n$ heißt* perfekt, *falls es eine Zahl e gibt, so daß zu jedem $a \in \mathbb{F}_q^n$ genau ein $c \in C$ existiert mit $d(a,c) \leq e$.*

Beispiel: (i) $C = \mathbb{F}_q^n$ ist ein perfekter Code mit $e = 0$.
(ii) Ist $A = \mathbb{F}_2$ und n ungerade, so ist der Wiederholungscode $C = \{(0,\ldots,0),(1,\ldots,1)\}$ ein perfekter Code mit $e = \frac{n-1}{2}$.
(iii) Der Hamming Code $H(\mathbb{F}_2, 3)$ ist ein perfekter Code mit $e = 1$.

Satz 2.12 *Hamming Codes sind perfekte Codes mit $e = 1$.*

Beweis. Sei C der Hamming Code der Länge $n = q^r - 1$ mit Prüfmatrix P und $a \in \mathbb{F}_q^n$. Dann gilt entweder $aP = 0$ oder $aP = \alpha x_i = \alpha e_i P$ ist ein Vektor $\neq 0$ in $\mathbb{F}_q^r$ und damit gleich dem Vielfachen einer Zeile (der i-ten) von P. D.h. entweder $a \in C$, oder $a - \alpha e_i \in C$. Da $d(a - \alpha e_i, a) = w(\alpha e_i) = 1$ ist, gibt es also zu jedem $a \in \mathbb{F}_q^n$ ein $c \in C$ mit $d(a,c) \leq 1$. Die Eindeutigkeit eines solchen c folgt, da $d(C) = 3$ ist. □

2.2 Von Codes zu Gittern.

Definition 2.13 *Sei p eine Primzahl und $C \leq \mathbb{F}_p^n$ ein Code. Sei $(e_1,\ldots,e_n)$ eine Orthogonalbasis von $(\mathbb{R}^n,(,))$ mit $(e_i,e_i) = \frac{1}{p}$ und $M := \langle e_1,\ldots,e_n\rangle_{\mathbb{Z}}$. Dann ist $\pi : M \to \mathbb{F}_p^n, e_i \mapsto (0,\ldots,0,1,0,\ldots,0)$ ein Epimorphismus mit Kern $\ker(\pi) = pM$. Dann heißt $L_C := \pi^{-1}(C) \leq M$ das* Codegitter *zu C.*

Bemerkung 2.14 *(i) $pM = M^{\#} \leq L_C \leq M$.*
(ii) $L_C^{\#} = L_{C^\perp}$. Insbesondere ist L_C ganz genau dann wenn $C \subset C^\perp$ (also C ein selbstorthogonaler Code ist) und L_C unimodular genau dann, wenn $C = C^\perp$ (ein selbstdualer Code).
(iii) L_C ist gerade, genau dann wenn $p = 2$ und C ein sogenannter doppelt-gerader Code *ist, d.h. $w(c) \in 4\mathbb{Z}$ für alle $c \in C$.*

Beweis. Nur (ii) bedarf eines Beweises. Es ist $L_C/pM \cong C$, insbesondere ist $\det(L_C) = p^{n-2k}$, falls $k = \dim(C)$. Da $\dim(C^\perp) = n - k$ ist, gilt $\det(L_{C^\perp}) = p^{n-2(n-k)} = p^{2k-n} = \det(L_C^{\#})$. Es genügt also zu zeigen, dass $L_{C^\perp} \subset L_C^{\#}$. Klar ist $pM = M^{\#} \subset L_C^{\#}$. Sei $c = (c_1,\ldots,c_n) \in C^\perp$ und $\ell = \sum_{i=1}^n a_i e_i \in L_C$. Dann ist $(a_1 + p\mathbb{Z},\ldots,a_n + p\mathbb{Z}) \in C$ und daher $\sum a_i c_i \equiv_p 0$. Also ist auch $(\sum c_i e_i, \sum a_i e_i) = \frac{1}{p}\sum a_i c_i \in \mathbb{Z}$. □

Bemerkung 2.15 *Definiert man das* Minimum *eines Gitters L als*

$$\min(L) := \min\{(\ell, \ell) \mid 0 \neq \ell \in L\}$$

so gilt für einen Code $C \leq \mathbb{F}_p^n$

$$\min(L_C) \geq \min\{p, \frac{1}{p} d(C)\}$$

mit "=", falls $p = 2$ oder $p = 3$ ist. Es gilt immer $pe_1 \in L_C$ ein Vektor der Quadratlänge p.

Die Konstruktion des Codegitters L_C aus dem Code $C \leq \mathbb{F}_p^n$ nennt man auch manchmal Konstruktion A .

Beispiel 2.16 *Der erweiterte Hamming-Code e_8 und $\mathbb{E}_8$.*
Für einen Code $C \leq \mathbb{F}_q^n$ definiert man den erweiterten Code *$\tilde{C} \leq \mathbb{F}_q^{n+1}$ als*

$$\tilde{C} = \{(c_1, \ldots, c_n, -\sum_{i=1}^{n} c_i) \mid c = (c_1, \ldots, c_n) \in C\}.$$

Dann ist $\dim(C) = \dim(\tilde{C})$.
Ist $C = H(\mathbb{F}_2, 3)$ mit Erzeugermatrix G wie oben, so hat $\tilde{C} =: e_8 \leq \mathbb{F}_2^8$ die Erzeugermatrix

$$\tilde{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Es gilt $\tilde{C} = \tilde{C}^{\perp}$. Also ist $L_{\tilde{C}}$ ein unimodulares Gitter. Es gilt $L_{\tilde{C}} \cong \mathbb{E}_8$.

Ende am 17.4.07

2.3 Wurzelgitter als Codegitter.

In diesem Abschnitt wollen wir sehen, welche Wurzelgitter von der Form L_C für einen Code $C \leq \mathbb{F}_p^n$ sind. Da Wurzelgitter gerade Gitter sind, ist notwendigerweise $p = 2$ und C ein doppelt gerader Code.

Wir beginnen mit einigen interessanten und nützlichen Eigenschaften der Weyl-Gruppe $W(L)$ (siehe Bemerkung 1.12) eines irreduziblen Wurzelgitters.

Definition 2.17 *Ein Gitter L heißt* irreduzibel *oder auch* orthogonal unzerlegbar, *falls L nicht orthogonale Summe echter Teilgitter ist.*

Mit dieser Definition liest sich also Satz 1.15 wie folgt: Jedes irreduzible Wurzelgitter ist von der Form $\mathbb{A}_n$, $\mathbb{D}_m$ ($m \geq 4$), $\mathbb{E}_6$, $\mathbb{E}_7$ oder $\mathbb{E}_8$.

Satz 2.18 *Sei L ein Wurzelgitter und $W(L)$ seine Weyl-Gruppe. Dann ist L irreduzibel, genau dann weinn $W(L)$* irreduzibel *auf $V := \mathbb{R}L$ operiert, d.h. jeder $W(L)$-invariante Teilraum $U \leq V$ ist entweder $\{0\}$ oder V.*

Beweis. $\Rightarrow$: Sei $\{0\} \neq U < V$ mit $Ug = U$ für alle $g \in W(L)$. Dann ist auch $U^\perp$ ein $W(L)$-invarianter Teilraum, da $W(L) \leq O(V)$ und $V = U \oplus U^\perp$. Sei $\alpha \in R(L)$. Wir wollen zeigen, dass entweder $\alpha \in U$ oder $\alpha \in U^\perp$ liegt. Das widerspricht dann der Irreduzibilität von L. Angenommen $\alpha \notin U$. Für $u \in U$ ist dann $u\sigma_\alpha = u - (u, \alpha)\alpha \in U$, da U invariant unter $W(L)$ ist. Also ist $(u, \alpha) = 0$ für alle $u \in U$ (da $\alpha \notin U$) und somit $\alpha \in U^\perp$.
$\Leftarrow$: Wir zeigen: Ist $L = L_1 \perp L_2$, so ist $U := \mathbb{R}L_1$ ein $W(L)$-invarianter Teilraum von V. Denn dann ist $R(L) = R(L_1) \cup R(L_2)$. Für $u \in U$ und $\alpha \in R(L_2)$ ist $u\sigma_\alpha = u \in U$ und für $\alpha \in R(L_1)$ ist $u\sigma_\alpha \in U$. □

Lemma 2.19 *Sei L ein irreduzibles Wurzelgitter. Dann operiert $W(L)$ transitiv auf $R(L)$, d.h. für je zwei Wurzeln $\alpha, \beta \in R(L)$ gibt es ein $g \in W(L)$ mit $\alpha g = \beta$.*

Beweis. Seien $\alpha, \beta \in R(L)$. Dann ist $U := \langle \alpha g \mid g \in W(L) \rangle_\mathbb{R}$ ein $W(L)$-invarianter Teilraum von $\mathbb{R}L = V$ und also nach Lemma 2.18 $U = V$. Die Bilder von α unter den Gruppenelementen erzeugen also den ganzen Raum. Daher gibt es ein $g \in W(L)$ mit $(\alpha g, \beta) \neq 0$. Indem wir α durch αg ersetzen, können wir annehmen, dass $(\alpha, \beta) \neq 0$. Ersetzt man α durch $-\alpha = \alpha\sigma_\alpha$, so kann man weiter annehmen, dass $(\alpha, \beta) > 0$ ist. Dann ist aber entweder $\alpha = \beta$ oder $(\alpha, \beta) = 1$ und $v := \alpha - \beta \in R(L)$. Im letzten Fall ist

$$\alpha\sigma_v = \alpha - (v, \alpha)v = \alpha - (\alpha - \beta) = \beta.$$

□

Satz 2.20 *Sei L ein irreduzibles Wurzelgitter der Dimension n. Dann sind äquivalent:*
(a) $L = L_C$ für einen Code $C \leq \mathbb{F}_p^n$.
(b) $L = L_C$ für einen doppelt geraden Code $C \leq \mathbb{F}_2^n$.
(c) L enthält n paarweise orthogonale Wurzeln, d.h. ein Teilgitter isometrisch zu $\mathbb{A}_1^n := \mathbb{A}_1 \perp \ldots \perp \mathbb{A}_1$.
(d) $-1 \in W(L)$.
(e) $2L^\# \subset L$.
(f) $L \cong \mathbb{A}_1$, $\mathbb{D}_n$ mit $n \geq 4$ gerade, $\mathbb{E}_7$ oder $\mathbb{E}_8$.

Beweis. (a) $\Leftrightarrow$ (b) haben wir oben schon gesehen.
(b) $\Rightarrow$ (c) klar aus Konstruktion von L_C.
(c) $\Rightarrow$ (d): Sind $\alpha_1, \ldots, \alpha_n$ die paarweise orthogonalen Wurzeln, so gilt für

$$g := \sigma_{\alpha_1} \ldots \sigma_{\alpha_n}$$

dass $\alpha_i g = -\alpha_i$ ist $(1 \leq i \leq n)$. Da $(\alpha_1, \ldots, \alpha_n)$ eine $\mathbb{R}$-Basis von $\mathbb{R}L$ ist folgt daraus $g = -1 \in W(L)$.
(d) $\Rightarrow$ (e): Sei $x \in L^\#$ und $\alpha \in R(L)$. Dann ist $(x, \alpha) \in \mathbb{Z}$ und daher

$$x\sigma_\alpha = x - (x, \alpha)\alpha \in x + L$$

d.h. $x - x\sigma_\alpha \in L$. Daher folgt für beliebiges $g \in W(L)$, dass $x - xg \in L$. Insbesondere gilt dies für $g = -1 \in W(L)$ und somit ist $x - (-x) = 2x \in L$. Da $x \in L^\#$ beliebig war, folgt daraus $2L^\# \subset L$.
(e) $\Rightarrow$ (f): Folgt aus Satz 1.15.
(f) $\Rightarrow$ (b): Durch explizite Angabe eines Codes C:
$\mathbb{A}_1$: $C = \{0\} \leq \mathbb{F}_2^1$.
$\mathbb{D}_n$ ($n \geq 4$), gerade: Setze

$$C' := \{(c_1, \ldots, c_{n/2}) \mid \sum c_i = 0\} \leq \mathbb{F}_2^{n/2}$$

und

$$C := \{(c_1, c_1, c_2, c_2, \ldots, c_{n/2}, c_{n/2}) \mid (c_1, \ldots, c_{n/2}) \in C'\}.$$

Eine Basis mit Grammatrix wie in Abschnitt 1.1 erhält man z.B. als Zeilen der Matrix

$$\begin{array}{cccccccc}
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & \ldots \\
1 & 1 & -1 & -1 & 0 & 0 & 0 & 0 & \ldots \\
-2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\
1 & -1 & 1 & -1 & 0 & 0 & 0 & 0 & \ldots \\
0 & 0 & -1 & 1 & 1 & 1 & 0 & 0 & \ldots \\
0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & \ldots \\
0 & 0 & 0 & 0 & 1 & -1 & 1 & 1 & \ldots \\
0 & 0 & 0 & 0 & 0 & 0 & -2 & 0 & \ldots \\
\vdots & & & & & \vdots & & &
\end{array}$$

$\mathbb{E}_7$: $C = H(\mathbb{F}_2, 3)^\perp$.
$\mathbb{E}_8$: $C = e_8 = \widetilde{H(\mathbb{F}_2, 3)}$. □

Satz 2.21 *(Kneser) Jedes Gitter lässt sich eindeutig schreiben als orthogonale Summe irreduzibler Gitter.*

Beweis. Dazu zunächst eine kleine Definition. Wir nennen einen Vektor $x \in L$ unzerlegbar, falls es keine $y, z \in L - \{0\}$ gibt mit $x = y + z$ und $(y, z) = 0$.
Dann gilt: Jeder Vektor $0 \neq x \in L$ ist Summe von unzerlegbaren Vektoren. Denn dies ist klar, wenn x unzerlegbar ist. Ist aber x nicht unzerlegbar, so ist $x = y + z$ mit $0 < (y, y) < (x, x)$ und $0 < (z, z) < (x, x)$. Ist einer der Summanden y oder z nicht unzerlegbar, so kann man ihn wiederum als Summe von Vektoren kleinerer Norm schreiben. Da $L_{<=(x,x)}$ endlich ist, terminiert dieses Verfahren nach endlich vielen Schritten.
Insbesondere wird L von unzerlegbaren Vektoren erzeugt.
Wir nennen zwei unzerlegbare Vektoren y, z verbunden, falls es unzerlegbare Vektoren $x_0 = y, x_1, \ldots, x_t = z$ in L gibt, mit $(x_i, x_{i+1}) \neq 0$ für alle i. Diese Äquivalenzrelation teilt die Menge der unzerlegbaren Vektoren in endlich viele Klassen $K_1, \ldots, K_s$.
Sei $L_i := \langle K_i \rangle_\mathbb{Z}$.
Dann ist $L = L_1 \perp \ldots \perp L_s$ eine Zerlegung in irreduzible Gitter und diese Zerlegung ist eindeutig. □

3 Der LLL-Algorithmus und Anwendungen.

Viele ganz allgemeine Probleme kann man auf das Bestimmen kurzer Vektoren in Gittern zurückführen. Exemplarisch möchte ich hier ein solches Problem (mit Variationen) vorstellen.

Algorithmus 3.1 *Finden $\mathbb{Z}$-linearer Abhängigkeiten komplexer Zahlen.*
EINGABE*: $z_1, \ldots, z_n \in \mathbb{C}$ (bzw. gute Approximationen).*
AUSGABE*: $a_1, \ldots, a_n \in \mathbb{Z}$ mit $\sum_{i=1}^n a_i z_i = 0$.*
IDEE*: Formuliere das Problem so um, dass $(a_1, \ldots, a_n)$ ein kurzer Vektor in einem Gitter ist.*
Wähle $N \in \mathbb{R}_{>0}$ groß und definiere

$$(-,=) : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}, (x,y) := \sum_{j=1}^n x_j y_j + N(\sum_{i=1}^n z_i x_i)(\sum_{i=1}^n \overline{z_i} y_i).$$

Dann ist $(-,=)$ positiv definit. Sei $L = \mathbb{Z}^n$. Ist $a = (a_1, \ldots, a_n) \in L$, mit (a,a) klein, so gilt, falls N groß genug ist, dass $\sum_{i=1}^n a_i z_i$ sehr nahe bei 0 ist.

Beispiel 3.2 *Setzt man $y := 1 + 2^{1/3}$ so ergibt sich $y = z_2 \sim 2.260$, $y^2 = z_3 \sim 5.117$, $y^3 = z_4 \sim 11.542$. Wir wollen eine $\mathbb{Z}$-lineare Abhängigkeit zwischen $z_1 := 1, y, y^2, y^3$ finden. Dazu konstruieren wir zuerst die Grammatrix $\mathcal{G} := I_4 + 10^{10} Z \cdot Z^{tr}$ mit $Z = (1, y, y^2, y^3)$. Dann ist*

$$\mathcal{G} \sim \begin{pmatrix} 10000000001.000 & 22599210498.949 & 51072431517.580 & 115419663055.89 \\ 22599210498.949 & 51072431518.580 & 115419663055.89 & 260839326111.79 \\ 51072431517.580 & 115419663055.89 & 260839326112.79 & 589476283720.41 \\ 115419663055.89 & 260839326111.79 & 589476283720.41 & 1332169861994.6 \end{pmatrix}$$

Der Vektor $v := (-3, 3, -3, 1)$ erfüllt $v \cdot \mathcal{G} \cdot v^{tr} \sim 19$ und ist ein kurzer Vektor in dem Gitter mit Grammatrix $\mathcal{G}$. Tatsächlich gilt $y^3 - 3y^2 + 3y - 3 = 0$.

Algorithmus 3.1 kann man auch benutzen um $\mathbb{Z}$-lineare Abhängigkeiten von Vektoren $z_1, \ldots, z_n \in \mathbb{C}^k$ zu bestimmen.

Eine Anwendung von Algorithmus 3.1 ist das Faktorisieren von Polynomin in $\mathbb{Z}[x]$.

Algorithmus 3.3 EINGABE*: $f \in \mathbb{Z}[x]$ Polynom und numerische Approximation einer komplexen Nullstelle $z \in \mathbb{C}$ mit $f(z) = 0$.*
AUSGABE*: $h, g \in \mathbb{Z}[x]$ mit $f = hg$.*
IDEE*: In der obigen Faktorisierung gilt entweder $h(z) = 0$ oder $g(z) = 0$, d.h. die Koeffizienten von h oder g liefern eine $\mathbb{Z}$-lineare Abhängigkeit der Potenzen von z. Solche Koeffizienten lassen sich also mit Algorithmus 3.1 bestimmen.*

Das Bestimmen kurzer Vektoren in einem Gitter ist ein schwieriges Problem, die vorhandenen Algorithmen können auf heutigen Rechnern die kürzesten Vektoren in Gittern in etwa bis zur Dimension 60 bestimmen. Daher benötigt man einen schnellen Algorithmus, um kurze Vektoren in Gittern zu finden. Dies ist der berühmte LLL-Algorithmus.

Ende am 20.4.2007

Satz 3.4 *(Hermite Ungleichung): Sei $L \subseteq (V, (,))$ ein Gitter. Dann gibt es eine Gitterbasis $B = (b_1, \ldots, b_n)$ von L so dass*

$$\prod_{i=1}^{n} (b_i, b_i) \leq \frac{4}{3}^{n(n-1)/2} \det(L).$$

Beweisidee: Zeige zunächst

Lemma 3.5 *Sei $v \in L$ mit $(v, v) = \min\{(\ell, \ell) \mid 0 \neq \ell \in L\} =: \min(L)$ und $\pi : V \to v^\perp$ die Orthogonalprojektion auf $v^\perp$. Ist $x \in \pi(L)$, so gibt es ein $x_1 \in L$ mit $\pi(x_1) = x$ und $(x_1, x_1) \leq 4/3(x, x)$.*

Beweis. Sei $x_1 \in L$ so, dass $x = \pi(x_1)$ und $x_1 - x = sv$ mit $|s| \leq 1/2$. Dann ist

$$(x_1, x_1) = (sv + x, sv + x) = s^2(v, v) + (x, x) \leq \frac{1}{4}(v, v) + (x, x) \leq 4/3(x, x)$$

denn es ist $(v, v) \leq (x_1, x_1) \leq \frac{1}{4}(v, v) + (x, x)$ und damit $\frac{3}{4}(v, v) \leq (x, x)$, also $\frac{1}{4}(v, v) \leq \frac{1}{3}(x, x)$. Dieses x_1 erfüllt also die Behauptung. □

Beweis. (von Satz 3.4) Induktion über n: $n = 1$ ist trivial.
$(n-1) \Rightarrow n$: Wähle $b_1 \in L$ mit $(b_1, b_1) = \min(L)$. Sei $\pi : V \to b_1^\perp$ wie in 3.5 und $L' := \pi(L)$. Nach Induktion gibt es eine Gitterbasis $(b_2', \ldots, b_n')$ von L' mit $\prod_{i=2}^{n}(b_i', b_i') \leq \frac{4}{3}^{(n-1)(n-2)/2} \det(L')$. Für $i = 2, \ldots, n$ sei $b_i \in L$ mit $\pi(b_i) = b_i'$ und $(b_i, b_i) \leq 4/3(b_i', b_i')$.
Dann ist $(b_1, \ldots, b_n)$ eine Gitterbasis von L:
(Denn sei $L_1 := \langle b_1, \ldots, b_n \rangle \leq L$. Dann ist $\pi(L_1) = L' = \pi(L)$. Also gibt es zu jedem $\ell \in L$ ein $\ell_1 \in L_1$ mit $\ell - \ell_1 \in \ker(\pi_{|L})$. Aber $\ker(\pi) = \langle b_1 \rangle \subset L_1$, also ist $\ell - \ell_1 \in L_1$ und somit $L \subset L_1$.)
Wie im Gram-Schmidt Verfahren sieht man $\det(L')(b_1, b_1) = \det(L)$. Also erfüllt die Basis $(b_1, \ldots, b_n)$ die Behauptung. □

Definition 3.6 *(vgl. Lenstra, Lenstra, Lovasz: Math. Annalen 261, 515-534 (1982))*
Eine Gitterbasis $B := (b_1, \ldots, b_n)$ eines Gitters L heißt LLL-reduziert *(zum Parameter $\frac{3}{4}$), falls für die μ_{ij} und b_i' aus dem Gram-Schmidt-Verfahren 1.6 gilt:*

(a) $|\mu_{ij}| \leq 1/2$ *für alle* $1 \leq j < i \leq n$

(b) $(b_i', b_i') + \mu_{i,i-1}^2(b_{i-1}', b_{i-1}') \geq \frac{3}{4}(b_{i-1}', b_{i-1}')$ *für alle* $i = 2, \ldots, n$.

(Die Bedingung (b) sagt aus, dass die Projektion von b_i auf $\langle b_1, \ldots, b_{i-2} \rangle^\perp$ nicht wesentlich kürzer ist als die Projektion von b_{i-1} auf denselben Raum.) Den Parameter $3/4$ in (b) kann man durch eine beliebige reelle Zahl $\alpha \in (1/4, 1)$ ersetzen.

Satz 3.7 *Sei $B = (b_1, \ldots, b_n)$ eine LLL-reduzierte Basis des Gitters L und $(b_1', \ldots, b_n')$ wie in 1.6. Dann gilt:*

(i) $(b_j, b_j) \leq 2^{i-1}(b'_i, b'_i)$ *für alle* $1 \leq j \leq i \leq n$.

(ii) $\det(L) = \prod_{i=1}^{n}(b'_i, b'_i) \leq \prod_{i=1}^{n}(b_i, b_i) \leq 2^{n(n-1)/2}\det(L)$.

(iii) $(b_1, b_1) \leq 2^{(n-1)/2}\det(L)^{1/n}$.

Ersetzt man den Parameter $3/4$ *in 3.6 (b) durch ein* α *mit* $1/4 < \alpha < 1$, *so gelten analoge Aussagen zu 3.7 (i), (ii), (iii) in denen man 2 durch* $4/(4\alpha - 1)$ *ersetzt.*

Beweis. (i)

$$(b'_i, b'_i) \geq 1/2(b'_{i-1}, b'_{i-1})$$

für alle $2 \leq i \leq n$ nach Definition 3.6 (a) und (b). Also folgt durch Induktion:

$$(b'_j, b'_j) \leq 2^{i-j}(b'_i, b'_i)$$

für alle $1 \leq j \leq i \leq n$. Daraus ergibt sich

$$(b_i, b_i) = (b'_i, b'_i) + \sum_{j=1}^{i-1} \mu_{ij}^2 (b'_j, b'_j) \leq$$

$$(b'_i, b'_i)(1 + 1/4 \sum_{j=1}^{i-1} 2^{i-j}) = (b'_i, b'_i)(1 + 1/4 \cdot (2^i - 2)) \leq 2^{i-1}(b'_i, b'_i).$$

Also $(b_j, b_j) \leq 2^{j-1}(b'_j, b'_j) \leq 2^{i-1}(b'_i, b'_i)$ für alle $1 \leq j \leq i \leq n$.
(ii) Die linke Ungleichung ist die Hadamard Schranke 1.8. Die rechte ergibt sich aus (i):

$$\det(L) = \prod_{j=1}^{n}(b'_j, b'_j) \geq \prod_{j=1}^{n} \frac{1}{2^{j-1}}(b_j, b_j) = 2^{-n(n-1)/2} \prod_{j=1}^{n}(b_j, b_j).$$

(iii) Folgt direkt aus (i), da

$$(b_1, b_1)^n \leq \prod_{i=1}^{n} 2^{i-1}(b'_i, b'_i) = 2^{n(n-1)/2}\det(L).$$

□

Folgerung 3.8 *Ist* $(b_1, \ldots, b_n)$ *eine LLL-reduzierte Basis des Gitters* L, *so ist*

$$(b_1, b_1) \leq 2^{n-1}(x, x)$$

für alle $0 \neq x \in L$.

Beweis. Sei $x = \sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} \alpha_i b'_i$ mit $a_i \in \mathbb{Z}, \alpha_i \in \mathbb{R}$ $(1 \leq i \leq n)$. Ist i maximal mit $a_i \neq 0$, so ist $\alpha_i = a_i$ und $(x, x) \geq a_i^2(b'_i, b'_i) \geq (b'_i, b'_i) \geq 1/2^{i-1}(b_1, b_1) \geq 1/2^{n-1}(b_1, b_1)$. □

Satz 3.9 *Jedes Gitter* L *hat eine LLL-reduzierte Basis.*

Zum Beweis geben wir einen Algorithmus zur Berechnung einer LLL-reduzierten Basis an:

Algorithmus 3.10 *(LLL-Reduktion)*
EINGABE*: Gitterbasis* $(\tilde{b}_1, \ldots, \tilde{b}_n)$ *von* L.
AUSGABE*: LLL-reduzierte Gitterbasis* $(b_1, \ldots, b_n)$ *von* L *und Transformationsmatrix* $T = (t_{ij}) \in GL_n(\mathbb{Z})$ *mit* $b_i = \sum_{j=1}^{n} t_{ij}\tilde{b}_j$.
IDEE*: Iteration über* k*: Im Schritt* k *gilt, dass* $(b_1, \ldots, b_{k-1})$ *eine LLL-reduzierte Basis ist. Man startet mit* $k = 2$*. Ist* $k = n + 1$*, so ist man fertig.*
T_k *bezeichne die* k*-te Zeile von* T.
ALGORITHMUS*:* $T := I_n$*;* $b_i := \tilde{b}_i$ $(1 \leq i \leq n)$*;* $k := 2$*;*
while $(k \leq n)$ *do*
  if $(k \geq 2)$ *then* $\mu_{k,k-1} := (b_k, b'_{k-1})/(b'_{k-1}, b'_{k-1})$*;*
    if $(|\mu_{k,k-1}| > 1/2)$ *then* $r := round(\mu_{k,k-1})$*;* $b_k := b_k - rb_{k-1}$*;*
      $T_k := T_k - rT_{k-1}$*; end if;*
    for $j = 1, \ldots, k-2$ *do* $\mu_{k,j} := (b_k, b'_j)/(b'_j, b'_j)$*; end for;*
    $b'_k := b_k - \sum_{j=1}^{k-1} \mu_{k,j} b'_j$*;*
    Teste Bedingung 3.6 (b) für $i = k$.
    Fall 1: nicht erfüllt
      vertausche b_k *und* b_{k-1} *und* T_k *und* T_{k-1}*;* $k := k - 1$*;*
    end Fall 1;
    Fall 2: erfüllt
      for $j = k-2, \ldots, 1$ *do* $r := round(\mu_{k,j})$*;*
        $b_k := b_k - rb_j$*;* $T_k := T_k - rT_j$*;* $\mu_{k,j} := \mu_{k,j} - r$*;*
        for $l = 1, \ldots, j-1$ *do* $\mu_{k,l} := \mu_{k,l} - r\mu_{j,l}$*; end for;*
      end for;
      k:=k+1;
    end Fall 2;
  else k:=k+1;
  end if;
end while;

Bemerkung 3.11 *(1) Algorithmus 3.10 läßt sich so umformulieren, dass er nur mit Grammatrizen arbeitet.*
(2) Die Koeffizienten von kurzen Gittervektoren bzgl. einer LLL-reduzierten Basis sind klein. Also läuft der Algorithmus zum Berechnen von $L_{\leq S}$ *in Satz 1.9 schneller mit einer LLL-reduzierten Basis.*

Satz 3.12 *Algorithmus 3.10 terminiert.*

Beweis. Sei $d_k := \det((b_i, b_j)_{1 \leq i,j \leq k})$ Setzt man $L_k := \langle b_1, \ldots, b_k \rangle_{\mathbb{Z}}$ so ist $d_k = \det(L_k) = \prod_{j=1}^{k} (b'_j, b'_j)$. Es gilt $d_0 = 1$, $d_n = det(L)$, $d_k \in \mathbb{R}_{>0}$. Ist $m := min(L)$, so ist nach der Hermite Ungleichung (3.8) $d_k \geq \frac{3}{4}^{k(k-1)/2} m^k$ durch eine positive Zahl nach unten beschränkt. Sei $D := \prod_{k=1}^{n-1} d_k$.
Dann ändert sich D nur dann, wenn sich ein (b'_j, b'_j) ändert, also nur im Fall 1.

Dann wird aber d_{k-1} mit einem Faktor $< 3/4$ multipliziert.
d_j bleibt gleich für $j \neq k-1$ da die Menge $\{b_1, \ldots, b_j\}$ und damit auch L_j gleich bleibt. Also wird im Fall 1 die Zahl D mit einem Faktor $< 3/4$ multipliziert. D ist durch eine positive nach unten beschränkt, also tritt Fall 1 nur endlich oft auf und der Algorithmus terminiert. □

Algorithmus 3.13 *MLLL-Algorithmus (=modifizierter LLL-Algorithmus (M. Pohst))*
Algorithmus 3.10 kann so abgeändert werden, dass er mit linear abhängigen Vektoren arbeitet.
EINGABE*: Teilmenge* $(\tilde{b}_1, \ldots, \tilde{b}_m)$ *von* V*.*
AUSGABE*: LLL-reduzierte Menge* $(b_1, \ldots, b_m)$ *mit* $L := \langle \tilde{b}_1, \ldots, \tilde{b}_m \rangle_{\mathbb{Z}} = \langle b_1, \ldots, b_m \rangle_{\mathbb{Z}}$ *und eine Transformationsmatrix* $T = (t_{ij}) \in GL_m(\mathbb{Z})$ *mit* $b_i = \sum_{j=1}^{m} t_{ij} \tilde{b}_j$*.*
IDEE*: Verfahre wie in 3.10 mit dem folgenden Unterschied: Ist* $(b'_k, b'_k) = 0$ *(also* $b'_k = 0$*, d.h.* b_k *ist* $\mathbb{R}$*-linear abhängig von* $b_1, \ldots, b_{k-1}$*), so ist* b'_k *im Gram-Schmidt-Verfahren überflüssig. Setze also* $\mu_{l,k} = 0$ *für alle* $l = k+1, \ldots, m$*.*

Bemerkung 3.14 *Der MLLL-Algorithmus terminiert.*

Beweis. Analog zum Beweis von 3.12. Sei $g_i := (b'_i, b'_i)$ und

$$d_k := \prod_{i \leq k, g_i \neq 0} g_i, \quad D := \prod_{k \leq m, g_k \neq 0} d_k \prod_{k \leq m, g_k = 0} 2^k.$$

D wird nur im Fall 1 verändert.
Ist $g_k \neq 0$, so wird D mit einem Faktor $\leq 3/4$ multipliziert, wie in 3.12.
Ist $g_k = 0$, so werden b_k und b_{k-1} vertauscht. d_{k-1} wird auf d_{k-2} gesetzt, d_k bleibt gleich und D wird insgesamt mit einem Faktor $2^{k-1}/2^k = 1/2 < 1$ multipliziert.
Wie in 3.12 ist D durch eine positive Zahl $(\min(L)^{\dim(L)} 2^{m-\dim(L)})$ nach unten beschränkt. Also tritt Fall 1 nur endlich oft ein und Algorithmus 3.13 terminiert. □

Bemerkung 3.15 *Sei* $n := \dim(\langle \tilde{b}_1, \ldots, \tilde{b}_m \rangle_{\mathbb{R}})$*. Dann gilt für die in 3.13 berechneten Vektoren* $(b_1, \ldots, b_m)$*:* $b_1 = \ldots = b_{m-n} = 0$ *und* $(b_{m-n+1}, \ldots, b_m)$ *ist eine LLL-reduzierte Gitterbasis von* L*.*

II Extreme Gitter.

4 Dichte Kugelpackungen.

Definition 4.1 *Sei $L \in (\mathbb{R}^n, (,))$ ein Gitter. Dann ist*

$$\min(L) := \min\{(\ell, \ell) \mid 0 \neq \ell \in L\}$$

das Minimum *von L und*

$$S(L) := \{\ell \in L \mid (\ell, \ell) = \min(L)\}$$

die Menge der kürzesten Vektoren von L. Nach Satz 1.9 ist $S(L) = \{\ell_1, \ldots, \ell_k\}$ eine endliche Menge. $k = |S(L)|$ heißt auch die Kußzahl *oder auch* kissing number *von L.*

$\frac{1}{2}\sqrt{\min(L)}$ ist der Radius der Kugeln in der zu L gehörenden Kugelpackung. Die Kußzahl ist die Anzahl der Kugeln in der Gitterkugelpackung, die eine feste weitere Kugel berühren.

Definition 4.2 *Bezeichne $\mathcal{L}_n$ die Menge aller n-dimensionalen Gitter. Die* Hermite-Funktion *$\gamma : \mathcal{L}_n \to \mathbb{R}_{>0}$ ist definiert durch*

$$\gamma(L) := \frac{\min(L)}{\det(L)^{1/n}}.$$

$\gamma_n := \sup\{\gamma(L) \mid L \in \mathcal{L}_n\}$ *heißt die* Hermite-Konstante.

Bemerkung 4.3 *Die Dichte der zu L gehörenden gitterförmigen Kugelpackung ist*

$$\Delta(L) = 2^{-n}\gamma(L)^{n/2}V_n$$

wobei V_n das Volumen der n-dimensionalen Einheitskugel bezeichnet. Insbesondere ist $\Delta(L)$ maximal, genau dann wenn $\gamma(L)$ maximal ist.
Das Ziel dieses Abschnitts ist es, einen Algorithmus anzugeben, der die lokalen Maxima von γ auf dem Raum der Ähnlichkeitsklassen von n-dimensionalen Gittern bestimmt.
Dazu müssen wir zunächst auf $\mathcal{L}_n$ eine Topologie definieren.

Hermite Funktion auf Wurzelgittern.

L	$\mathbb{A}_2$	$\mathbb{A}_3$	$\mathbb{A}_4$	$\mathbb{D}_4$	$\mathbb{D}_5$	$\mathbb{D}_6$	$\mathbb{E}_6$	$\mathbb{E}_7$	$\mathbb{E}_8$
$\gamma(L)$	1.155	1.260	1.337	1.414	1.516	1.587	1.665	1.811	2

Bemerkung 4.4 *(a) Die Hermite-Funktion $\gamma : \mathcal{L}_n \to \mathbb{R}_{>0}$ ist konstant auf den Isometrieklassen von Gittern, d.h. $\gamma(L) = \gamma(L')$ falls $L \cong L'$. Sie ändert sich auch nicht bei Skalieren*

$\gamma(sL) = \gamma(L)$ *für alle* $s \in \mathbb{R}_{>0}$. *Also ist* γ *eine Funktion auf der Menge der* Ähnlichkeitsklassen *von* n*-dimensionalen Gittern,* $\gamma : \mathcal{L}_n/(\mathbb{R}^* O_n(\mathbb{R})) \to \mathbb{R}_{>0}$, $[L] \mapsto \gamma(L)$.
(b)

$$\mathrm{Gram} : \mathcal{L}_n/(\mathbb{R}^* O_n(\mathbb{R})) \to \mathbb{R}_{>0}\backslash\mathbb{R}^{n\times n}_{sym,>0}/\,\mathrm{GL}_n(\mathbb{Z}) =: \mathrm{Quad}_n, [L] \mapsto [\mathcal{G}(B)]$$

wo B *eine Gitterbasis von* L *ist, ist eine Bijektion.*
(c) Auf $\mathrm{Sym}_n(\mathbb{R}) := \mathbb{R}^{n\times n}_{sym} := \{A \in \mathbb{R}^{n\times n} \mid A = A^{tr}\}$ *definiert* $(A, B) := \mathrm{Spur}(AB)$ *ein Skalarprodukt und macht* $\mathrm{Sym}_n(\mathbb{R})$ *zu einem Euklidischen Vektorraum* $(\mathrm{Sym}_n(\mathbb{R}), \mathrm{Spur})$ *(der Dimension* $n(n+1)/2$*). Diese Skalarprodukt definiert auch eine Topologie auf* $\mathrm{Sym}_n(\mathbb{R})$.

Definition 4.5 *Sei* $F \in \mathrm{Sym}_n(\mathbb{R})$ *positiv definit.*
(i) $\min(F) := \min\{\ell F \ell^{tr} \mid 0 \neq \ell \in \mathbb{Z}^n\}$ *heißt das* Minimum *von* F.
(ii) $S(F) := \{\ell \in \mathbb{Z}^n \mid \ell F \ell^{tr} = \min(F)\}$ *die Menge aller kürzesten Vektoren von* F.
(iii) $\gamma(F) := \frac{\min(F)}{\det(F)^{1/n}}$ *die* Hermite-Funktion *bei* F.

Bemerkung 4.6 $\gamma(aF) = \gamma(F)$ *für alle* $a \in \mathbb{R}_{>0}$.
$\gamma(TFT^{tr}) = \gamma(F)$ *für alle* $T \in \mathrm{GL}_n(\mathbb{Z})$.
$\gamma(L) = \gamma([L]) = \gamma(\mathrm{Gram}(L))$.

Definition 4.7 *Ein Gitter* $L \in \mathcal{L}_n$ *heißt* extrem *, falls* $[L]$ *ein lokales Maximum der Hermite Funktion* $\gamma : \mathcal{L}_n/(\mathbb{R}^* O_n(\mathbb{R})) \to \mathbb{R}$ *ist, also falls es eine Umgebung* $\mathcal{U}$ *von* $F := \mathrm{Gram}(L)$ *in* $\mathrm{Sym}_n(\mathbb{R})$ *gibt, so dass* $\gamma_{|\mathcal{U}}$ *sein Maximum in* F *annimmt.*

Das Hauptergebnis dieses Abschnitts ist die Voronoi'sche Charakterisierung extremer Gitter Satz 4.19 (unten).

Definition 4.8 *Eine positive definite Matrix* $F \in \mathrm{Sym}_n(\mathbb{R})$ *heißt* perfekt *, falls*

$$\langle x^{tr} x \mid x \in S(F)\rangle_{\mathbb{R}} = \mathrm{Sym}_n(\mathbb{R}).$$

Beachten Sie, dass diese Definition koordinatenunabhängig ist. Ist $T \in \mathrm{GL}_n(\mathbb{R})$ so sind die beiden Vektorräume $\langle (xT)^{tr}(xT) \mid x \in S(F)\rangle_{\mathbb{R}}$ und $\langle x^{tr} x \mid x \in S(F)\rangle_{\mathbb{R}}$ isomorph.

Bemerkung 4.9 *Ist* $T \in \mathrm{GL}_n(\mathbb{Z})$, $s \in \mathbb{R}_{>0}$ *so ist* F *perfekt* $\Leftrightarrow$ $sTFT^{tr}$ *perfekt. Perfektion ist also eine Eigenschaft der Klasse von* F *in* Quad_n. *Ein Gitter* $L \in \mathcal{L}_n$ *heißt* perfekt*, falls* $\mathrm{Gram}(L) \in \mathrm{Quad}_n$ *perfekt ist.*

Ende am 27.4.07

Satz 4.10 *(Korkine, Zolotareff)* $F \in \mathrm{Sym}_{n,>0}(\mathbb{R})$ *ist perfekt, genau dann wenn*

$$\{F\} = \{A \in \mathrm{Sym}_n(\mathbb{R}) \mid xAx^{tr} = \min(F) \text{ für alle } x \in S(F)\}.$$

Die Matrix F *ist durch ihre kürzesten Vektoren eindeutig bestimmt.*

Beweis. Sei $A \in \mathrm{Sym}_n(\mathbb{R})$ eine weitere Lösung des inhomogenen linearen Gleichungssystems $xAx^{tr} = \min(F)$ für alle $x \in S(F)$. Dann ist für alle $x \in S(F)$

$$x(A-F)x^{tr} = \mathrm{Spur}(x(A-F)x^{tr}) = \mathrm{Spur}(x^{tr}x(A-F)) = 0$$

also ist $A - F \in \langle x^{tr}x \mid x \in S(F)\rangle_{\mathbb{R}}^{\perp}$. Dieser Raum ist gleich 0, genau dann wenn F perfekt ist. □

Bemerkung 4.11 *Ist F perfekt, so ist $\frac{1}{2}|S(F)| \geq \dim \mathrm{Sym}_n(\mathbb{R}) = n(n+1)/2$, also $|S(F)| \geq n(n+1)$.*

Bemerkung 4.12 *Ist F perfekt, so ist $\langle S(F)\rangle_{\mathbb{R}} = \mathbb{R}^n$.*

Beweis. Ansonsten gibt es ein $0 \neq y \in \mathbb{R}^n$ mit $(y,x)^2 = 0$ für alle $x \in S(F)$. Dann ist

$$0 = (y,x)^2 = (yx^{tr})^2 = yx^{tr}xy^{tr} = \mathrm{Spur}(yx^{tr}xy^{tr}) = \mathrm{Spur}((y^{tr}y)(x^{tr}x))$$

für alle $x \in S(F)$. Also ist die symmetrische Matrix $y^{tr}y$ aus $\langle x^{tr}x \mid x \in S(F)\rangle_{\mathbb{R}}^{\perp}$. □

Folgerung 4.13 *Ist F perfekt, so gibt es ein $a \in \mathbb{R}_{>0}$ mit $aF \in \mathbb{Z}^{n\times n}$.*

Beweis. Ersetze F durch $\frac{1}{\min(F)}F$. Dann gilt $\min(F) = 1$ und F ist die einzige Lösung des inhomogenen linearen Gleichungssystems $xFx^{tr} = 1$ für alle $x \in S(F) \subset \mathbb{Z}^n$ mit ganzzahligen Koeffizienten. Diese ist rational (Cramer) und daher ist $F \in \mathbb{Q}^{n\times n}$. Nach Multiplikation mit dem Hauptnenner ist F ganzzahlig. □

Satz 4.14 *(Voronoi) Bis auf Ähnlichkeit gibt es nur endlich viele perfekte Gitter in $\mathcal{L}_n$. $\mathrm{Perf}_n := \{[L] \in \mathbb{R}_{>0}\backslash\mathcal{L}_n/O_n(\mathbb{R}) \mid L \text{ ist perfekt }\}$ ist endlich.*

Beweis. Sei $F = \mathrm{Gram}(L)$ perfekt. Œ sei $\min(F) = 1$. Wähle n linear unabhängige Vektoren $x_1, \ldots, x_n \in S(L)$. Dann ist nach Folgerung 1.8

$$\det(L) \leq \det\langle x_1, \ldots, x_n\rangle_{\mathbb{Z}} \leq \prod_{i=1}^{n}(x_i, x_i) \leq 1.$$

Sei $C_n := (4/3)^{n(n-1)/2}$ und $(b_1, \ldots, b_n)$ eine nach Satz 3.4 existierende Gitterbasis von L mit

$$\prod_{i=1}^{n}(b_i, b_i) \leq C_n \det(L) \leq C_n.$$

Dann ist auch $(b_i, b_i) \leq \frac{C_n}{\prod_{j\neq i}(b_j,b_j)} \leq C_n$. Ist $x = \sum_{i=1}^{n} a_i b_i \in L$, so ist

$$a_i^2 = \frac{\det(\langle b_1, \ldots, b_{i-1}, x, b_{i+1}, \ldots, b_n\rangle_{\mathbb{Z}})}{\det(L)} \leq C_n \frac{\prod_{j\neq i}(b_j,b_j)(x,x)}{\prod_{j=1}^{n}(b_j,b_j)} = C_n\frac{(x,x)}{(b_i,b_i)} \leq C_n(x,x).$$

Also gilt für $x \in S(L)$, dass $|a_i| \leq \sqrt{C_n}$.
Also gibt es eine Matrix $TFT^{tr} \in [F]$ mit $T \in \mathrm{GL}_n(\mathbb{Z})$ so dass $S(F) \subset \{(a_1, \ldots, a_n) \in \mathbb{Z}^n \mid |a_i| \leq \sqrt{C_n} = (4/3)^{n(n-1)/4}\}$. Diese Menge ist aber endlich, hat also auch nur endlich viele Teilmengen. Da F nach Satz 4.10 durch $S(F)$ eindeutig bestimmt ist, gibt es auch nur endlich viele Möglichkeiten für F. □

Beispiel 4.15 *$\mathbb{A}_2$ ist einziges 2-dimensionales perfektes Gitter.*

Beweis. $\mathbb{A}_2$ ist perfekt (leicht nachzurechnen, oder siehe Beispiel 4.18). Ist $F \in \mathbb{R}^{2\times 2}$ perfekt, so ist $|S(F)| \geq 2 \cdot 3 = 6$. Weiter gibt es nach obigem Beweis eine zu F äquivalente Form F' so dass

$$S(F') \subset \{(a_1, a_2) \in \mathbb{Z}^2 \mid |a_i| \leq (4/3)^{1/2} < 2\}$$

Insbesondere enthält $S(F)$ eine Basis von $\mathbb{Z}^2$. Bezüglich einer solchen Basis ist $F = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$ mit $b = \pm a/2$ also F ähnlich zu $\mathbb{A}_2$. □

Im nächsten Abschnitt werden wir einen Algorithmus kennenlernen, der es ermöglicht, alle perfekten Gitter aufzulisten. Mit dem Hauptsatz 4.19 liefert dies einen Algorithmus zur Bestimmung aller extremen Gitter und damit auch zur Berechnung der Hermite-Konstante γ_n.

Definition 4.16 *Eine positiv definite Matrix $F \in \mathrm{Sym}_n(\mathbb{R})$ heißt* eutaktisch*, falls es Zahlen $\rho_x > 0$ für alle $x \in S(F)$ gibt mit*

$$F^{-1} = \sum_{x \in S(F)} \rho_x x^{tr} x.$$

Bemerkung 4.17 *Eutaktisch zu sein ist eine Eigenschaft von $[F] \in \mathrm{Quad}_n$. Daher nennen wir ein Gitter L* eutaktisch*, genau dann wenn $\mathrm{Gram}(L)$ eutaktisch ist.*

Beweis. Für $T \in \mathrm{GL}_n(\mathbb{Z})$ ist $S(TFT^{tr}) = S(F)T^{-1}$ und es gilt

$$(TFT^{tr})^{-1} = T^{-tr}F^{-1}T^{-1} = T^{-tr}(\sum_{x \in S(F)} \rho_x x^{tr} x)T^{-1} = \sum_{x \in S(F)} \rho_x (xT^{-1})^{tr} xT^{-1}.$$

□

Beispiel 4.18 *I_n ist eutaktisch aber nicht perfekt.*
$\mathbb{A}_n$ ist eutaktisch und perfekt. Eine mögliche Grammatrix von $\mathbb{A}_n$ ist $A_n := I_n + J_n$ mit $J_n = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \vdots & \vdots \\ 1 & \dots & 1 \end{pmatrix} \in \{1\}^{n\times n}$. (In der Beschreibung $\mathbb{A}_n = \{\sum_{i=1}^{n+1} a_i z_i \in \mathbb{Z}^{n+1} \mid \sum a_i = 0\}$ wo $(z_1, \dots, z_{n+1})$ eine ON-Basis von $\mathbb{Z}^{n+1}$ ist, ist $(z_1 - z_2, \dots, z_1 - z_{n+1})$ eine Gitterbasis von $\mathbb{A}_n$ mit Grammatrix A_n.) Dann gilt $S(A_n) = \{\pm e_i, e_i - e_j \mid 0 \leq i \neq j \leq n\}$ und

$$A_n^{-1} = I_n - \frac{1}{n+1} J_n = \frac{1}{2}\frac{1}{n+1} \sum_{x \in S(A_n)} x^{tr} x.$$

A_n ist minimal perfekt, d.h. $S(A_n) = n(n+1)$. Es ist $(e_i - e_j)^{tr}(e_i - e_j)$ die Matrix die an den Stellen (i,i) und (j,j) eine 1 und bei (i,j) und (j,i) eine -1 stehen hat, und $e_i^{tr} e_i$ die Diagonalmatrix mit einer 1 an Stelle (i,i). Daraus erkennt man, dass die $(x^{tr}x \mid x \in \{e_i, e_i - e_j \mid 0 \leq i < j \leq n\}$ eine Basis von $\mathrm{Sym}_n(\mathbb{R})$ bilden.

Ziel dieses Abschnittes ist es, den folgenden Satz von Voronoi zu beweisen:

Hauptsatz 4.19 *(Voronoi) Ein Gitter L ist extrem genau dann wenn es perfekt und eutaktisch ist.*

Daraus erhält man dann z.B. dass das Gitter $\mathbb{A}_n$ eine lokal dichteste Kugelpackung liefert.

Folgerung 4.20 *(aus dem Hauptsatz)* $\mathrm{Extr}_n := \{[L] \in \mathbb{R}_{>0}\backslash\mathcal{L}_n/O_n(\mathbb{R}) \mid L \text{ ist extrem }\}$ *ist endlich.*

Anzahl Ähnlichkeitsklassen perfekter Gitter.

n	1	2	3	4	5	6	7	8	9
$\lvert\mathrm{Perf}_n\rvert$	1	1	1	2	3	7	33	10916	≥ 524289
$\lvert\mathrm{Extr}_n\rvert$	1	1	1	2	3	6	30	2408	≥ 12814

4.1 Der Beweis der Voronoischen Charakterisierung extremer Gitter.

Eine kleine Vorbemerkung zu Linearformen und Matrizen, die dem gesamten Beweis zugrundeliegt und einen basisfreien Zugang zu den Begriffen perfekt und eutaktisch liefert.

Bemerkung 4.21 *Sei* $\mathrm{End}_s(E)$ *der Raum aller selbstadjungierten Endomorphismen von* $E = (\mathbb{R}^n, (,))$.

$$\mathrm{End}_s(E) = \{f \in \mathrm{End}(\mathbb{R}^n) \mid \ {}_{B^*}f_B \in \mathrm{Sym}_n(\mathbb{R})\}.$$

Die Spurbilinearform macht $\mathrm{End}_s(E)$ *zu einem Euklidischen Vektorraum,* $\mathrm{Spur}(f,g) := \mathrm{Spur}(fg)$ *für* $f, g \in \mathrm{End}_s(E)$. *Also liefert uns die Spurbilinearform einen Isomorphismus*

$$\mathrm{Spur}^* : \mathrm{End}_s(E) \to \mathrm{End}_s(E)^* : f \mapsto (g \mapsto \mathrm{Spur}(gf)).$$

Jedes $0 \neq x \in E$ *definiert einen selbstadjungierten Endomorphismus, die Orthogonalprojektion* p_x *auf* $\langle x\rangle_{\mathbb{R}}$ *definiert durch*

$$p_x : v \mapsto \frac{(v,x)}{(x,x)}x.$$

Die Matrix von p_x *bezüglich einer Orthonormalbasis ist* $\frac{1}{(x,x)}x^{tr}x$. *Es ist* $(x,x)\,\mathrm{Spur}^*(p_x) =: \varphi_x$ *mit*

$$\varphi_x(f) = (xf, x).$$

(Achtung, Normierung !)

Beweis. Zur Berechnung von $\varphi_x(f)$ sei $(b_2, \ldots, b_n)$ eine Basis von $x^\perp$, Dann ist $B := (x, b_2, \ldots, b_n)$ eine Basis von E und ${}_B(p_x)_B = \mathrm{diag}(1, 0, \ldots, 0)$. Sei $f \in \mathrm{End}_s(E)$ und (f_{ij}) die Matrix von f bezüglich B. Dann ist $\mathrm{Spur}(fp_x) = f_{11}$ und $xf = f_{11}x + z$ mit $z \in x^\perp$. Also ist $f_{11} = \frac{(x,xf)}{(x,x)}$. □

Bemerkung 4.22 *Die Bedingung dass $F \in \mathrm{Sym}_n(\mathbb{R})$ perfekt ist, bedeutet dass die $\{\varphi_x \mid x \in S(F)\}$ den Dualraum $\mathrm{End}_s(E)^*$ erzeugen. Die Eutaxiebedingung*

$$\star \quad F^{-1} = \sum_{x \in S(F)} \rho_x x^{tr} x$$

mit positiven ρ_x liest sich in der Sprache der Linearformen wie folgt: Ist B eine Basis mit Grammatrix F, so ist $F^{-1} = {}_{B^*}\mathrm{id}_B$. Ist x die Koordinatenzeile bezüglich der Basis B, so ist $x^{tr}x = (x,x)_{B^*}(p_x)_B$. Also liest sich $\star$ als

$$\mathrm{id} = \min(F) \sum_{x \in S(F)} \rho_x p_x$$

was unter der Identifikation mit dem Dualraum übergeht zu

$$\mathrm{Spur} = \sum_{x \in S(F)} \rho_x \varphi_x$$

als Gleichung für Linearformen auf $\mathrm{End}_s(E)$.

Dies zeigt unter anderem, dass die Eigenschaft eines Gitters perfekt, bzw. eutaktisch zu sein nur von der Geometrie der Menge der kürzesten Vektoren abhängt.

Definition 4.23 *Sei $M \subset E$ eine endliche Menge von Vektoren im Euklidischen Raum.*
(i) M heißt perfekt *, falls*

$$\langle \varphi_x \mid x \in M \rangle = \mathrm{End}_s(E)^*.$$

(ii) M heißt eutaktisch *, falls Zahlen $\rho_x > 0$ (für alle $x \in M$) existieren mit*

$$\mathrm{Spur} = \sum_{x \in M} \rho_x \varphi_x.$$

Ein Gitter, oder auch eine symmetrische positiv definite Matrix, ist also eutaktisch bzw. perfekt, genau dann, wenn seine Menge von kürzesten Vektoren eutaktisch bzw. perfekt ist.

Der Rest des Abschnitts ist einem Beweis des Hauptsatzes 4.19 gewidmet. Dazu zunächst ein Satz von allgemeinem Interesse:

Satz 4.24 *(Stiemke, 1915) Sei V ein $\mathbb{R}$-Vektorraum, $\varphi_1, \ldots, \varphi_t \in V^*$. Äquivalent sind:*
(i) $\{x \in V \mid \varphi_j(x) \geq 0$ für alle $1 \leq j \leq t\} = \bigcap_{i=1}^t \ker(\varphi_i)$.
(ii) Es gibt $a_1, \ldots, a_t \in \mathbb{R}_{>0}$ mit $a_1\varphi_1 + \ldots + a_t\varphi_t = 0$.

Beweis. (ii) $\Rightarrow$ (i) Ist klar. Ist nämlich $x \in V$ mit $\varphi_j(x) \geq 0$ für alle $1 \leq j \leq t$, so ist auch $0 = \sum_{j=1}^t a_j\varphi_j(x)$ eine Summe von nichtnegativen Zahlen. Also ist $\varphi_j(x) = 0$ für alle j und damit $x \in \bigcap_{i=1}^t \ker(\varphi_i)$.
(i) $\Rightarrow$ (ii): Wir gehen zu $V/\bigcap_{i=1}^t \ker(\varphi_i)$ über und nehmen an, dass $\bigcap_{i=1}^t \ker(\varphi_i) = \{0\}$, also $V^* = \langle \varphi_1, \ldots, \varphi_t \rangle$. Betrachte

$$\star := \{M \subset \{\varphi_1, \ldots, \varphi_t\} \mid \exists x \in V, \psi(x) \geq 0 \text{ für alle } \psi \in M,\ \psi(x) > 0 \text{ für ein } \psi \in M\}$$

Sei $M \in \star$ eine Menge mit maximaler Kardinalität $|M| =: m$. Œ $M = \{\varphi_1, \ldots, \varphi_m\}$. Dann gilt $\langle M \rangle = V^*$, denn sonst gibt es ein $y \in V$ mit $\varphi_i(y) = 0$ für alle $1 \leq i \leq m$. Da $\langle \varphi_1, \ldots, \varphi_t \rangle = V^*$, gibt es ein φ_s mit $\varphi_s(y) \neq 0$. Wählt man $\lambda \in \mathbb{R}$ so daß $\varphi_s(x + \lambda y) \geq 0$ mit x wie in $\star$, so sieht man, dass $M \cup \{\varphi_s\} \in \star$ ein Widerspruch zur Maximalität von M.
Fall 1: Es ist $t > m+1$: Dann ist $t-1 > m$ und Induktion über t liefert $a'_1, \ldots, a'_{t-1} > 0$ mit $\sum_{i=1}^{t-1} a'_i \varphi_i = 0$. Da $\langle \varphi_1, \ldots, \varphi_m \rangle = V^*$ gibt es $b_1, \ldots, b_m$ mit $\varphi_t = \sum_{j=1}^{m} b_j \varphi_j$. Wähle $a_t > 0$ mit $a_i := a'_i - a_t b_i > 0$ für $i = 1, \ldots, m$ und setze $a_i := a'_i$ für $i = m+1, \ldots, t-1$. Dann ist $\sum_{i=1}^{t} a_i \varphi_i = 0$.
Fall 2: Es ist $t = m+1$. Sei $W := \ker(\varphi_t)$ und wende Induktion an auf $\varphi_{1|W}, \ldots, \varphi_{(t-1)|W}$. Danach gibt es $a_1, \ldots, a_{t-1} > 0$ mit $(\sum_{i=1}^{t-1} a_i \varphi_i)_{|W} = 0$. Nach Definition von m gibt es $x \in V$ mit $\varphi_i(x) \geq 0$ für alle $1 \leq i \leq m = t-1$ und $\varphi_i(x) > 0$ für ein i. Da m maximal war folgt dann $\varphi_t(x) < 0$. Setze $a_t := -\frac{1}{\varphi_t(x)} \sum_{i=1}^{t-1} a_i \varphi_i(x)$. Dann ist $a_t > 0$ und $\sum_{i=1}^{t} a_i \varphi_i(x) = 0$. Da $(\sum_{i=1}^{t} a_i \varphi_i)_{|W} = 0$ ist und $V = \langle W, x \rangle$ folgt $\sum_{i=1}^{t} a_i \varphi_i = 0$. □

Satz 4.25 *Sei $0 \neq \alpha \in \mathrm{End}_s(E)$ und $J := [-\epsilon, \epsilon]$ ein Intervall, so dass $\alpha_t := t\alpha + \mathrm{id}$ für $t \in J$ nur positive Eigenwerte hat. Dann ist die Funktion*

$$f : J \to \mathbb{R}, t \mapsto \det(\alpha_t)$$

strikt logarithmisch konkav (d.h. $g := \log(f)$ ist strikt konkav) und $1/f : J \to \mathbb{R}, t \mapsto \det(\alpha_t)^{-1}$ ist strikt konvex.

Beweis. Sind $a_1, \ldots, a_n \in \mathbb{R}$ die Eigenwerte von α, so ist $\det(\alpha_t) = \prod_{i=1}^{n}(1 + \lambda_i t)$. Sei $g := \log(f)$. Dann ist $g' = \sum_{i=1}^{n} \frac{\lambda_i}{1+t\lambda_i}$ und $g'' = -\sum_{i=1}^{n} \frac{\lambda_i^2}{(1+t\lambda_i)^2} < 0$. Also ist g' streng monoton fallend und damit $g = \log(f)$ strikt konkav.
Sei $\tilde{f} := \frac{1}{f} = \prod_{i=1}^{n} g_i$ mit $g_i(t) = \frac{1}{1+t\lambda_i}$. Dann ist $\tilde{f}' = \sum_{j=1}^{n} g'_j \prod_{i \neq j} g_i$ und

$$\tilde{f}'' = \sum_{j=1}^{n} g''_j \prod_{i \neq j} g_i + \sum_{j \neq k} g'_j g'_k \prod_{i \neq j,k} g_i.$$

Nun ist $g'_i = \frac{-\lambda_i}{(1+\lambda_i t)^2}$ und $g''_i = \frac{2\lambda_i^2}{(1+\lambda_i t)^3}$ also

$$\frac{\tilde{f}''}{\tilde{f}} = \sum_{j=1}^{n} 2\Big(\frac{\lambda_j}{1+t\lambda_j}\Big)^2 + \sum_{j \neq k} \frac{\lambda_j}{1+t\lambda_j} \frac{\lambda_k}{1+t\lambda_k} > 0$$

da $2\sum x_i^2 + \sum_{i \neq j} x_i x_j$ positiv definit ist. Da aber $\tilde{f} > 0$ auf J ist, ist somit auch $\tilde{f}'' > 0$ und damit $\tilde{f}$ strikt konvex. □

Lemma 4.26 *(i) Es gibt eine Umgebung $\mathcal{U}$ von 0 in $\mathrm{End}_s(E)$ so dass für jedes $h \in \mathcal{U}$ mit $\mathrm{Spur}(h) \leq 0$ und jedes $g \in \mathrm{End}(E)$ mit $gg^{tr} = \mathrm{id} + h$ gilt: $g \in O(E)$ (also $h = 0$) oder $|\det(g)| < 1$.*
(ii) Sei K ein abgeschlossener Kegel in $\mathrm{End}_s(E)$ mit $\mathrm{Spur}(h) > 0$ für alle $0 \neq h \in K$. Dann gibt es $\alpha > 0$ so dass für alle $h \in K$ mit $0 < \mathrm{Spur}(h^2) < \alpha$ gilt $\det(\mathrm{id} + h) > 1$.

Beweis. (i) Seien $\lambda_1, \ldots, \lambda_n$ die Eigenwerte von h. Dann sind $1+\lambda_1, \ldots, 1+\lambda_n$ die Eigenwerte von $\mathrm{id}+h$. Bei geeigneter Wahl von $\mathcal{U}$ kann man erreichen dass die $1+\lambda_i$ alle positiv sind für alle $h \in \mathcal{U}$. Betrachte

$$f = f_h : [0,1] \to \mathbb{R}, t \mapsto \det(\mathrm{id}+th) = \prod_{i=1}^{n}(1+t\lambda_i)$$

und setze $f_1 := \log(f)$. Dann ist $f_1'(t) = \sum_{i=1}^{n} \frac{\lambda_i}{1+t\lambda_i}$ und insbesondere $f_1'(0) = \mathrm{Spur}(h) \leq 0$
Ist $h = 0$, so ist $g \in O(E)$.
Ist $h \neq 0$, so ist so ist nach Satz 4.25 die Funktion f_1 strikt konkav, also f_1' streng monoton fallend und $f_1'(t) \leq 0$ für $t \in [0,1]$. Damit ist aber $f_1(1) < f_1(0) = 1$ also

$$\det(\mathrm{id}+h) = \exp(f_1(1)) < \exp(f_1(0)) = 1.$$

(ii) Sei $M := \{h \in \mathrm{End}_s(E) \mid \mathrm{Spur}(h^2) = 1\}$ und wähle $h \in K \cap M$ und sei $f_h : t \mapsto \det(\mathrm{id}+th)$, $g_h := \log(f_h)$ wie eben. Dann ist $g_h'(0) = \mathrm{Spur}(h) > 0$ und $g_h(0) = 0$. Also gibt es ein $t_h > 0$ mit $g_h(t_h) > 0$. Die Abbildung

$$\tilde{g} : K \cap M \to \mathbb{R}, h' \mapsto g_{h'}(t_h) = \log(\prod_{i=1}^{n}(1+t_h\lambda_i'))$$

ist stetig und positive bei h. Also gibt es eine Umgebung U_h von h in $K \cap M$ mit $\tilde{g}(h') > 0$ für alle $h' \in U_h$. Nun ist $K \cap M$ kompakt (da K abgeschlossen und M kompakt), d.h. es gibt endlich viele h_i $1 \leq i \leq a$ mit

$$K \cap M = \cup_{i=1}^{a} U_{h_i}.$$

Setze $\alpha := \min\{t_{h_i}^2 \mid 1 \leq i \leq a\}$. Ist nun $h \in K$ mit $0 \leq \mathrm{Spur}(h^2) \leq \alpha$ so ist $h' := \frac{1}{\sqrt{\mathrm{Spur}(h^2)}} h \in M \cap K$ und es gibt ein h_i mit $h' \in U_{h_i}$. Dann ist $g_{h'}(t) > 0$ auf $[0, \sqrt{\alpha}] \subset [0, t_{h_i}]$ und daher auch für $t := \sqrt{\mathrm{Spur}(h^2)}$, d.h. $\det(\mathrm{id}+h) > 1$. □

Erinnerung an die Polarzerlegung

Lemma 4.27 *Sei $L \in \mathcal{L}_n$. Dann gibt es eine Umgebung $\mathcal{U}$ von $\mathrm{id} \in \mathrm{End}(E)$, so dass*

$$S(Lg) \subset S(L)g \text{ für alle } g \in \mathcal{U}.$$

Beweis. Sei $m_1 := \min(L)$ und $m_2 := \min\{(x,x) \mid x \in L, (x,x) > m_1\}$. Wir benutzen die Polarzerlegung von $g \in \mathrm{GL}(E)$ als $g = g_o g_s$ mit $g_o \in O(E)$ und $g_s \in \mathrm{End}_s(E)$. Wähle $\mathcal{U}$ so klein, dass für alle $g \in \mathcal{U}$ alle Eigenwerte des symmetrischen Anteils g_s positiv sind und für den kleinsten und gröss ten Eigenwert $\lambda_{\max}$ bzw. $\lambda_{\min}$ von g_s gilt, dass

$$\left(\frac{\lambda_{\max}}{\lambda_{\min}}\right)^2 < \frac{m_2}{m_1}.$$

Dann ist für $x \in L$ mit $(x,x) > m_1$ (d.h. $(x,x) \geq m_2$) und $y \in L$ mit $(y,y) = m_1$

$$(yg, yg) = (yg_s, yg_s) \leq \lambda_{\max}^2 (y,y) = \lambda_{\max}^2 m_1$$
$$(xg, xg) = (xg_s, xg_s) \geq \lambda_{\min}^2 (x,x) \geq \lambda_{\min}^2 m_2 > (yg, yg)$$

□

Lemma 4.28 *Es gibt eine Umgebung $\mathcal{U}$ von* $\mathrm{id} \in \mathrm{End}(E)$*, so dass für alle $g \in \mathcal{U}$ gilt* $\min(Lg) = \min(L)$ *genau dann wenn* $\min\{\varphi_x(h_g) \mid x \in S(L)\} = 0$ *wobei* $h_g = g_s^2 - \mathrm{id} \in \mathrm{End}_s(E)$.

Beweis. Sei $\mathcal{U}$ so klein, dass $S(Lg) \subset S(L)g$ für alle $g \in \mathcal{U}$ (existiert nach Lemma 4.27). Es ist für $x \in S(L)$:

$$(xg, xg) = (xg_s^2, x) = (x(\mathrm{id} + h_g), x) = \varphi_x(\mathrm{id}) + \varphi_x(h_g) = (x, x) + \varphi_x(h_g).$$

Also ist

$$\min(Lg) = \min(L) + \min\{\varphi_x(h_g) \mid x \in S(L)\}.$$

□

Satz 4.29 *(Korkine, Zolotareff, 1877) Sei $L \in \mathcal{L}_n$. Dann gilt: L ist extrem genau dann wenn für alle $h \in \mathrm{End}_s(E)$ mit* $\mathrm{Spur}(h) \leq 0$ *und* $\min\{\varphi_x(h) \mid x \in S(L)\} = 0$ *gilt $h = 0$.*

Beweis. L ist nach Definition extrem, wenn eine Umgebung $\mathcal{U}$ von $\mathrm{id} \in \mathrm{End}(E)$ existiert so dass für $g \in \mathcal{U}$ gilt

$$\gamma(Lg) \geq \gamma(L) \Rightarrow g \in \mathbb{R}^* O(E) \text{ und dann natürlich auch } \gamma(Lg) = \gamma(L).$$

Durch Skalieren mit $\mathbb{R}^*$ können wir uns auf solche $g \in \mathcal{U}$ beschränken, mit $\min(Lg) = \min(L)$. Dann ist $h_g := g_s^2 - \mathrm{id} \in \mathrm{End}_s(E)$ mit $\min\{\varphi_x(h_g) \mid x \in S(L)\} = 0$. Jedes solche h_g liegt dann also in

$$K := \{h \in \mathrm{End}_s(E) \mid \varphi_x(h) \geq 0 \text{ für alle } x \in S(L)\}.$$

Dies ist ein abgeschlossener Kegel in $\mathrm{End}_s(E)$.
$\Rightarrow$: Sei L extrem und $h = h_g \in K$ mit $\mathrm{Spur}(h) \leq 0$. Dann ist nach Lemma 4.26 entweder g orthogonal (und damit $L \cong Lg$) oder $|\det(g)| < 1$ und damit $\det(Lg) < \det(L)$. In diesem Fall ist aber wegen $\min(L) = \min(Lg)$ die Hermite Funktion $\gamma(L) > \gamma(Lg)$.
$\Leftarrow$: Angenommen L ist nicht extrem. Dann gibt es für jede Umgebung $\mathcal{U}$ von id in $\mathrm{End}(E)$ ein $g \in \mathcal{U}$ mit $\min(L) = \min(Lg)$ (also $h_g = g_s^2 - \mathrm{id} \in K$) und $\gamma(Lg) \geq \gamma(L)$ aber $g \notin O(E)$. Dann ist $|\det(g)| \leq 1$ und also

$$\det(g_s^2) = \det(h_g + \mathrm{id}) \leq 1.$$

Wählt man g nahe genug bei id, so kann man h_g beliebig klein machen. Nach Lemma 4.26 (ii) kann dann aber nicht $\mathrm{Spur}(h_g) > 0$ gelten für alle $g \in \mathcal{U}$. Also gibt es ein $0 \neq h_g \in K$ mit $\mathrm{Spur}(h_g) < 0$, ein Widerspruch zur Voraussetzung. □

Beweis. (von Hauptsatz 4.19) Dazu benutzen wir die Charakterisierung von Extremheit in Satz 4.29.
$\Leftarrow$: Sei L eutaktisch und perfekt und betrachte $h \in \mathrm{End}_s(E)$ mit $\min\{\varphi_x(h) \mid x \in S(L)\} = 0$ und $\mathrm{Spur}(h) \leq 0$. Da L eutaktisch ist, gibt es $a_x \in \mathbb{R}_{>0}$ mit

$$\mathrm{Spur}(h) = \sum_{x \in S(L)} a_x \varphi_x(h)$$

Das $\mathrm{Spur}(h) \leq 0$ ist und $\varphi_x(h) \geq 0$ für alle $x \in S(L)$ folgt $\varphi_x(h) = 0$ für alle $x \in S(L)$. Da jetzt L perfekt ist folgt daraus dann $h = 0$, da die φ_x mit $x \in S(L)$ den Raum $\mathrm{End}_s(E)^*$ erzeugen. Also ist L extrem mit Satz 4.29.
$\Rightarrow$: Sei nun L extrem. Zeigen L ist perfekt und eutaktisch.
L ist perfekt: Sei $h \in \mathrm{End}_s(E)$ mit $\varphi_x(h) = 0$ für alle $x \in S(L)$. Œ sei $\mathrm{Spur}(h) \leq 0$, sonst ersetzen wir h durch $-h$. Da L extrem ist folgt nach Satz 4.29, dass $h = 0$ ist. Damit ist aber $\langle \varphi_x \mid x \in S(L)\rangle^{\perp} = 0$ und also $\langle \varphi_x \mid x \in S(L)\rangle = \mathrm{End}_s(E)$ was bedeutet, dass L perfekt ist.
L ist eutaktisch: Wende Satz 4.24 an auf φ_x ($x \in S(L)$) und $-\mathrm{Spur}$. Dazu genügt es aus den Ungleichungen

$$\varphi_x(h) \geq 0,\ \mathrm{Spur}(h) \leq 0 \text{ für } h \in \mathrm{End}_s(E)$$

zu folgern, dass $h = 0$ ist. Für $r \in \mathbb{R}$ setze $h' := h - r\,\mathrm{id}$. Dann ist $\mathrm{Spur}(h') = \mathrm{Spur}(h) - nr$ und $\varphi_x(h') = \varphi_x(h) - r\min(L)$. Wähle $r \geq 0$ so dass $\min\{\varphi_x(h') \mid x \in S(L)\} = 0$. Dann gilt immer noch $\mathrm{Spur}(h') \leq 0$. Also nach Satz 4.29 ist $h' = 0$. Damit ist aber $h = r\,\mathrm{id}$ für ein $r \geq 0$. Wegen $\mathrm{Spur}(h) \leq 0$ folgt $r = 0$ und somit $h = 0$. □

5 Der Voronoi Algorithmus zur Bestimmung aller perfekter Gitter.

Um Trivialitäten zu vermeiden setzen wir im ganzen Abschnitt voraus, dass die Dimension $n \geq 2$ ist.

Bemerkung 5.1 $\mathrm{Sym}_n^{\geq 0}(\mathbb{R}) =: \mathcal{K}$ *bezeichne den Kegel aller positiv semidefiniten symmetrischen Matrizen. Dies ist ein konvexer abgeschlossener Kegel in* $\mathrm{Sym}_n(\mathbb{R})$*, der den Raum aller symmetrischen Matrizen* $\mathrm{Sym}_n(\mathbb{R})$ *erzeugt.*
Auf $\mathrm{Sym}_n(\mathbb{R})$ *definiert* $(A, B) \mapsto \mathrm{Spur}(AB)$ *ein euklidisches Skalarprodukt wodurch* $\mathrm{Sym}_n(\mathbb{R})$ *mit seinem Dualraum* $\mathrm{Sym}_n(\mathbb{R})^*$ *identifiziert wird.*

Definition 5.2 *Sei* $F \in \mathrm{Sym}_n(\mathbb{R})$ *positiv definit. Dann bezeichnet* $\mathcal{V}(F)$ *den* Voronoi Bereich *von* F*, das ist der Kegel in* $\mathrm{Sym}_n(\mathbb{R})$*, der von den symmetrischen positiv semidefiniten Matrizen* $x^{tr}x$ *mit* $x \in S(F)$ *erzeugt wird.*

$$\mathcal{V}(F) := \{ \sum_{x \in S(F)} \lambda_x x^{tr} x \mid \lambda_x \geq 0\}.$$

Für ein Gitter L *setzen wir*

$$\mathcal{V}(L) := \{ \sum_{x \in S(L)} \lambda_x x^{tr} x \mid \lambda_x \geq 0\}.$$

Bemerkung 5.3 $\mathcal{V}(F) \subset \mathrm{Sym}_n^{\geq 0}(\mathbb{R})$.
F ist perfekt, genau dann wenn $\mathcal{V}(F)$ nicht leeres Inneres hat, genau dann, wenn $\mathcal{V}(F)$ in keiner Hyperebene von $\mathrm{Sym}_n(\mathbb{R})$ *enthalten ist.*

Das Hauptergebnis dieses Abschnitts wird sein, dass die Voronoi-Bereiche der perfekten Formen eine face-to-face Pflasterung von $\mathcal{K}$ bilden, d.h. die Vereinigung aller Voronoi-Bereiche perfekter Formen ist ganz $\mathcal{K}$ und der Schnitt zweier benachbarter Voronoibereiche ist eine ganze Seite von jedem der beiden Voronoibereiche.

Lemma 5.4 *Sei $F \in \mathrm{Sym}_n(\mathbb{R})$ positiv definit. Dann sind die Kanten von $\mathcal{V}(F)$ genau die Strahlen $\{\mathbb{R}_{>0}x^{tr}x \mid x \in S(F)\}$. Insbesondere ist $S(F)$ durch $\mathcal{V}(F)$ eindeutig bestimmt.*

Beweis. Den Beweis führen wir in der Sprache der Gitter. Sei also L ein Gitter mit Grammatrix F. Œ sei $\min(L) = 1$. Wir betrachten Koordinatenzeilen bezüglich einer ON-Basis von $\mathbb{R}^n$.
Sei $H := \{X \in \mathrm{Sym}_n^{\geq 0}(\mathbb{R}) \mid \mathrm{Spur}(X) = 1\}$. Dann ist $P := H \cap \mathcal{V}(L)$ die konvexe Hülle der Rang 1 Matrizen in $\mathcal{X} := \{x^{tr}x \mid x \in S(L)\}$. Insbesondere sind die Ecken von P alle in $\mathcal{X}$. Sei umgekehrt $X = x^{tr}x \in \mathcal{X}$ keine Ecke von P. Dann gibt es $Y_i = y_i^{tr}y_i \in \mathcal{X}$ mit $Y_i \neq X$ für alle i und positive Zahlen $\lambda_i > 0$ mit $\sum_{i=1}^t \lambda_i = 1$ und

$$x^{tr}x = \sum_{i=1}^{t} \lambda_i y_i^{tr} y_i.$$

Sei $z := \max\{(x, y_i)^2 \mid 1 \leq i \leq t\}$. Dann ist $z < 1$, da $x \neq \pm y_i$ für alle i (nach Cauchy-Schwarz). Es ist aber

$$1 = (x,x)^2 = xx^{tr}xx^{tr} = \sum_{i=1}^{t} \lambda_i (xy_i^{tr})(y_i x^{tr}) \leq \sum_{i=1}^{t} \lambda_i z = z < 1$$

ein Widerspruch. □

Bemerkung zum relativen Inneren.
Sei M eine Teilmenge eines Euklidischen Raums E und $\tilde{E} = \langle M \rangle$ der von M erzeugte Teilraum.
Das relative Innere von M ist die Menge aller $z \in \tilde{E}$, für die eine Umgebung von z in $\tilde{E}$ existiert, die ganz in M liegt. Da Innere von M ist die Menge aller $z \in E$, für die eine Umgebung von z in E existiert, die ganz in M liegt. Insbesondere ist das Innere von M gleich leer, falls $\tilde{E} \neq E$.
Nach Lemma 5.4 ist das relative Innere von $\mathcal{V}(F)$ gleich

$$\{ \sum_{x \in S(F)} \lambda_x x^{tr}x \mid \lambda_x > 0 \text{ für alle } x \in S(F)\}.$$

Denn sei $z = \sum_{x \in S(F)} \lambda_x x^{tr}x$ im relativen Inneren von $\mathcal{V}(F)$. Dann sind die λ_x in der Regel nicht eindeutig und auch nicht notwendigerweise > 0. Sei U eine Umgebung von z, die ganz in $\mathcal{V}(F)$ liegt. Dann gibt es $\epsilon > 0$ mit $z - \epsilon \sum_{x \in S(F)} x^{tr}x \in U$. Also gibt es $a_x \geq 0$ mit $z - \epsilon \sum_{x \in S(F)} x^{tr}x = \sum_{x \in S(F)} a_x x^{tr}x$ und daher ist $z = \sum_{x \in S(F)} (a_x + \epsilon) x^{tr}x$ eine positive Linearkombination der $x^{tr}x$.

Folgerung 5.5 *F ist eutaktisch, genau dann, wenn F^{-1} im relativen Inneren von $\mathcal{V}(F)$ liegt.*

Bemerkung 5.6 *Sei $F \in \mathrm{Sym}_n(\mathbb{R})$ positiv definit, so dass $\langle S(F)\rangle = \mathbb{R}^n$. (Man nennt dann F auch* well-rounded *.) Sei G im relativen Inneren von $\mathcal{V}(F)$. Dann ist G auch positiv definit.*

Beweis. Ist G im relativen Inneren von $\mathcal{V}(F)$, so gibt es $\lambda_x > 0$ mit $G = \sum_{x \in S(F)} \lambda_x x^{tr} x$. Dann ist aber für beliebiges $0 \neq v \in \mathbb{R}^n$:

$$vGv^{tr} = \sum_{x \in S(F)} \lambda_x (vx^{tr} xv^{tr}) = \sum_{x \in S(F)} \lambda_x (xv^{tr})^2 > 0$$

da $v \notin S(F)^\perp = 0$ (bezüglich des Standardskalarprodukts). □

Definition 5.7 *Sei F perfekt und $\mathcal{S}$ eine Seite des Voronoi-Bereichs $\mathcal{V}(F)$. Ein* Seitenvektor *(facet vector, vecteur de face) von F zur Seite $\mathcal{S}$ ist eine Matrix $0 \neq R \in \mathrm{Sym}_n(\mathbb{R})$ mit $\mathrm{Spur}(RS) = 0$ für alle $S \in \mathcal{S}$ und $\mathrm{Spur}(RT) \geq 0$ für alle $T \in \mathcal{V}(F)$.*

Bemerkung 5.8 *Ist F perfekt und $\mathcal{S}$ eine Seite von $\mathcal{V}(F)$, so ist $R \in \mathrm{Sym}_n(\mathbb{R})$ genau dann ein Seitenvektor zu $\mathcal{S}$, wenn*
(i) Für alle $x \in S(F)$ mit $x^{tr}x \in \mathcal{S}$ ist $\mathrm{Spur}(x^{tr}xR) = xRx^{tr} = 0$ und
(ii) Für alle $x \in S(F)$ mit $x^{tr}x \notin \mathcal{S}$ ist $\mathrm{Spur}(x^{tr}xR) = xRx^{tr} > 0$.

Der Seitenvektor R erzeugt also die Lösungsmenge des rationalen homogenen linearen GLS $xRx^{tr} = 0$ für alle $x \in S(F)$ mit $x^{tr}x \in \mathcal{S}$ und kann daher rational gewählt werden.

Satz 5.9 *Sei $n \geq 2$. Sei F perfekt und $\mathcal{S}$ eine Seite von $\mathcal{V}(F)$ mit Seitenvektor $R \in \mathrm{Sym}_n(\mathbb{R})$. Dann ist R indefinit und es gibt ein $x \in \mathbb{Z}^n$ mit $xRx^{tr} < 0$.*

Beweis. Erinnerung: Ist $R \in \mathrm{Sym}_n(\mathbb{R})$ positiv semidefinit, so gibt es $T \in \mathrm{GL}_n(\mathbb{R})$ mit $TRT^{tr} = \mathrm{diag}(1, \ldots, 1, 0, \ldots, 0)$. Insbesondere ist das Radikal von R $\mathrm{rad}(R) := \{v \in \mathbb{R}^n \mid vR = 0\} \leq \mathbb{R}^n$ genau die Menge aller isotroper Vektoren von R, $\mathrm{iso}(R) := \{v \in \mathbb{R}^n \mid vRv^{tr} = 0\}$. Diese bilden also einen Teilraum von $\mathbb{R}^n$ der Dimension $d < n$. Also ist $\langle v^{tr}v \mid \mathrm{Spur}(v^{tr}vR) = 0\rangle$ ein Teilraum von $\mathrm{Sym}_n(\mathbb{R})$ der Dimension

$$\leq \frac{d(d+1)}{2} \leq \frac{(n-1)n}{2} < \frac{n(n+1)}{2} - 1 = \dim(\mathrm{Sym}_n(\mathbb{R})) - 1.$$

Die Seite $\mathcal{S}$ hat aber Dimension $\frac{n(n+1)}{2} - 1$ und wird von gewissen $v^{tr}v$ mit $v \in \mathrm{iso}(R)$ erzeugt. Also ist R indefinit.
Dann gibt es aber auch ein $x \in \mathbb{Z}^n$ mit $xRx^{tr} < 0$. Denn es gibt ein solches $x \in \mathbb{R}^n$ mit $xRx^{tr} \leq -\epsilon < 0$. Die Abbildung $x \mapsto xRx^{tr}$ ist stetig (als Polynom in n Unbestimmten) und $\mathbb{Q}^n$ liegt dicht in $\mathbb{R}^n$. Also kann man ein $y \in \mathbb{Q}^n$ finden mit $yRy^{tr} < 0$. Ist N der Hauptnenner der Koordinaten y_i, so ist $z := Ny \in \mathbb{Z}^n$ und $zRz^{tr} = N^2(yRy^{tr}) < 0$. □

Satz 5.10 *Seien F_1, F_2 symmetrische positiv definite Matrizen,*
(a) Sei $T \in \mathcal{V}(F_2)$ im relativen Inneren von $\mathcal{V}(F_1)$. Dann gilt $\mathcal{V}(F_1) \subset \mathcal{V}(F_2)$.
(b) Keine Matrix im Inneren des Voronoi-Bereichs einer perfekten Form liegt in irgendeinem anderen Voronoi-Bereich.

Beweis. (a) Œ sei $\min(F_1) = \min(F_2) =: m$. Sei $T \in \mathcal{V}(F_1) \cap \mathcal{V}(F_2)$. Dann gibt es $\lambda_x \geq 0$ mit

$$T = \sum_{x \in S(F_1)} \lambda_x x^{tr} x.$$

Dann ist

$$\mathrm{Spur}(TF_1) = \sum_{x \in S(F_1)} \lambda_x \,\mathrm{Spur}(x^{tr} x F_1) = m \sum_{x \in S(F_1)} \lambda_x$$

und

$$\mathrm{Spur}(TF_2) = \sum_{x \in S(F_1)} \lambda_x (x F_2 x^{tr}) \geq m \sum_{x \in S(F_1)} \lambda_x = \mathrm{Spur}(TF_1).$$

Ebenso findet man $\mathrm{Spur}(TF_1) \geq \mathrm{Spur}(TF_2)$ also $\mathrm{Spur}(TF_1) = \mathrm{Spur}(TF_2)$. Ist T im relativen Inneren von $\mathcal{V}(F_1)$, so sind alle $\lambda_x > 0$ und $\mathrm{Spur}(TF_1) = \mathrm{Spur}(TF_2)$ ist dann gleichbedeutend mit $xF_2x^{tr} = m$ für alle $x \in S(F_1)$ also $S(F_1) \subset S(F_2)$ und damit gilt dies auch für die von diesen Mengen aufgespannten Kegel, $\mathcal{V}(F_1) \subset \mathcal{V}(F_2)$.
(b) Ist F_1 in (a) zusätzlich perfekt, so ist F_1 durch die Gleichungen $xF_1x^{tr} = m$ für alle $x \in S(F_1)$ eindeutig bestimmt. Da F_2 diese Gleichungen nach dem Beweis von (a) auch erfüllt, gilt damit $F_1 = F_2$. □

Satz 5.11 *Sei F perfekt, $m := \min(F)$, R ein Seitenvektor zur Seite $\mathcal{S}$ von $\mathcal{V}(F)$ und $S := \{x \in S(F) \mid x^{tr} x \in \mathcal{S}\}$. Für $t \in \mathbb{R}$ setzen wir*

$$F_t := F + tR \in \mathrm{Sym}_n(\mathbb{R}).$$

(a) Es gibt ein eindeutig bestimmtes $\rho > 0$ so daß für $0 < t < \rho$ die Form F_t nicht perfekt ist und $\min(F_t) = m$ und für $t > \rho$ die Form F_t entweder nicht positiv definit ist, oder $\min(F_t) < m$ ist.
(b) Für $0 < t < \rho$ ist $S(F_t) = S$.
(c) Für $t < 0$ ist F_t entweder nicht positiv definit, oder $\min(F_t) < m$.
(d) Die Form F_ρ ist perfekt mit $\min(F_\rho) = m$. $\mathcal{S} = \mathcal{V}(F) \cap \mathcal{V}(F_\rho)$ und F und F_ρ sind die einzigen perfekten Formen, deren Voronoi-Bereich $\mathcal{S}$ enthält.

Wir haben also

$t < 0$: F_t nicht positiv definit oder $\min(F_t) < m$.

$t = 0$: $F_t = F$.

$0 < t < \rho$: $\min(F_t) = m$, $S(F_t) = S$ und F_t nicht perfekt.

$t = \rho$: $\min(F_\rho) = m$, $S(F_\rho) \cap S(F) = S$, F_ρ perfekt und $\mathcal{V}(F) \cap \mathcal{V}(F_\rho) = \mathcal{S}$.

$t > \rho$: F_t nicht positiv definit oder $\min(F_t) < m$.

Ende am 15.5.07

Beweis. (c) Ist $y \in S(F) - S$, dann ist $yRy^{tr} > 0$ und somit $yF_ty^{tr} = m + t(yRy^{tr}) < m$ für $t < 0$.
Nach Satz 5.9 gibt es ein $y \in \mathbb{Z}^n$ mit $yRy^{tr} < 0$. Also ist für großes t die Form F_t indefinit. Sei $T := \{t > 0 \mid \min(F_t) < m$ oder F_t nicht positiv definit $\}$. und $\rho := \inf(T)$ die größte untere Schranke von T.
Dann ist $\rho > 0$.
Zu (a) und (b): Sei $0 < t < \rho$. Nach Definition ist dann $\min(F_t) = m$. Es ist sicherlich $S \subset S(F_t)$ da $yRy^{tr} = 0$ für $y \in S$ und $S(F_t) \cap S(F) = S$. Sei $y \in S(F_t) - S$. Dann ist $yFy^{tr} > m$ und daher $yRy^{tr} = \frac{1}{t}(yF_ty^{tr} - yFy^{tr}) = m/t - yFy^{tr}/t < 0$. Ist nun $\epsilon > 0$ so ist $yF_{t+\epsilon}y^{tr} < m$ und daher $t + \epsilon \in T$. Dies ist ein Widerspruch zu $t < \rho = \inf(T)$.
Zu (d): Da $\min(F_t) < \min(F)$ ist für alle $t > \rho$ gibt es ein $y \in S(F_\rho)$ mit $yRy^{tr} < 0$. Da Projektionen entlang den Vektoren in $S \subset S(F_\rho)$ die Hyperebene $\langle \mathcal{S} \rangle$ in $\mathrm{Sym}_n(\mathbb{R})$ erzeugen, die senkrecht zu R steht, gilt somit $\langle p_x \mid x \in \{y\} \cup S \rangle = \mathrm{Sym}_n(\mathbb{R})$ und daher ist F_ρ perfekt. Ist F' eine dritte perfekte Form, mit $S \subset S(F')$. Da $\mathcal{V}(F_\rho)$ und $\mathcal{V}(F)$ sich genau in der gemeinsamen Seite $\mathcal{S}$ schneiden und $\mathcal{V}(F') \supset \mathcal{S}$ eine echte Obermenge von $\mathcal{S}$ ist, gibt es einen gemeinsamen inneren Punkt von $\mathcal{V}(F')$ und einem der beiden Vornoi-Bereiche $\mathcal{V}(F)$ oder $\mathcal{V}(F_\rho)$. Mit Satz 5.10 folgt dann $F' = F$ oder $F' = F_\rho$. □

Definition 5.12 *Die Form F_ρ aus Satz 5.11 heißt* direkter perfekter Nachbar *von F zur Seite $\mathcal{S}$.*

Bemerkung 5.13 *Ist $m := \min(F) \in \mathbb{Q}$, so ist die perfekte Form F rational. Wählt man auch noch den Seitenvektor $R \in \mathbb{Q}^{n \times n}$, so ist ρ aus Satz 5.11 eine rationale Zahl.*

Beispiel 5.14 *Der Voronoi-Bereich von $\mathbb{A}_2$. Es ist $A_2 := \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$ und $S(A_2)/\{\pm 1\} = \{(1,0),(0,1),(1,1)\}$. Da $|S(A_2)/\{\pm 1\}| = \dim(\mathrm{Sym}_2(\mathbb{R})) = 3$ ist, ist $\mathcal{V}(A_2) \cap H$ ein Simplex, also hier ein Dreieck, wobei $H = \{X \in \mathrm{Sym}_2(\mathbb{R}) \mid \mathrm{Spur}(X) = 1\}$ bezeichne. Die Ecken des Dreiecks sind $\mathcal{E} := \{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\}$ die Seitenvektoren sind*

$$R_1 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, R_2 := \begin{pmatrix} 2 & -1 \\ -1 & 0 \end{pmatrix}, R_3 := \begin{pmatrix} 0 & -1 \\ -1 & 2 \end{pmatrix}.$$

Die zugehörigen direkten Nachbarn sind $A_2 + 2R_1 = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$, $A_2 + 2R_2 = \begin{pmatrix} 6 & -3 \\ -3 & 2 \end{pmatrix}$, $A_2 + 2R_3 = \begin{pmatrix} 2 & -3 \\ -3 & 6 \end{pmatrix}$ und alle isometrisch zu A_2.

Übung: Bestimmen Sie die direkten Nachbarn von $\mathbb{A}_3$.

Ebenso wie den Hauptsatz 5.11 sieht man

Bemerkung 5.15 *Sei F eine nicht-perfekte positiv definite symmetrische Matrix mit $m := \min(F)$ und sei $R \in \mathcal{V}(F)^\perp$. Setzt man $F_t := F + tR$, so gibt es genau ein $\rho > 0$ so daß F_t*

Minimum m hat für $0 \leq t \leq \rho$ und nicht positiv definit oder von kleinerem Minimum ist für $t > \rho$. Weiter ist $\dim(\mathcal{V}(F_\rho)) > \dim(\mathcal{V}(F))$.

Beweis. Als Übung. □

Beispiel: Sie $F = I_2$. Dann ist $\mathcal{V}(F) = \{\text{diag}(\lambda_1, \lambda_2) \mid \lambda_i \geq 0\}$ mit Ecken $\text{diag}(1,0)$ und $\text{diag}(0,1)$ und $\mathcal{V}(F)^\perp = \langle R := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle$. Dann ist $F + \frac{1}{2}R$ perfekt.

Diese Bemerkung erlaubt es, zu einer gegebenen Form eine perfekte Form zu finden. Mit Satz 5.11 kann man dann alle direkten Nachbarn dieser perfekten Form bestimmen.

Übung: Wenden Sie diesen Algorithmus auf $F = I_3$ an.

Definition 5.16 *Der* Voronoi Graph *ist ein Graph, dessen Ecken genau die endlich vielen Ähnlichkeitsklassen perfekter Formen der Dimension n sind. Zwei Ecken sind durch eine Kante verbunden, genau dann, wenn geeignete Vertreter direkte Nachbarn sind.*

Satz 5.17 *Der Voronoi-Graph ist ein endlicher zusammenhängender Graph.*

Beweis. Die Endlichkeit haben wir schon in Satz 4.14 gesehen. Es genügt daher zu zeigen, dass es für je zwei perfekte Formen F und F' mit gleichem Minimum m eine Kette $F = F_0, F_1, \ldots, F_s = F'$ perfekter Formen mit Minimum m gibt, so dass F_{i-1} und F_i direkte Nachbarn sind ($1 \leq i \leq s$). Dazu wählen wir uns einen inneren Punkt $Q' \in \mathcal{V}(F')$. Ist $Q' \in \mathcal{V}(F)$ so ist $F = F'$ nach Satz 5.10. Ansonsten gibt es einen Seitenvektor R von F, so daß $\text{Spur}(RQ') < 0$. Sei $F_1 := F + \rho R$ die zu F über den Seitenvektor R direkt benachbarte Form. Dann ist $\text{Spur}(F_1Q') < \text{Spur}(FQ')$. Ist $Q' \in \mathcal{V}(F_1)$, so ist $F_1 = F'$ nach Satz 5.10. Ansonsten können wir $\text{Spur}(F_iQ')$ immer weiter verkleinern. Dies ist ein endlicher Prozess nach dem folgenden Satz. □

Satz 5.18 *Sei Q' eine positiv definite Form und seien $K, m > 0$. Dann ist*

$$\{F \in \text{Sym}_n^{>0}(\mathbb{R}) \mid \min(F) = m, F \text{ ist perfekt und } \text{Spur}(FQ') < K\}$$

endlich.

Beweis. Zum Beweis benutzen wir das folgende leichte Lemma

Lemma 5.19 *Seien Q, Q' zwei positiv definite symmetrische Matrizen.*
$\mu := \min\{xQx^{tr} \mid x \in \mathbb{R}^n, xx^{tr} = 1\}$.
Sind $\lambda_1, \ldots, \lambda_n$ die Eigenwerte von Q', so ist

$$0 < \lambda_i \leq \sum_{i=1}^{n} \lambda_i \leq \frac{1}{\mu} \text{Spur}(QQ')$$

Beweis. Sei $(b_1, \ldots, b_n)$ eine ON-Basis aus Eigenvektoren von Q'. Ist M die Matrix von Q bezüglich dieser Basis, so ist

$$\mathrm{Spur}(QQ') = \mathrm{Spur}(\mathrm{diag}(\lambda_1, \ldots, \lambda_n)M) = \sum_{i=1}^{n} \lambda_i M_{ii} \geq \mu \sum_{i=1}^{n} \lambda_i.$$

□

Ende am 18.5.2007

Bezeichne nun μ das Minimum von Q' auf der Einheitssphäre und sei F wie in Satz 5.18 mit Eigenwerten $\lambda_1, \ldots, \lambda_n$ und $m = \min(F)$. Nach der Hermite Ungleichung gilt dann

$$\prod_{i=1}^{n} \lambda_i = \det(F) \geq \frac{m^n}{\gamma_n^n}.$$

Wegen Lemma 5.19 gilt außerdem

$$0 \leq \lambda_i \leq \frac{K}{\mu} \text{ für alle } 1 \leq i \leq n.$$

Also gibt es ein $a > 0$ (z.B. $a = \frac{m^n}{\gamma_n^n} \frac{\mu^{n-1}}{K^{n-1}}$) mit $\lambda_i > a$ für alle i. In einer ON-Basis $B := (b_1, \ldots, b_n)$ aus Eigenvektoren von F gilt dann für einen Vektor $x = \sum_{i=1}^{n} y_i b_i \in S(F)$, daß

$$m = xFx^{tr} = \sum_{i=1}^{n} \lambda_i y_i^2 \geq a \sum_{i=1}^{n} y_i^2.$$

Dies beschränkt die Beträge der Komponenten von $x \in \mathbb{Z}^n$ in der festen Basis B. Also ist x in der endlichen Menge

$$\{x \in \mathbb{Z}^n \mid x_B x_B^{tr} \leq \frac{m}{a}\}.$$

Diese Menge hat nur endlich viele Teilmengen, also gibt es nur endlich viele Möglichkeiten für $S(F)$ und damit für die perfekte Form F nach Satz 4.10. □

Bemerkung 5.20 *Sei F perfekt, R ein Seitenvektor von $\mathcal{V}(F)$ zur Seite $\mathcal{S}$ und $g \in \mathrm{Aut}(F)$. Dann ist auch gRg^{tr} ein Seitenvektor von $\mathcal{V}(F)$. Ist $F_1 = F + \rho R$ ein direkter perfekter Nachbar zur Seite $\mathcal{S}$, so ist auch $F_2 := gF_1g^{tr} = F + \rho gRg^{tr}$ ein direkter perfekter Nachbar von F. F_1 und F_2 sind isometrisch also genügt es bei der Bestimmung des Voronoi-Graphen Vertreter der Bahnen von $Aut(F)$ auf den Seiten von $\mathcal{V}(F)$ zu betrachten.*

Satz 5.21 *Die direkten perfekten Nachbarn von $\mathbb{A}_n$ sind alle isometrisch zu $\mathbb{A}_n$ falls $n \leq 3$ ist und zu $\mathbb{D}_n$ falls $n \geq 4$ ist.*

Beweis. Nach Lemma 2.19 operiert die Weyl Gryppe $W(\mathbb{A}_n) \leq \mathrm{Aut}(\mathbb{A}_n)$ transitiv auf der Menge der Wurzeln $S(\mathbb{A}_n)$. Schneidet man den Voronoi-Bereich $\mathcal{V}(\mathbb{A}_n)$ mit der Hyperebene $H := \{X \in \mathrm{Sym}_n(\mathbb{R}) \mid \mathrm{Spur}(X) = 1\}$, so erhält man einen konvexen Polyeder der Dimension $n(n+1)/2-1$ mit genau $|S(\mathbb{A}_n)|/2 = n(n+1)/2$ Ecken. Dieser ist daher ein Simplex, dessen

Seiten genau $n(n+1)/2-1$ Ecken enthalten. ($\mathcal{V}(\mathbb{A}_n)$ ist ein sogennanter simplizialer Kegel.) Insbesondere operiert $W(\mathbb{A}_n)$ auch transitiv auf den Seiten von $\mathcal{V}(\mathbb{A}_n)$. Nach Bemerkung 5.20 sind daher alle direkten Nachbarn von $\mathbb{A}_n$ isometrisch. Es genügt also einen direkten Nachbarn von $\mathbb{A}_n$ zu bestimmen. Dazu rechnen wir wieder mit der Grammatrix $A_n := I_n + J_n$ von $\mathbb{A}_n$ aus Beispiel 4.18. In dieser Basis ist $S(A_n) = \{\pm e_i, \pm(e_j - e_k) \mid 1 \leq i \leq n, 1 \leq j < k \leq n\}$. Sei $T_i := e_i^{tr} e_i = \mathrm{diag}(0, \ldots, 0, 1, 0, \ldots, 0)$ und $T_{jk} := (e_j - e_k)^{tr}(e_j - e_k)$. Dann ist $(T_{jk})_{xy} = 0$ falls $\{x, y\} \not\subset \{j, k\}$, $(T_{jk})_{jj} = (T_{jk})_{kk} = 1$ und $(T_{jk})_{jk} = (T_{jk})_{kj} = -1$. Sei $\mathcal{S}$ die Seite die alle Ecken von $\mathcal{V}(\mathbb{A}_n)$ bis auf T_{12} enthält. Dann ist

$$R := \begin{pmatrix} 0 & -1 & 0 & \ldots & 0 \\ -1 & 0 & 0 & \ldots & 0 \\ 0 & \ldots & \ldots & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & \ldots & \ldots & 0 \end{pmatrix}$$

ein Seitenvektor zu dieser Seite und $A_n + R =: D_n$ ist eine Grammatrix des perfekten Gitters

$$\mathbb{D}_n = \langle e_1 + e_2, e_1 - e_2, e_1 - e_3, \ldots, e_1 - e_n \rangle$$

(falls $n \geq 4$) bzw. von A_3 für $n = 3$. Also ist dies der direkte Nachbar von $\mathbb{A}_n$ zur Seite $\mathcal{S}$. Ist $n = 2$, so ist $A_n + R$ nicht perfekt, hat aber noch Minimum 2. Der direkte Nachbar für $n = 2$ ist dann $A_n + 2R = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$ und isometrisch zu $\mathbb{A}_2$. □

Folgerung 5.22 $\mathrm{Perf}_2 = \{[\mathbb{A}_2]\}$ *und* $\mathrm{Perf}_3 = \{[\mathbb{A}_3]\}$.

Beispiel Die Voronoi-Graphen in Dimension 2,3,4,5.

Satz 5.23 $\mathrm{Aut}(\mathbb{D}_4)$ *hat 2 Bahnen auf den Seitenvektoren von* $\mathcal{V}(\mathbb{D}_4)$. *Die entsprechenden direkten perfekten Nachbarn sind isometrisch zu* $\mathbb{D}_4$ *bzw.* $\mathbb{A}_4$.

Beweis. Wir rechnen bezüglich einer Basis von $\mathbb{Z}^4$ und benutzen die Beschreibung

$$\mathbb{D}_4 = \{(x_1, x_2, x_3, x_4) = \sum x_i e_i \in \mathbb{Z}^4 \mid \sum x_i \in 2\mathbb{Z}\}.$$

Dann ist $S(\mathbb{D}_4) = \{\pm e_i \pm e_j \mid 1 \leq i < j \leq 4\}$ und $|S(\mathbb{D}_4)|/2 = 12$. Weiter ist $\dim(\mathrm{Sym}_4(\mathbb{R})) = 10$. In jeder Seite von $\mathcal{V}(\mathbb{D}_4)$ liegen also mindestens 9 Ecken. Wir bestimmen also die Bahnen von $\mathrm{Aut}(\mathbb{D}_4)$ auf den 1, 2, und 3-elementigen Teilmengen von $S(\mathbb{D}_4)/\pm 1$. $\mathrm{Aut}(\mathbb{D}_4)$ ist transitiv auf $S(\mathbb{D}_4)$. Der Stabilisator von $\{\pm(e_1 + e_2)\}$ hat 3 Bahnen auf $S(\mathbb{D}_4)/\pm 1$ gemäss der 3 möglichen Skalarprodukte 0, ± 1, ± 2. Durch explizites Nachrechnen sieht man die folgenden 3 Behauptungen.
Behauptung1: Vertreter dieser Bahnen sind $\{\pm(e_1 - e_2)\}$, $\{\pm(e_1 + e_3)\}$, $\{\pm(e_1 + e_2)\}$
Behauptung2: $\langle x^{tr} x \mid x \in S(\mathbb{D}_4) - \{\pm(e_1 + e_3), \pm(e_1 + e_2)\}\rangle = \mathrm{Sym}_4(\mathbb{R})$.
Behauptung3: $H := \langle x^{tr} x \mid x \in S(\mathbb{D}_4) - \{\pm(e_1 - e_2), \pm(e_1 + e_2)\}\rangle$ ist eine Hyperebene in $\mathrm{Sym}_4(\mathbb{R})$, welche jedoch keine Seite von $\mathcal{V}(\mathbb{D}_4)$ ist.

Dass H eine Hyperebene ist, rechnet man wieder leicht nach. $H^\perp = \langle R := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rangle$.
Die beiden Skalarprodukte $\mathrm{Spur}(R(e_1 - e_2)^{tr}(e_1 - e_2))$ und $\mathrm{Spur}(R(e_1 + e_2)^{tr}(e_1 + e_2))$ haben unterschiedliches Vorzeichen, also ist H keine Seite von $\mathcal{V}(\mathbb{D}_4)$.
Also gibt es keine 10 Ecken von $\mathcal{V}(\mathbb{D}_4)$ die in einer Seite von $\mathcal{V}(\mathbb{D}_4)$ liegen und somit enthält jede Seite $\mathcal{S}$ von $\mathcal{V}(\mathbb{D}_4)$ genau 9 Ecken. Die drei Paare $\pm x_i \in S(\mathbb{D}_4)$ mit $x_i^{tr} x_i \notin \mathcal{S}$ erfüllen nach Behauptung 3 ausserdem $(x_i, x_j) \neq 0$. Es bleibt also mit Behauptung 1 die Fälle $x_1 = e_1 + e_2$, $x_2 = e_1 + e_3$ und $x_3 \in \{e_2 - e_3, e_2 + e_3, e_1 + e_4, e_1 - e_4\}$ zu betrachten. Die Matrix $\mathrm{diag}(1, 1, 1, -1) \in \mathrm{Aut}(\mathbb{D}_4)$ fixiert x_1 und x_2 und bildet $e_1 + e_4$ auf $e_1 - e_4$ ab. Die Spiegelung σ_v entlang des Vektors $v = \frac{1}{2}(e_1 - e_2 - e_3 + e_4)$ ist ein Automorphismus von $\mathbb{D}_4$, da $2v \in \mathbb{D}_4$, $(v, v) = 1$ und $v \in \mathbb{D}_4^{\#}$. Es ist $\sigma_v(x_1) = x_1$ und $\sigma_v(x_2) = x_2$, da $x_i \in v^\perp$ und $\sigma_v(e_2 + e_3) = e_1 + e_4$. Also genügt es, die beiden Fälle $x_3 = e_2 - e_3$ und $x_3 = e_2 + e_3$ zu betrachten. Da die Gitter $\langle x_1, x_2, x_3 \rangle \cong A_2$ bzw. A_3 unterschiedlich sind, haben wir gezeigt, dass die Automorphismengruppe $\mathrm{Aut}(\mathbb{D}_4)$ genau 2 Bahnen auf den Seiten von $\mathcal{V}(\mathbb{D}_4)$ hat. Die entsprechenden Seitenvektoren ergeben sich als

$$R = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & -1 & 0 \\ 1 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \text{ bzw. } R' = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

mit zugehörigen perfekten Nachbarn $F = T(I_4 + \frac{1}{2}R)T^{tr} \cong D_4$ bzw. $F' = T(I_4 + \frac{1}{2}R')T^{tr} \cong A_4$
wo $T = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}$. □

Folgerung 5.24 $\mathrm{Perf}_4 = \{[\mathbb{A}_4], [\mathbb{D}_4]\}$.

Übung: Bestimmen Sie die perfekten direkten Nachbarn von $\mathbb{D}_5$.

Bemerkung 5.25 *Der Voronoi-Bereich $\mathcal{V}(\mathbb{E}_8)$ hat 25075566937584 Seiten die in 83092 Bahnen unter* $\mathrm{Aut}(\mathbb{E}_8)$ *fallen. Alle bis auf 2 perfekte Formen in Dimension 8 sind direkte Nachbarn von $\mathbb{E}_8$.*

6 Stark perfekte Gitter und sphärische Designs.

In diesem Abschnitt möchte ich in die Theorie von Boris Venkov einführen, die es erlaubt sphärische Designs zu benutzen, um extreme Gitter in hohen Dimensionen zu konstruieren. Venkov nennt ein Gitter L stark perfekt, falls $S(L)$ ein sphärisches 4-Design (siehe Definition 6.20) bilden. Wir werden sehen, dass stark perfekte Gitter perfekt und eutaktisch und daher extrem sind. Die stark perfekten Gitter sind bis zur Dimension 12 alle mit Hilfe von kombinatorischen Methoden klassifiziert.

6.1 Harmonische Polynome und die orthogonale Gruppe.

Definition 6.1 $\mathbb{R}[X] := \mathbb{R}[X_1, \ldots, X_n]$ *bezeichne den* Polynomring *in n Unbestimmten. Für einen Multiindex $i = (i_1, \ldots, i_n)$ definieren wir das Monom $X^i := X_1^{i_1} \ldots X_n^{i_n}$ vom Grad $|i| := \sum_{j=1}^n i_j$ sowie den* Multinomialkoeffizient

$$\binom{|i|}{i} := \frac{|i|!}{i_1! \cdots i_n!}.$$

Weiter bezeichne $\mathcal{F}_{n,m} := \mathcal{F}_m$ den Raum aller Polynome in $\mathbb{R}[X_1, \ldots, X_n]$ vom Grad m. Ist $T_m := \{i = (i_1, \ldots, i_n) \mid |i| = m\}$ so bilden die Monome X^i mit $i \in T_m$ eine $\mathbb{R}$-Basis von $\mathcal{F}_{n,m}$. Für $f := \sum_{i \in T_m} a_i X^i$ und $g := \sum_{i \in T_m} b_i X^i$ in $\mathcal{F}_{n,m}$ definieren wir das Skalarprodukt

$$[f, g] := \sum_{i \in T_m} \binom{|i|}{i}^{-1} a_i b_i.$$

Dies definiert ein euklidisches Skalarprodukt auf $\mathcal{F}_{n,m}$ für die die Monome X^i eine OG-Basis bilden mit $[X^i, X^i] = \binom{|i|}{i}^{-1}$.

Bemerkung 6.2 *Es gilt* $\dim(\mathcal{F}_{n,m}) = \binom{n+m-1}{n-1}$.

Beweis. Jeder Multiindex $i \in T_m$ lässt sich als Folge von m Punkten und $n-1$ Strichen kodieren. $i = (i_1, \ldots, i_n)$ entspricht dabei die Folge

$$\underbrace{\cdots}_{i_1}|\underbrace{\cdots}_{i_2}|\cdots\underbrace{\cdots}_{i_{n-1}}|\underbrace{\cdots}_{i_n}$$

Solche Folgen sind eindeutig durch die Positionen der Striche bestimmt, wobei man $\binom{n+m-1}{n-1}$ Möglichkeiten hat. □

Beispiel 6.3 *Sei $\omega := \sum_{j=1}^n X_j^2 \in \mathcal{F}_{n,2}$. Für $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^n$ setzen wir $\rho_\alpha := \sum_{j=1}^n \alpha_j X_j \in \mathcal{F}_{n,1}$. Dann sind $\omega^{m/2}$ und ρ_α^m in $\mathcal{F}_{n,m}$*

Bemerkung 6.4 *Die orthogonale Gruppe*

$$O_n(\mathbb{R}) := \{\sigma \in \mathbb{R}^{n \times n} \mid \sigma\sigma^{tr} = 1\}$$

, operiert durch Ringautomorphismen auf $\mathcal{F}_{n,m}$ vermöge $(\sigma, f) \mapsto \sigma f := f(X\sigma)$. Dann ist $\sigma\rho_\alpha = \rho_{\alpha\sigma}$ und $\sigma\omega = \omega$ für alle $\sigma \in O_n(\mathbb{R})$.

Beweis. Sei $\sigma := (\sigma_{ij}) \in O_n(\mathbb{R})$. Dann ist

$$(\sigma\rho_\alpha)(X) = \rho_\alpha(X\sigma) = \sum_{j=1}^{n} \alpha_j \sum_{i=1}^{n} \sigma_{ij} X_i = \sum_{i=1}^{n} (\sum_{j=1}^{n} \sigma_{ij}\alpha_j) X_i = \rho_{\alpha\sigma}(X).$$

Weiter ist

$$(\sigma\omega)(X) = \sum_{j=1}^{n} (\sum_{i=1}^{n} \sigma_{ij} X_i)^2 = \sum_{j=1}^{n} \sum_{k=1}^{n} \sum_{i=1}^{n} \sigma_{ij}\sigma_{kj} X_i X_k = \sum_{i=1}^{n} X_i^2 = \omega(X)$$

da $\sum_{k=1}^{n} \sum_{i=1}^{n} \sigma_{ij}\sigma_{kj} = (\sigma\sigma^{tr})_{i,k} = \delta_{ik}$. □

Lemma 6.5 *Für $f \in \mathcal{F}_{n,m}$ und $\alpha \in \mathbb{R}^n$ gilt*

$$[f, \rho_\alpha^m] = f(\alpha).$$

Beweis. $\rho_\alpha^m = (\alpha_1 X_1 + \ldots + \alpha_n X_n)^m = \sum_{i \in T_m} \binom{m}{i} \alpha_1^{i_1} \cdots \alpha_n^{i_n} X^i \sum_{i \in T_m} \binom{m}{i} \alpha^i X^i$. Ist $f = \sum_{i \in T_m} b_i X^i$, so ist $[f, \rho_\alpha^m] = \sum_{i \in T_m} b_i \alpha^i = f(\alpha)$. □

Folgerung 6.6 $\mathcal{F}_{n,m} = \langle \rho_\alpha^m \mid \alpha \in \mathbb{R}^n \rangle$

Beweis. Sei $U := \langle \rho_\alpha^m \mid \alpha \in \mathbb{R}^n \rangle$. Dann ist $U \leq \mathcal{F}_{n,m}$ und es genügt zu zeigen, dass $U^\perp = \{0\}$ ist. Ist aber $f \in U^\perp \subset \mathcal{F}_{n,m}$, so gilt für alle $\alpha \in \mathbb{R}^n$, dass $0 = [f, \rho_\alpha^m] = f(\alpha)$. Also ist $f = 0$. □

Bemerkung 6.7 *Sei $\nabla := (\frac{\partial}{\partial X_1}, \ldots, \frac{\partial}{\partial X_n})$. Es gilt dann für $f, g \in \mathcal{F}_{n,m}$ dass*

$$m![f, g] = f(\nabla)g.$$

Beweis. Die Abbildung $(a, b) \mapsto a(\nabla)b$ ist bilinear auf $\mathcal{F}_{n,m} \times \mathcal{F}_{n,m}$ also genügt es die Gleichheit für Monome nachzurechnen. Sind $i, j \in T_m$, so ist $X^i(\nabla)X^j = 0$ falls $i \neq j$ und ansonsten ergibt sich $i_1! \cdots i_n!$. □

Definition 6.8 *Der Operator*

$$\Delta := \omega(\nabla) = \sum_{i=1}^{n} \frac{\partial^2}{\partial X_i^2}$$

heißt der Laplace-Operator *. Dies ist eine Abbildung von $\mathcal{F}_{n,m}$ nach $\mathcal{F}_{n,m-2}$.*

$$\mathrm{Harm}_{n,m} := \ker(\Delta) := \{f \in \mathcal{F}_{n,m} \mid \Delta(f) = 0\}$$

heißt der Raum der harmonischen Polynome *vom Grad m in n Variablen.*

Beispiel 6.9 $\Delta(\rho_\alpha^m) = m(m-1)(\alpha,\alpha)\rho_\alpha^{m-2}$
$\Delta(\omega^\ell) = 2\ell(2\ell+n-2)\omega^{\ell-1}$
$\Delta(\omega^\ell\rho_\alpha^k) = 2\ell(2\ell+2k+n-2)\omega^{\ell-1}\rho_\alpha^k + k(k-1)(\alpha,\alpha)\omega^\ell\rho_\alpha^{k-2}$

Beispiel 6.10 *Für $\alpha \in \mathbb{R}^n$ sind*

$$P_\alpha^{(2)} := \rho_\alpha^2 - \frac{(\alpha,\alpha)}{n}\omega \in \mathrm{Harm}_{n,2}$$

und

$$P_\alpha^{(4)} := \rho_\alpha^4 - \frac{6(\alpha,\alpha)}{n+4}\rho_\alpha^2\omega + \frac{3(\alpha,\alpha)^2}{(n+2)(n+4)}\omega^2 \in \mathrm{Harm}_{n,4}\,.$$

Bemerkung 6.11 *Der Laplace-Operator ist ein $O_n(\mathbb{R})$-invarianter Differentialoperator. D.h. es gilt für $f \in \mathcal{F}_{n,m}$ und $g \in O_n(\mathbb{R})$, dass*

$$\Delta(gf) = g(\Delta f).$$

Beweis. Übung. □

Bemerkung 6.12 *Jedes durch ω teilbare harmonische Polynom ist gleich 0.*

Beweis. Sei $f \in \mathrm{Harm}_{n,m}$ und $g \in \mathcal{F}_{n,m-2}$ mit $f = \omega g$. Dann ist

$$[f,f] = [g\omega, f] = g(\nabla)\omega(\nabla)f = g(\nabla)\Delta f = 0$$

da f harmonisch ist. Also ist $f = 0$, da das Skalarprodukt positiv definit ist. □

Satz 6.13 *$\Delta : \mathcal{F}_{n,m} \to \mathcal{F}_{n,m-2}$ ist surjektiv.*

Beweis. Sei $g \in \mathcal{F}_{n,m-2}$ im orthogonalen Komplement von Bild(Δ). Dann ist $\omega g \in \mathcal{F}_{n,m}$ und für $f \in \mathcal{F}_{n,m}$ gilt

$$m![\omega g, f] = (g\omega)(\nabla)f = g(\nabla)\omega(\nabla)f = g(\nabla)\Delta(f) = (m-2)![g, \Delta f] = 0.$$

Also ist $\omega g \in \mathcal{F}_{n,m}^\perp = \{0\}$ und damit $g = 0$. □

Satz 6.14

$$\mathcal{F}_{n,m} = \mathrm{Harm}_{n,m} \perp \omega\,\mathrm{Harm}_{n,m-2} \perp \omega^2\,\mathrm{Harm}_{n,m-4} \perp \ldots \perp \omega^{\lfloor m/2\rfloor}\,\mathrm{Harm}_{n,m-2\lfloor m/2\rfloor}$$

ist eine Zerlegung von $\mathcal{F}_{n,m}$ in irreduzible $O(n)$-invariante Teilmoduln.

Beweis. Da $\Delta : \mathcal{F}_{n,m} \to \mathcal{F}_{n,m-2}$ surjektiv ist, ist $\mathcal{F}_{n,m} = \mathrm{Harm}_{n,m} \perp \omega\mathcal{F}_{n,m-2}$, da jedes durch ω teilbare Polynom in $\mathcal{F}_{n,m}$ senkrecht auf allen harmonischen Polynomen steht (siehe oben) oder auch wegen $O_n(\mathbb{R})$-Invarianz des Skalarprodukts $[-,=]$, die Sie in den Übungen zeigen. Die Zerlegung in $O(n)$-invariante Teilmoduln erhält man nun durch Induktion. Die Irreduzibilität von $\mathrm{Harm}_{n,m}$ beweisen wir im Rest dieses Abschnitts. Daraus ergibt sich, dass die O_n-Teilmoduln $V_j := \omega^j \mathrm{Harm}_{n,m-2j} \leq \mathcal{F}_{n,m}$ für $j = 0, \ldots, \lfloor m/2 \rfloor$ paarweise senkrecht aufeinander stehen. Denn ist $f \in V_j$ mit $[f,g] \neq 0$ für ein $g \in V_k$ so ist die Abbildung $\alpha_f : h \mapsto [f,h]$ eine Abbildung $\neq 0$ in $V_k^* = \mathrm{Hom}_{\mathbb{R}}(V_k, \mathbb{R})$ und die Abbildung $\alpha : V_j \to V_k^*, g \mapsto \alpha_g$ ist ein O_n-Homomorphismus $\neq 0$. Da sowohl V_j als auch V_k^* irreduzible O_n-Moduln sind, ist α also ein Isomorphismus, was aus Dimensionsgründen unmöglich ist. □

Bemerkung: Die Orthogonalität der Zerlegung läßt sich auch elementar nachrechnen. Sind $f \in \mathrm{Harm}_{m-2k}, g \in \mathrm{Harm}_{m-2l}$ harmonisch so ist

$$[\omega^k f, \omega^l g] = c\delta_{k,l}[f,g]$$

für eine von n, k und m abhängige Konstante c. Es gilt nämlich

$$\begin{aligned}
\Delta(\omega^k f) &= \omega\Delta(\omega^{k-1}f) + \Delta(\omega)(\omega^{k-1}f) + \textstyle\sum_{i=1}^n \frac{\partial\omega}{\partial X_i}\frac{\partial\omega^{k-1}f}{\partial X_i} \\
&= \omega\Delta(\omega^{k-1}f) + (2n + 2(m-2))\omega^{k-1}f \\
&= \omega^2\Delta(\omega^{k-2}f) + (2n + 2(m-2) + 2(m-4))\omega^{k-1}f \\
&= \omega^k\Delta(f) + (2n + 2(m-2) + 2(m-4) + \ldots)\omega^{k-1}f \\
&= const.\omega^{k-1}f
\end{aligned}$$

da $\Delta(f) = 0$. Induktiv ergibt sich damit $\Delta^k(\omega^k f) = c(n,m,k)f$ und daher für $l \geq k$:

$$[\omega^l g, \omega^k f] = g(\nabla)\Delta^{l-k}(\Delta^k(\omega^k f)) = c(n,m,k)[\omega^{l-k}g, f] = \begin{cases} 0 & l \neq k \\ c(n,m,k)[g,f] & l = k \end{cases}.$$

Ende am 25.5.

Bemerkung 6.15 *Sei $\mathcal{M} := \{ f : S^{n-1} \to \mathbb{R} \mid f \text{ stetig} \}$ der Raum aller stetigen reellen Funktionen auf der Sphäre. Da S^{n-1} kompakt ist, ist jedes $f \in \mathcal{M}$ integrierbar und*

$$(f,g) := \int_{S^{n-1}} f(x)g(x)dx$$

definiert ein $O_n(\mathbb{R})$-invariantes Skalarprodukt auf $\mathcal{M}$. Sei V ein $O_n(\mathbb{R})$-invarianter Teilraum von $\mathcal{M}$ endlicher Dimension $N = \dim(V)$ und $(f_1, \ldots, f_N)$ eine ON-Basis von V. Definieren

$$\alpha_V : S^{n-1} \times S^{n-1} \to \mathbb{R}, \alpha_V(x_1,x_2) := \sum_{i=1}^N f_i(x_1)f_i(x_2).$$

Dann hängt α_V nicht von der Wahl der ON-Basis ab und $\alpha_V(x_1,x_2)$ hängt nur von dem inneren Produkt (x_1,x_2) ab, d.h. $\alpha_V(x_1,x_2) = \alpha_V(y_1,y_2)$ falls $(x_1,x_2) = (y_1,y_2)$.

Beweis. Für $\sigma \in O_n(\mathbb{R})$ und $f,g \in \mathcal{M}$ ist

$$(\sigma f, \sigma g) := \int_{S^{n-1}} (fg)(x\sigma)dx = \det(\sigma) \int_{S^{n-1}\sigma} (fg)(x)dx = (f,g).$$

Sei $(g_1, \ldots, g_N)$ eine weitere ON-Basis von V und $g_i = \sum_{j=1}^N \alpha_{ij} f_j$. Da beides ON-Basen sind, ist die Basiswechselmatrix (α_{ij}) orthogonal, d.h. $\sum_{i=1}^N \alpha_{ji}\alpha_{ki} = \delta_{jk}$. Also gilt

$$\sum_{i=1}^N g_i(x_1)g_i(x_2) = \sum_{i=1}^N \sum_{j=1}^N \alpha_{ij} \sum_{k=1}^N \alpha_{ik} f_j(x_1) f_k(x_2) = \sum_{i=1}^N f_i(x_1) f_i(x_2).$$

Seien jetzt $x_1, x_2, y_1, y_2 \in S^{n-1}$ mit $(x_1, x_2) = (y_1, y_2)$. Dann gibt es $\sigma \in O_n(\mathbb{R})$ so daß$x_1\sigma = y_1$ und $x_2\sigma = y_2$. Also ist

$$\alpha_V(y_1, y_2) = \alpha_V(x_1\sigma, x_2\sigma) = \sum_{i=1}^N f_i(x_1\sigma) f_i(x_2\sigma) == \sum_{i=1}^N (\sigma f_i)(x_1)(\sigma f_i)(x_2).$$

Nun ist mit $(f_1, \ldots, f_N)$ auch $(\sigma f_1, \ldots, \sigma f_N)$ eine ON-Basis von V und daher $\alpha_V(y_1, y_2) = \alpha_V(x_1, x_2)$. □

Definition 6.16 *Sei $e \in S^{n-1}$ fest gewählt. Eine* zonale sphärische Funktion *ist eine reelle Funktion $f : S^{n-1} \to \mathbb{R}$ mit $f(x) = f(y)$ für alle $x, y \in S^{n-1}$ für die $(x, e) = (y, e)$ gilt.*

Bemerkung 6.17 *Jeder endlich dimensionale $O_n(\mathbb{R})$-invariante Teilraum $0 \neq V \leq \mathcal{M}$ enthält eine zonale Funktion $f \neq 0$.*

Beweis. Sei α_V wie eben und definieren $\alpha : S^{n-1} \to \mathbb{R}$ als $\alpha(x) := \alpha_V(x, e) = \sum_{i=1}^N f_i(e) f_i(x)$. Dann ist $\alpha \in V$ eine zonale Funktion. Diese ist $\neq 0$, denn sonst ist $0 = \alpha(e) = \sum_{i=1}^N f_i(e)^2$ also $f_i(e) = 0$ für alle i. Da $(f_1, \ldots, f_N)$ eine Basis von V war gilt dann auch $f(e) = 0$ für alle $f \in V$. Für $x \in S^{n-1}$ gibt es jedoch ein $\sigma \in O_n(\mathbb{R})$ mit $e\sigma = x$. Damit ist auch $f(x) = (\sigma f)(e) = 0$ für beliebiges $f \in V$ und $x \in S^{n-1}$, also $V = 0$. □

Folgerung 6.18 *Ist V ein endlich dimensionaler $O_n(\mathbb{R})$-invarianter Teilraum von $\mathcal{M}$, so dass die zonalen Funktionen in V einen eindimensionalen Teilraum bilden, dann ist V irreduzibel, d.h. jeder $O_n(\mathbb{R})$ invariante Teilmodul $W \leq V$ ist entweder 0 oder V.*

Beweis. Sei $0 \neq W \neq V$ ein $O_n(\mathbb{R})$-invarianter Teilmodul von $V = W \perp W^\perp$. Dann ist auch $W^\perp$ O_n-invariant und die beiden zonalen Funktionen $x \mapsto \alpha_W(x, e)$ und $x \mapsto \alpha_{W^\perp}(x, e)$ sind linear unabhängig. □

Satz 6.19 $\mathrm{Harm}_{m,n}$ *ist ein irreduzibler $O_n(\mathbb{R})$-Modul.*

Beweis. Seien $f, g \in \mathrm{Harm}_{m,n}$ zonale Funktionen ungleich 0. Da harmonische Polynome nicht durch ω teilbar sind, können wir nach Multiplikation mit einer reellen Zahl annehmen dass

$$f(x) = (x, e)^m + \alpha_1\omega(x)(x, e)^{m-2} + \ldots$$
$$g(x) = (x, e)^m + \beta_1\omega(x)(x, e)^{m-2} + \ldots$$

Die Differenz $f - g$ ist dann ein harmonisches Polynom, das durch ω teilbar ist, also $f - g = 0$ und daher $f = g$. □

6.2 Sphärische Designs und stark perfekte Gitter

Sei $n \geq 2$.

Definition 6.20 *Sei $t \in \mathbb{N}$. Eine endliche nicht leere Teilmenge $\mathcal{X} \subset S^{n-1} = \{x \in \mathbb{R}^n \mid (x,x) = 1\}$ heißt* sphärisches t-Design, *falls für alle $m \leq t$ und $f \in \mathcal{F}_{n,m}$ gilt*

$$\star \quad \int_{S^{n-1}} f(x)dx = \frac{1}{|\mathcal{X}|} \sum_{x \in \mathcal{X}} f(x).$$

Bemerkung 6.21 *Für $\sigma \in O_n(\mathbb{R})$ und $f \in \mathcal{F}_{n,m}$ gilt*

$$\int_{S^{n-1}} f(x\sigma)dx = \int_{S^{n-1}} f(x)|\det(\sigma)|dx = \int_{S^{n-1}} f(x)dx.$$

Die symmetrische Bilinearform

$$(f,g) \mapsto \int_{S^{n-1}} f(x)g(x)dx$$

ist ein $O_n(\mathbb{R})$ invariantes Skalarprodukt auf $\mathcal{F}_{n,m}$.

Satz 6.22 *Äquivalent sind für eine endliche nicht-leere Teilmenge $\mathcal{X} \subset S^{n-1}$:*
(a) $\mathcal{X}$ ist ein sphärisches t-design.
(b) Für alle $m \leq t$ und alle Polynome $f \in \mathcal{F}_{n,m}$ ist

$$\sum_{x \in \mathcal{X}} f(x) = \sum_{x \in \mathcal{X}} (\sigma f)(x) \text{ für alle } \sigma \in O_n(\mathbb{R}).$$

(c) Für jedes $1 \leq m \leq t$ und jedes harmonische Polynom $f \in \mathrm{Harm}_{n,m}$ ist $\sum_{x \in \mathcal{X}} f(x) = 0$.
(d) Sei $\{g,u\} = \{t, t-1\}$ und u ungerade, g gerade. Dann gibt es eine Konstante c_g mit

$$\sum_{x \in \mathcal{X}} (x,\alpha)^g = c_g(\alpha,\alpha)^{g/2} \text{ und } \sum_{x \in \mathcal{X}} (x,\alpha)^u = 0 \text{ für alle } \alpha \in \mathbb{R}^n.$$

Beweis. (a) $\Rightarrow$ (b): aus der $O_n(\mathbb{R})$-Invarianz von $\int_{S^{n-1}} f(x)dx$
(b) $\Rightarrow$ (c): Die Abbildung $f \mapsto \sum_{x \in \mathcal{X}} f(x), \mathrm{Harm}_{n,m} \to \mathbb{R}$ ist eine $O_n(\mathbb{R})$-invariante Abbildung. Also ist ihr Kern $K := \{f \in \mathrm{Harm}_{n,m} \mid \sum_{x \in \mathcal{X}} f(x) = 0\}$ ein $O_n(\mathbb{R})$-invarianter Teilraum von $\mathrm{Harm}_{n,m}$. Wegen der Irreduzibilität von $\mathrm{Harm}_{n,m}$ ist also $K = 0$ oder $K = \mathrm{Harm}_{n,m}$. Im ersten Fall ist $\mathrm{Harm}_{n,m} \cong \mathbb{R}$ eindimensional, also $m = 0$. Im zweiten Fall gilt (c).
Ende am 4.6.07
(c) $\Rightarrow$ (d): Induktion über t:
Ist $u = 1$, so ist ρ_α harmonisch und nach Beispiel 6.10 ist $\rho_\alpha^2 - \frac{(\alpha,\alpha)}{n}\omega \in \mathrm{Harm}_{n,2}$ ebenfalls harmonisch. Also gilt die Behauptung für $t = 1$ und $t = 2$.

$t-2 \Rightarrow t$: Es ist $\rho_\alpha^i = h + \sum_{j=0, j\equiv_2 i}^{i-1} d_j(\alpha,\alpha)^{(i-j)/2}\rho_\alpha^j\omega^{(i-j)/2}$ für ein harmonisches Polynom h und $d_j \in \mathbb{R}$ (s. Beispiel 6.9, z.B. ist $d_{i-2} = i(i-1)/(2(i+n-2))$). Also ist

$$\sum_{x\in\mathcal{X}} \rho_\alpha^i(x) = \sum_{j=0, j\equiv_2 i}^{i-1} d_j(\alpha,\alpha)^{(i-j)/2} \sum_{x\in\mathcal{X}} \rho_\alpha^j(x) = \begin{cases} 0 & i \text{ ungerade} \\ const.(\alpha,\alpha)^{i/2} & i \text{ gerade} \end{cases}$$

nach Induktionsvoraussetzung.
(d) $\Rightarrow$ (a): Da die ρ_α^m den Raum $\mathcal{F}_{n,m}$ erzeugen, genügt es die Gleichung $\star$ für ρ_α^m mit $0 \le m \le t$ und $\alpha \in \mathbb{R}^n$ beliebig nachzurechnen. Nach Bemerkung 6.23 ist die Konstante aus (d) eindeutig festgelegt. Wendet man auf die Gleichungen in (d) den Laplace-Operator an, so erhält man analoge Gleichungen

$$\sum_{x\in\mathcal{X}} \rho_\alpha^m(x) = \begin{cases} 0 & m \text{ ungerade} \\ c_m(\alpha,\alpha)^{m/2} & m \text{ gerade.} \end{cases}$$

Es genügt also zu zeigen, dass für alle $m \le t$

$$\int_{S^{n-1}} \rho_\alpha^m(x)dx = \int_{S^{n-1}} (x,\alpha)^m dx = \begin{cases} 0 & m \text{ ungerade} \\ \frac{c_m}{|\mathcal{X}|}(\alpha,\alpha)^{m/2} & m \text{ gerade.} \end{cases}$$

Da der Laplace-Operator mit der Integration vertauscht, erhält man wieder die spezielle Gestalt der Konstanten auf der rechten Seite durch Anwenden des Laplace-Operators. Es genügt also zu zeigen, dass das Integral auf der linken Seite nur von der Länge von α abhängt, also unabhängig von der Wahl von $\alpha \in S^{n-1}$ ist. Dies ist aber klar, da die Gruppe $O_n(\mathbb{R})$ transitiv auf der Sphäre S^{n-1} operiert. □

Bemerkung 6.23 *Die Konstante c_g in Satz 6.22 (d) ist gegeben durch*

$$c_g = \frac{1\cdot 3\cdot 5\cdots(g-1)}{n(n+2)(n+4)\cdots(n+g-2)}|\mathcal{X}|.$$

Beweis. Wende den Laplace-Operator bezüglich α auf beide Seiten der Gleichung in 6.22 (d) $g/2$ mal an. □

Bemerkung 6.24 *Häufig wird $\mathcal{X}$ symmetrisch sein (z.B. $\mathcal{X} = S(L)$), das heisst mit $x \in \mathcal{X}$ ist auch $-x \in \mathcal{X}$. Dann ist die 2. Gleichung in Satz 6.22 (d) trivialerweise immer erfüllt.*

Ein Nachteil der Charakterisierung von Designs in Satz 6.22 (d) ist es, dass man diese Gleichheit für alle $\alpha \in \mathbb{R}^n$ nachrechnen muss. Zum Testen, ob eine gegebene Menge ein Design ist, gibt es folgendes einfachere Kriterium, was man direkt aus der positiven Definitheit des Skalarprodukts $[-,=]$ erhält.

Satz 6.25 *Sei $\mathcal{X} = -\mathcal{X} \subset S^{n-1}(a) := \{x \in \mathbb{R}^n \mid (x,x) = a\}$. Dann gilt*

$$\sum_{x,y\in\mathcal{X}} (x,y)^{2\ell} \ge \frac{1\cdot 3\cdot 5\cdots(2\ell-1)}{n(n+2)(n+4)\cdots(n+2\ell-2)} a^{2\ell}|\mathcal{X}|^2$$

für alle $\ell \in \mathbb{N}$ mit Gleichheit, genau dann wenn $\mathcal{X}$ ein sphärisches $(2\ell+1)$-design ist.

Beweis. Wie immer beweisen wir den Satz für $a = 1$, der allgemeine Fall folgt durch Reskalieren. Setze $c := \frac{1\cdot 3\cdot 5\cdots(2\ell-1)}{n(n+2)(n+4)\cdots(n+2\ell-2)}|\mathcal{X}|$ und betrachte das Polynom

$$p := \sum_{x\in\mathcal{X}} \rho_x^{2\ell} - c\omega^\ell.$$

Genau dann ist $\mathcal{X}$ ein $(2\ell+1)$-design, wenn $p = 0$ ist, also genau dann wenn $[p,p] = 0$ für das Skalarprodukt aus 6.1. Im allgemeinen ist $[p,p] \geq 0$, was die behauptete Ungleichung ergeben wird. Es ist nämlich

$$\begin{aligned}
&[p,p] = [\textstyle\sum_{x\in\mathcal{X}} \rho_x^{2\ell} - c\omega^\ell, \sum_{x\in\mathcal{X}} \rho_x^{2\ell} - c\omega^\ell] \\
&= \textstyle\sum_{x,y\in\mathcal{X}} [\rho_x^{2\ell}, \rho_y^{2\ell}] - 2c\sum_{x\in\mathcal{X}} [\rho_x^{2\ell}, \omega^\ell] + c^2[\omega^\ell, \omega^\ell] \\
&= \textstyle\sum_{x,y\in\mathcal{X}} (x,y)^{2\ell} - 2c\sum_{x\in\mathcal{X}} (x,x)^\ell + c^2[\omega^\ell, \omega^\ell]
\end{aligned}$$

Der letzte Term ergibt sich aus der Gleichheit $[\omega^\ell, \omega^\ell] = \frac{1}{(2\ell)!}\Delta^\ell(\omega^\ell)$ rekursiv, da $\Delta(\omega^\ell) = 2\ell(2\ell+n-2)\omega^{\ell-1}$ ist, als

$$\begin{aligned}
&\tfrac{1}{(2\ell)!}\Delta^\ell(\omega^\ell) = \tfrac{1}{(2\ell)!} 2\ell(2\ell-2)\cdots 2(2\ell+n-2)(2\ell+n-4)\cdots n = \\
&\tfrac{2^\ell \ell!}{(2\ell)!} n(n+2)\ldots(n+2\ell-2) = \tfrac{n(n+2)\ldots(n+2\ell-2)}{1\cdot 3\cdots(2\ell-1)} = c|\mathcal{X}|
\end{aligned}$$

Also ergibt sich insgesamt

$$0 \leq [p,p] = \sum_{x,y\in\mathcal{X}} (x,y)^{2\ell} - c|\mathcal{X}|.$$

□

Beispiel: $S(\mathbb{A}_2)$ ist ein 4-Design aber kein 6-Design.

Definition 6.26 *Ein Gitter L heißt* stark eutaktisch*, falls L eutaktisch ist und alle Eutaxiekoeffizienten λ_x mit $x \in S(L)$ gleich gewählt werden können.*

Beispiel 6.27 *Ist $G = \mathrm{Aut}(L)$ absolut irreduzibel, so ist L stark eutaktisch.*

Beweis. $G = \mathrm{Aut}(L) = \{g \in O_n(\mathbb{R}) \mid Lg = L\}$. Da $S(L)$ eine Vereinigung von G-Bahnen ist, erfüllt $F := \sum_{x\in S(L)} x^{tr}x$ die Gleichung $g^{tr}Fg = F$ für alle $g \in G$. Da G absolut irreduzibel ist, folgt daraus $F = \lambda I_n$ für ein $\lambda \in \mathbb{R}$. Als Summe von positiv semidefiniten Matrizen ist $F \neq 0$ positiv semidefinit, also ist $\lambda > 0$ und daher $I_n = \lambda^{-1}\sum_{x\in S(L)} x^{tr}x$. □

Beispiel 6.28 *Irreduzible Wurzelgitter sind stark eutaktisch.*

Satz 6.29 *Ein Gitter L ist stark eutaktisch, genau dann wenn $S(L)$ ein sphärisches 2-Design ist.*

Beweis. L ist stark eutaktisch, genau dann wenn es ein $\lambda > 0$ gibt, so dass

$$I_n = \lambda \sum_{x \in S(L)} x^{tr} x.$$

Dann ist aber für $\alpha \in \mathbb{R}^n$

$$\alpha I_n \alpha^{tr} = (\alpha, \alpha) = \lambda \sum_{x \in S(L)} \alpha x^{tr} x \alpha^{tr} = \lambda \sum_{x \in S(L)} (\alpha, x)^2$$

und die 1. Gleichung in Satz 6.22 (d) mit $g = 2$ und $c_2 = \frac{1}{\lambda}$ ist erfüllt. Da die 2. Gleichung in Satz 6.22 (d) mit $u = 1$ nach Bemerkung 6.24 trivialerweise erfüllt ist, ist somit $S(L)$ ein 2-Design (sogar ein 3-Design wegen Bemerkung 6.24). □

Definition 6.30 *Ein Gitter L heißt* stark perfekt*, falls $S(L)$ ein sphärisches 4-Design ist.*

Hauptsatz 6.31 *Stark perfekte Gitter sind perfekt und eutaktisch und daher lokale Maxima der Dichtefunktion.*

Beweis. Sei L ein stark perfektes Gitter. Œ sei $\min(L) = 1$. Dann ist L eutaktisch nach Satz 6.29. Es genügt also zu zeigen, dass L auch perfekt ist, d.h. dass $\langle x^{tr} x \mid x \in S(L) \rangle = \mathrm{Sym}_n(\mathbb{R})$. Sei dazu $A \in \mathrm{Sym}_n(\mathbb{R})$ mit $\mathrm{Spur}(Ax^{tr} x) = 0$ für alle $x \in S(L)$. Es ist

$$\mathrm{Spur}(Ax^{tr} x) = xAx^{tr} = p_A(x) = [p_A, \rho_x^2]$$

mit $p_A(X_1, \ldots, X_n) = \sum_{i,j} A_{ij} X_i X_j \in \mathcal{F}_{n,2}$. Dann ist $p_A^2 \in \mathcal{F}_{n,4}$. Da $S(L)$ ein 4-design ist, gilt

$$\int_{S^{(n-1)}} p_A^2(x) dx = \frac{1}{|S(L)|} \sum_{x \in S(L)} p_A(x)^2 = 0.$$

Da p_A als Polynom aber stetig ist und p_A^2 nichtnegativ, folgt daraus $p_A = 0$ also auch $A = 0$ was zu zeigen war. □

Ende am 8.6.07

Folgerung 6.32 *Die stark perfekten Gitter der Dimension ≤ 8 sind vertreten durch $\mathbb{Z}$, $\mathbb{A}_2$, $\mathbb{D}_4$, $\mathbb{E}_6$, $\mathbb{E}_6^{\#}$, $\mathbb{E}_7$, $\mathbb{E}_7^{\#}$ und $\mathbb{E}_8$.*

Beweis. Teste die Bedingung 6.25 für alle perfekten Gitter dieser Dimension. □

Bemerkung 6.33 *Ein Gitter L von Minimum m ist stark perfekt, genau dann wenn für alle $\alpha \in \mathbb{R}^n$ gilt*

$$(\star) \quad \sum_{x \in S(L)} (x, \alpha)^2 = \frac{|S(L)|}{n} m(\alpha, \alpha)$$
$$(\star\star) \quad \sum_{x \in S(L)} (x, \alpha)^4 = \frac{3|S(L)|}{n(n+2)} m^2 (\alpha, \alpha)^2$$

Setzt man $\alpha = \xi_1 \alpha_1 + \xi_2 \alpha_2$ in die 2. Gleichung ein, so ergibt sich durch Koeffizientenvergleich (bei $\xi_1 \xi_2$)

$$(\star\star)_1 \quad \sum_{x \in S(L)} (x, \alpha_1)^2 (x, \alpha_2)^2 = \frac{m^2 |S(L)|}{n(n+2)} (2(\alpha_1, \alpha_2)^2 + (\alpha_1, \alpha_1)(\alpha_2, \alpha_2)).$$

Bemerkung 6.34 *Einen zweiten Beweis des Hauptsatzes 6.31 werden Sie in der Übung kennenlernen. Dort wird gezeigt, dass die Grammatrix*

$$G := ([\rho_x^2, \rho_y^2])_{x,y\in S(L)} = ((x,y)^2)_{x,y\in S(L)} = (\mathrm{Spur}(x^{tr}xy^{tr}y)_{x,y\in S(L)} \in \mathbb{R}^{|S(L)|\times|S(L)|}$$

Rang $n(n+1)/2$ hat. Dazu wird gezeigt, dass

$$G^2 = 2aG + aJ \text{ mit } a = \frac{|S(L)|}{n(n+2)}$$

und $GJ = JG = cJ$ mit $c = |S(L)|/n$ ist. Daraus ergibt sich, dass die Eigenwerte von G genau c (mit Vielfachheit 1), 0 und a sind. Aus $\mathrm{Spur}(G) = |S(L)| = c + (\mathrm{Rang}(G) - 1)a = |S(L)|$ *ergibt sich dann* $\mathrm{Rang}(G) = n(n+1)/2$.

Satz 6.35 *Sei L ein stark perfektes Gitter der Dimension n. Dann ist* $\min(L)\min(L^\#) \geq \frac{n+2}{3}$.

Beweis. Sei $m := \min(L)$, $m' := \min(L^\#)$ und $\alpha \in S(L^\#)$. Dann gilt $(x,\alpha) \in \mathbb{Z}$ für alle $x \in S(L)$ und

$$\begin{aligned} \textstyle\sum_{x\in S(L)}(x,\alpha)^2 &= \tfrac{|S(L)|}{n}mm' \\ \textstyle\sum_{x\in S(L)}(x,\alpha)^4 &= \tfrac{3|S(L)|}{n(n+2)}(mm')^2 \end{aligned}$$

Die Differenz dieser beiden Gleichung ergibt

$$\sum_{x\in S(L)} (x,\alpha)^2((x,\alpha)^2 - 1) = \frac{|S(L)|mm'}{n}(\frac{3mm'}{n+2} - 1).$$

Dies ist ≥ 0, da $(x,\alpha)^2$ entweder $0, 1$ oder ≥ 4 ist. Also ist $\frac{3mm'}{n+2} - 1 \geq 0$ und damit $mm' \geq \frac{n+2}{3}$. □

Definition 6.36 *Ein stark perfektes Gitter, bei dem Gleichheit gilt in Satz 6.35 heißt* vom minimalem Typ.

Bemerkung 6.37 *Ein stark perfektes Gitter L ist vom minimalen Typ, genau dann wenn für alle $\alpha \in S(L^\#)$ und alle $x \in S(L)$ gilt, dass $(x,\alpha) \in \{0, \pm 1\}$.*

Bemerkung Stark perfekte Wurzelgitter $\neq \mathbb{E}_8$ sind vom minimalen Typ.

Beweis. Sei L ein stark perfektes Wurzelgitter, $\alpha \in S(L^*)$ und $x \in S(L)$. Dann ist $(\alpha, x) \in \mathbb{Z}$. Ist $(\alpha, x) \geq 2$, so ist $(\alpha - x, \alpha - x) < (\alpha, \alpha)$ also (da $L \subset L^*$ und $\alpha \in S(L^*)$ kürzester Vektor) $\alpha = x$. Dann ist aber L^* auch ein Wurzelgitter (da $\mathrm{Aut}(L) = \mathrm{Aut}(L^*)$ transitiv auf den Wurzeln operiert) und daher $L = L^* \cong \mathbb{E}_8$. Sonst ist $|(\alpha, x)| \leq 1$ und damit L von minimalem Typ. □

6.3 Designs und Wurzelgitter.

Definition 6.38 *Sei L ein irreduzibles Wurzelgitter der Dimension n und $s := |R(L)| = |S(L)|$. Dann heißt $h := s/n$ die* Coxeter-Zahl *von L.*
Für $r \in R(L)$ bezeichne $n_0 := |\{x \in R(L) \mid (x,r) = 0\}|$ und $n_1 := |\{x \in R(L) \mid (x,r) = 1\}|$.

Bemerkung 6.39 *Die Coxeter-Zahlen der irreduziblen Wurzelgitter sind $h(\mathbb{A}_n) = n+1$, $h(\mathbb{D}_n) = 2(n-1)$, $h(\mathbb{E}_6) = 12$, $h(\mathbb{E}_7) = 18$ und $h(\mathbb{E}_8) = 30$.*

	h	s	n_0	n_1	$t-$Design
$\mathbb{A}_1$	2	2	0	0	$t \leq \infty$
$\mathbb{A}_2$	3	6	0	2	$t \leq 5$
$\mathbb{A}_n (n \geq 3)$	$n+1$	$n(n+1)$	$(n-1)(n-2)$	$2(n-1)$	$t \leq 3$
$\mathbb{D}_4$	6	24	6	8	$t \leq 5$
$\mathbb{D}_n (n \geq 5)$	$2(n-1)$	$2n(n-1)$	$2(n^2-5n+7)$	$4(n-2)$	$t \leq 3$
$\mathbb{E}_6$	12	72	30	20	$t \leq 5$
$\mathbb{E}_7$	18	126	60	32	$t \leq 5$
$\mathbb{E}_8$	30	240	126	56	$t \leq 7$

Satz 6.40 *Mit den Bezeichungen aus Definition 6.38 gilt:*
(a) n_0 und n_1 sind unabhängig von der Wahl von $r \in R(L)$.
(b) L ist stark eutaktisch.
(c) Für jedes $\alpha \in \mathbb{R}^n$ ist

$$\sum_{x \in R(L)} (x,\alpha)^2 = 2h(\alpha,\alpha).$$

(d) $n_0 + 2n_1 = s - 2$.
(e) $n_1 = 2h - 4$.
(f) $n_0 = s - 2 - 2n_1 = hn - 2 - 4h + 8 = h(n-4) + 6$.

Beweis. (a) folgt aus der Transitivität der Weyl-Gruppe auf $R(L)$.
(b) folgt aus der Irreduzibilität der Weyl-Gruppe.
(c) Direkt aus der expliziten Form der Konstante c_2 in Satz 6.22.
(d) ist klar da die Skalarprodukte unter den Wurzeln $0, \pm 1, \pm 2$ sind und $(x,y) = \pm 2$ genau dann wenn $x = \pm y$ für $x, y \in R(L)$.
(e) ergibt sich durch Einsetzen von $\alpha = r$ in (c).
(f) folgt aus (e) und (d). □

Satz 6.41 *Sei L ein stark perfektes Wurzelgitter. Dann ist L isometrisch zu $\mathbb{A}_1$, $\mathbb{A}_2$, $\mathbb{D}_4$, $\mathbb{E}_6$, $\mathbb{E}_7$, oder $\mathbb{E}_8$.*

Beweis. Zunächst zeigen wir, dass stark perfekte Gitter orthogonal unzerlegbar sind. Ist L stark perfekt und $L = L_1 \perp L_2$, so wählen wir $\alpha_1 \in L_1$ und $\alpha_2 \in L_2$ und erhalten mit

Bemerkung 6.33 $(\star\star)_1$:

$$0 = \sum_{x \in S(L)} (x, \alpha_1)^2 (x, \alpha_2)^2 = \frac{\min(L)^2 |S(L)|}{n(n+2)} (2(\alpha_1, \alpha_2)^2 + (\alpha_1, \alpha_1)(\alpha_2, \alpha_2)) > 0$$

ein Widerspruch.
Insbesondere sind stark perfekte Wurzelgitter irreduzibel.
Sei nun $\alpha \in R(L)$ eine Wurzel, $n_1 := \{x \in R(L) \mid (x, \alpha) = 1\}$. Dann ist

$$\begin{array}{ll} \sum_{x \in R(L)} (x, \alpha)^2 & = 2n_1 + 8 \quad = 4h \\ \sum_{x \in R(L)} (x, \alpha)^4 & = 2n_1 + 32 \quad = 48h/(n+2) \end{array}$$

woraus sich als Differenz

$$24 = 4h(12/(n+2) - 1) \Leftrightarrow 6(n+2) = h(10-n)$$

ergibt. Insbesondere ist $n \leq 9$. Für $n = 3$ und $n = 5$ gilt auch dass $10 - n$ nicht $6(n+2)$ teilt, also sind auch diese Fälle unmöglich und es bleiben die Dimensionen $n = 1, 2, 4, 6, 7, 8, 9$ übrig. Jetzt benutzen wir die Klassifikation aller irreduziblen Wurzelgitter.
Für $n = 9$ muss $h = 66$ gelten, ein Widerspruch zu $h(\mathbb{A}_9) < h(\mathbb{D}_9) = 16$.
Für $n = 8$ folgt $h = 30$, $|S(L)| = 240$ und daher $L = \mathbb{E}_8$.
Für $n = 7$ ergibt sich $h = 18$ und daher $L = \mathbb{E}_7$.
Ebenso findet man alle anderen Möglichkeiten. □

6.4 Klassifikation stark perfekter Gitter.

Eine kombinatorische Methode der Klassifikation aller stark perfekten Gitter in einer gegebenen Dimension n begründet sich auf die beiden Gleichungen

$$(D2) \quad \sum_{x \in X} (x, \alpha)^2 = \frac{sm}{n} (\alpha, \alpha) =: A_\alpha$$

und

$$(D4) \quad \sum_{x \in X} (x, \alpha)^4 = \frac{3sm^2}{n(n+2)} (\alpha, \alpha)^2 =: B_\alpha$$

wo $X \dot\cup -X = S(L)$ die Menge aller kürzesten Vektoren in einem stark perfekten Gitter $L \leq \mathbb{R}^n$ mit $\min(L) = m$ und $s := |X|$ die halbe Kusszahl von L bezeichnen.

Setzt man $\alpha := \xi_1 \alpha_1 + \xi_2 \alpha_2$ in $(D2)$ so erhält man durch Koeffizientenvergleich

$$(D11)(\alpha_1, \alpha_2) = \sum_{x \in X} (x, \alpha_1)(x, \alpha_2) = \frac{sm}{n} (\alpha_1, \alpha_2) \text{ für alle } \alpha_1, \alpha_2 \in \mathbb{R}^n$$

und aus der Gleichung $(D4)$ findet man

$$(D13)(\alpha_1, \alpha_2) = \sum_{x \in X} (x, \alpha_1)(x, \alpha_2)^3 = \frac{3sm^2}{n(n+2)} (\alpha_1, \alpha_2)(\alpha_2, \alpha_2)$$

$$(D22)(\alpha_1, \alpha_2) = \sum_{x \in X} (x, \alpha_1)^2 (x, \alpha_2)^2 = \frac{sm^2}{n(n+2)} (2(\alpha_1, \alpha_2)^2 + (\alpha_1, \alpha_1)(\alpha_2, \alpha_2))$$

Bemerkung 6.42 *Für $\alpha \in L^{\#}$ sind A_α, B_α und $C_\alpha := \frac{1}{12}(B_\alpha - A_\alpha) \in \mathbb{Z}$*

Beweis. Für $\alpha \in L^{\#}$ liegt $j := (x, \alpha) \in \mathbb{Z}$ für jedes $x \in L$. Weiter ist $j^4 - j^2 = j^2(j-1)(j+1)$ immer durch 12 teilbar und daher

$$C_\alpha = \sum_{x \in X} \frac{1}{12}((x,\alpha)^4 - (x,\alpha)^2) = \frac{sm}{12n(n+2)}(\alpha,\alpha)(3m(\alpha,\alpha) - (n+2)) \in \mathbb{Z}_{\geq 0}.$$

□

Ende am 12.6.

Ebenso zeigt man:

Bemerkung 6.43 *Für $\alpha_1, \alpha_2 \in L^{\#}$ sind $(D11)(\alpha_1,\alpha_2)$, $(D13)(\alpha_1,\alpha_2)$, $(D22)(\alpha_1,\alpha_2)$ ganz. Weiter ist für $j \in \mathbb{Z}$ die Zahl $j(j-1)(j+1)$ immer durch 6 teilbar und somit*

$$C_{\alpha_1,\alpha_2} := \frac{1}{6}((D13)(\alpha_1,\alpha_2) - (D11)(\alpha_1,\alpha_2)) = \frac{sm}{6n(n+2)}(\alpha_1,\alpha_2)(3m(\alpha_2,\alpha_2) - (n+2)) \in \mathbb{Z}_{\geq 0}.$$

6.4.1 Die stark perfekten Gitter in Dimension 7

Sei nun L ein stark perfektes Gitter der Dimension $n = 7$ mit $\min(L) =: m$, $S(L) = X \dot\cup -X$, $|S(L)| = 2s$ und $\min(L^{\#}) = r$. Dann ergibt sich mit Satz 6.35:

$$\frac{7+2}{3} = 3 \leq mr \leq \left(\frac{4}{3}\right)^6 \leq 5,62.$$

Ist also $\alpha \in S(L^*)$ und $x \in S(L)$, so ist

$$(\alpha, x)^2 \leq mr, \text{ also } (\alpha, x) \in \{0, \pm 1, \pm 2\}.$$

Sei $\alpha \in S(L^{\#})$ fest gewählt, $s := |S(L)|$, $mr := \min(L^{\#})\min(L) \in \mathbb{Q}$ und

$$n_i := |\{x \in S(L) \mid (x,\alpha) = i\}| \text{ für } i = 0, 1, 2.$$

Da $S(L)$ ein 4-design ist findet man

$$\begin{array}{lll} (\star)_0: & n_0/2 + n_1 + n_2 & = s \\ (\star)_2: & n_1 + 4n_2 & = \frac{smr}{7} \\ (\star)_4: & n_1 + 16n_2 & = \frac{s(mr)^2}{3 \cdot 7}. \end{array}$$

Dieses Gleichungssystem ist eindeutig nach $n_0 = 2(s - n_1 - n_2)$, n_1 und n_2 auflösbar und es ergibt sich

$$n_2 = \frac{(mr-3)mrs}{2^2 3^2 7}.$$

Fact: Mit Hilfe von Linearer Programmierung erhält man eine obere Schranke an die Kusszahl s eines n-dimensionalen Gitters. Für $n = 7$ liefern diese Methoden $s \leq 70$. Es gibt auch eine bessere Schranke für die Hermite Konstante von Kumar und Elkies, $\gamma_7 \leq 1,866$, die wir

auch benutzen möchten. Also gilt $\min(L)\min(L^\#) \leq 1,866^2 \leq 3,5$. Damit folgt aber $n_2 = 0$ da für $\alpha \in S(L^\#)$ und $x \in S(L)$ gilt

$$(x,\alpha)^2 \leq (x,x)(\alpha,\alpha) \leq 3,5 < 4.$$

Also ist L von minimalem Typ:

Satz 6.44 *Sei L ein stark perfektes Gitter in Dimension 7. Dann ist L von minimalem Typ d.h.* $\min(L)\min(L^\#) = 3$.

Satz 6.45 *Sei L ein stark perfektes Gitter in Dimension 7. Dann ist L ähnlich zu $\mathbb{E}_7$ oder $\mathbb{E}_7^\#$.*

Beweis. Sei L ein solches stark perfektes Gitter. Dann ist $n_1 = \frac{3s}{7}$ also $s = 7t$ mit $t \in \{3,4,\ldots,10\}$.

Fall 1: t ist gerade.
Dann ist t durch kein ungerades Quadrat teilbar und nicht gleich 16. Wir skalieren L so, dass $m := \min(L) = 3/2$. Dann ist $r = \min(L^\#) = 2$ und für beliebiges $\alpha \in L^\#$ ist

$$C_\alpha = \sum_{x\in X} \frac{1}{12}((x,\alpha)^4 - (x,\alpha)^2) = \frac{t}{2^4}(\alpha,\alpha)((\alpha,\alpha)-2) \in \mathbb{Z}_{\geq 0}.$$

Also ist für jedes $\alpha \in L^\#$ der Wert $\frac{1}{2}(\alpha,\alpha)((\alpha,\alpha)-2) \in \mathbb{Z}_{\geq 0}$. Also ist $L^\#$ ein gerades Gitter. Insbesondere gilt $L^\# \subset L$. Wegen

$$\begin{array}{lll} 2/(\det(L^\#)^{1/7}) = & \min(L^\#)/(\det(L^\#)^{1/7}) & \leq 1,866 \\ 3/2(\det(L^\#)^{1/7}) = & \min(L)(\det(L^\#)^{1/7}) & \leq 1,866 \end{array}$$

findet man

$$1,66 \leq \det(L^\#) \leq 4,6.$$

Also ist $\det(L^\#) \in \{2,3,4\}$. Außerdem ist $\det(L^\#)$ durch 2 teilbar, da für jedes $x \in S(L)$ die Restklasse $x + L^\#$ in $L/L^\#$ durch 2 teilbare Ordnung hat.

Durch systematisches Auflisten aller solcher Gitter findet man, dass $L^\# \cong \mathbb{E}_7$ also $L \cong \mathbb{E}_7^\#$ ist.

Fall 2: t ist ungerade.
Dann skalieren wir L so dass $m = \min(L) = 1$ und erhalten

$$C_\alpha = \frac{t}{2^2 \cdot 3^2}(\alpha,\alpha)((\alpha,\alpha)-3) \in \mathbb{Z}_{\geq 0}.$$

Daraus erhalten wir $t = 9$ und $(\alpha,\alpha) \in \mathbb{Z}$ für jedes $\alpha \in L^\#$.

$(D22)(\alpha,\beta) = 2(\alpha,\beta)^2 + (\alpha,\alpha)(\beta,\beta) \in \mathbb{Z}$. liefert wieder, dass (α,β) nicht halbganz sein können für beliebiges $\alpha,\beta \in L^\#$ und daher ist $L^\#$ ein ganzes Gitter.

Sei Γ das gerade Teilgitter von $L^\#$. Dann ist (α,α) sogar durch 4 teilbar für alle $\alpha \in \Gamma$ und $\Gamma' = \frac{1}{\sqrt{2}}\Gamma$ ist ein gerades Gitter. Insbesondere ist $\det(\Gamma)$ durch 2^7 teilbar. Es gilt wie eben

$$113 \leq 4(3/\gamma_7)^7 \leq \det(\Gamma) = 4\det(L^\#) \leq 4\gamma_7^7 \leq 308,1$$

also $\det(\Gamma) = 128$ oder $\det(\Gamma) = 256$. D.h. Γ' ist ein gerades Gitter der Determinante 1 oder 2, woraus man wieder $\Gamma' \cong \mathbb{E}_7$ also $\Gamma = \sqrt{2}\mathbb{E}_7$ findet. Das Gitter L ist also ein Teilgitter vom Index 2 in $\frac{1}{\sqrt{2}}\mathbb{E}_7^{\#}$ mit Minimum 1. Alle diese 127 Teilgitter kann man aber leicht mit dem Rechner durchsuchen und findet $L \cong \frac{1}{\sqrt{2}}\mathbb{E}_7$ in diesem Fall. □

6.4.2 Die stark perfekten Gitter in Dimension 8

Satz 6.46 $\mathbb{E}_8$ *ist das einzige stark perfekte Gitter in Dimension 8.*

Beweis. (Skizze) Wir benutzen dass $\mathbb{E}_8$ das einzige dichteste 8-dimensionale Gitter ist (also insbesondere $\gamma_8 = 2$) und auch die maximale Kusszahl besitzt und jedes andere 8-dimensionale Gitter L Kusszahl $S(L) \leq 150$ hat.
Jedes andere solche stark perfekte Gitter $L \leq \mathbb{R}^8$ wäre von minimalem Typ da dann $\min(L)\min(L^{\#}) = mr < 4$ ist. Bezeichne $s = \frac{1}{2}|S(L)| \leq 75$ so gilt dann also

- $mr = \frac{10}{3}$.
- $n_1 = \frac{s}{n}mr = \frac{5s}{12}$.
- $s = 12t$ ist durch 12 teilbar mit $1 \leq t \leq 6$.

Wir reskalieren nun L so dass $\min(L) = 1$. Dann ist $\min(L^{\#}) = \frac{10}{3}$. Sei nun $0 \neq \alpha \in L^{\#}$ beliebig, $(\alpha, \alpha) = w =: \frac{p}{q}$ mit teilerfremden p, q. Dann sind

$$\frac{pt}{2q} \text{ und } \frac{3^2tp^2}{2^25q^2} \text{ ganz }.$$

Unterscheiden nun 2 Fälle:
1) $t \neq 5$. Dann ist $p = 5p_1$ durch 5 teilbar für alle $\alpha \in L^{\#}$ und die Gleichung $C_\alpha = \frac{5tp_1(3p_1-2q)}{16q^2} \in \mathbb{Z}_{\geq 0}$ liefert, da $t \leq 6$ nicht durch 16 teilbar ist, dass $p_1 = 2p_2$ gerade ist. Daher ist q ungerade und q^2 teil 3^2t, was nur $q = 1$ oder $q = 3$ zulässt. Also ist für jedes $\alpha \in L^{\#}$ die Norm $(\alpha, \alpha) = \frac{5}{3}z$ für eine gerade Zahl z und somit

$$\sqrt{\frac{3}{5}}L^{\#} =: \Gamma$$

ein gerades Gitter mit Minimum 2 und $\Gamma^{\#}$ hat Minimum $\frac{5}{3}$. Für die Determinante $d := \det(\Gamma) \in \mathbb{Z}$ gilt dann

$$\gamma(\Gamma^{\#}) = \frac{5}{3}d^{1/8} < 2,$$

also $d < \left(\frac{6}{5}\right)^8 < 5$. Da für jedes $x \in S(\Gamma^{\#})$ die Klasse $x+\Gamma \in \Gamma^{\#}/\Gamma$ durch 3 teilbare Ordnung hat, gilt $3 \mid d$ und daher $d = 3$. Aus der Theorie der quadratischen Formen kann man jedoch die Existenz eines geraden positiv definiten Gitters der Dimension 8 mit Determinante 3 ausschliessen.

2) $t = 5$. Dann ist $s = 60$. Mit den obigen Ganzheitsargumenten findet man, dass die Normen der Vektoren $\neq 0$ in $L^\#$ von der Form

$$\frac{10}{3}, \frac{16}{3}, 6, 8, \frac{34}{3}, \frac{40}{3}, 14, 16, \ldots$$

sind. Insbesondere sind die Normen in $\Gamma := \sqrt{\frac{3}{2}} L^\#$ ganz und $\Gamma^\#$ stark perfekt von Minimum $\frac{2}{3}$. Für $\alpha, \beta \in \mathbb{R}^8$ ist dann

$$\sum_{x \in S(\Gamma^\#)/\pm 1} (x,\alpha)^2 (x,\beta)^2 = \frac{1}{3}(2(\alpha,\beta)^2 + (\alpha,\alpha)(\beta,\beta)).$$

Insbesondere ist $(\alpha, \beta) \in \mathbb{Z}$ für $\alpha, \beta \in \Gamma$ und damit Γ ein ganzes Gitter. Setze nun

$$\Gamma_0 := \{\alpha \in \Gamma \mid (\alpha,\alpha) \in 3\mathbb{Z}\} \subset \Gamma.$$

Aus der obigen Kongruenz ergibt sich, dass Γ_0 sogar ein Teilgitter von Γ ist (nicht nur eine Teilmenge). Sind nämlich $\alpha, \beta \in \Gamma_0$, so ist

$$\frac{1}{3}(2(\alpha,\beta)^2 + (\alpha,\alpha)(\beta,\beta)) \equiv \frac{2}{3}(\alpha,\beta)^2 \pmod{\mathbb{Z}}$$

und daher auch (α, β) durch 3 teilbar. Also ist Γ_0 ein Teilgitter. Weiter ist der Index $[\Gamma : \Gamma_0] \leq 3$ (also $= 3$). Denn sind $\alpha, \beta \in \Gamma - \Gamma_0$ so ist $\alpha \pm \beta \in \Gamma_0$ da

$$(\alpha \pm \beta, \alpha \pm \beta) = (\alpha,\alpha) + (\beta,\beta) \pm 2(\alpha,\beta) \in 3\mathbb{Z}$$

für ein geeignetes Vorzeichen. (Hier brauchen wir keine Perfektion o.ae., das geht ganz allgemein.) Sei nun $d := \det(\Gamma)$. Dann ist $\gamma(\Gamma^\#) = \frac{2}{3} d^{1/8} \leq \gamma_8 = 2$ und daher $d \leq 3^8$. Also ist $\det(\Gamma_0) = 9d \leq 3^{10}$. Da $\min(\Gamma_0) \geq 9$ findet man

$$\gamma(\Gamma_0) \geq \frac{9}{3^{10/8}} > 2,27$$

ein Widerspruch zu $\gamma_8 = 2$. □

Bemerkung. Die stark perfekten Gitter sind bis zur Dimension 12 alle klassifiziert. In Dimension 10 gibt es bis auf Ähnlichkeit zwei stark perfekte Gitter K'_{10} und $K_{10}^{'\#}$, in Dimension 11 kein und in Dimension 12 bis auf Ähnlichkeit genau ein stark perfektes Gitter, das Coxeter-Todd Gitter K_{12}, das ähnlich zu seinem dualen Gitter $K_{12}^\#$ ist. Weitere stark perfekte Gitter sind bekannt, jedoch keine vollständige Klassifikation.

Übung: Zeigen Sie, unter Benutzung der Tatsache dass $\gamma_9 \leq 2,142$ und die halbe Kusszahl eines 9-dimensionalen Gitters $s \leq 136$ ist, dass es keine stark perfekten Gitter der Dimension 9 gibt.

III Gewichtszähler und Thetareihen.

7 Extremale selbstduale Codes und Blockdesigns.

7.1 Gewichtszähler von Codes

Definition 7.1 *Sei $C \leq \mathbb{F}_q^N$ ein linearer Code. Der* vollständige Gewichtszähler $p_C \in \mathbb{C}[x_a \mid a \in \mathbb{F}_q] = \mathbb{C}[x_0, \ldots, x_{q-1}]$ *ist*

$$p_C(x) := \sum_{c \in C} \prod_{i=1}^{n} x_{c_i}.$$

Der Hamming Gewichtszähler $h_C \in \mathbb{C}[x, y]$ *ist*

$$h_C(x, y) := \sum_{c \in C} x^{N-w(c)} y^{w(c)}.$$

Bemerkung 7.2 *Der Gewichtszähler eines Codes $C \leq \mathbb{F}_q^N$ ist ein homogenes Polynom vom Grad N. Es ist $h_C(x, y) = p_C(x, y, \ldots, y)$.*

Beispiel: $p_{H(\mathbb{F}_2,3)} = x_0^7 + 7x_0^4x_1^3 + 7x_0^3x_1^4 + x_1^7$
$p_{e_8} = x_0^8 + 14x_0^4x_1^4 + x_1^8$.

Satz 7.3 *(MacWilliams Identität) Sei $C \leq \mathbb{F}_p^N$ ein linearer Code, p eine Primzahl. Dann ist*

$$p_{C^\perp}(x_0, \ldots, x_{p-1}) = \frac{1}{|C|} p_C(y_0, \ldots, y_{p-1})$$

wo $y_i = \sum_{j=0}^{p-1} \zeta_p^{ij} x_j$, $\zeta_p = \exp(2\pi i/p)$ eine primitive p-te Einheitswurzel in $\mathbb{C}$.

Beweis. Sei $\epsilon : \mathbb{F}_p^N \to \{0, 1\}$ die Indikatorfunktion von $C^\perp$, d.h. $\epsilon(v) = 1$ falls $v \in C^\perp$ und 0 sonst. Dann ist

$$p_{C^\perp} = \sum_{v \in \mathbb{F}_p^N} \epsilon(v) \prod_{i=1}^{N} x_{v_i}.$$

Wir wollen jetzt die Funktion ϵ kompliziert schreiben. Für $v, w \in \mathbb{F}_p^N$ sei $\zeta_v(w) := \prod_{i=1}^N \zeta_p^{v_i w_i} = \zeta_p^{v \cdot w}$. Dann gilt für $v \in \mathbb{F}_p^N$

$$\frac{1}{|C|} \sum_{c \in C} \zeta_v(c) = \epsilon(v).$$

Denn ist $v \in C^\perp$ so ist die linke Seite gleich 1. Ist $v \notin C^\perp$, so ist $\varphi_v : C \to \mathbb{F}_p, c \mapsto c \cdot v$ eine nichttriviale, also surjektive lineare Abbildung und daher $C = \dot{\cup}_{a=0}^{p-1} \varphi_v^{-1}(\{a\})$ disjunkte Vereinigung gleich großer Mengen. Daher ist in dem Fall

$$\sum_{c \in C} \zeta_v(c) = \frac{|C|}{p} \sum_{a=0}^{p-1} \zeta_p^a = 0.$$

Also ist

$$p_{C^\perp}(x_0, \ldots, x_{p-1}) = \sum_{a_1=0}^{p-1} \cdots \sum_{a_N=0}^{p-1} \epsilon((a_1, \ldots, a_N)) x_{a_1} \cdots x_{a_N} =$$
$$\sum_{a_1=0}^{p-1} \cdots \sum_{a_N=0}^{p-1} \frac{1}{|C|} \sum_{c \in C} \prod_{i=1}^{N} \zeta_p^{a_i c_i} x_{a_1} \cdots x_{a_N} =$$
$$\frac{1}{|C|} \sum_{c \in C} \prod_{i=1}^{N} (\sum_{j=0}^{p-1} \zeta_p^{jc_i} x_j) = \frac{1}{|C|} p_C(y_0, \ldots, y_{p-1}).$$

□

Folgerung 7.4 *Für den Hamming Gewichtszähler eines Codes $C \leq \mathbb{F}_p^N$ gilt:*

$$h_{C^\perp}(x, y) = \frac{1}{|C|} h_C(x + (p-1)y, x - y).$$

Beweis. $h_{C^\perp}(x, y) = p_{C^\perp}(x, y, \ldots, y) = \frac{1}{|C|} p_C(z_0, \ldots, z_{p-1})$ mit $z_i = x + \sum_{j=1}^{p-1} \zeta_p^{ij} y$. Ist $i = 0$, so erhält man $z_0 = x + (p-1)y$. Für $i \in \mathbb{F}_p^*$ durchläuft mit j auch ij ganz $\mathbb{F}_p^*$ also ist für $i \in \{1, \ldots, p-1\}$ die Summe $\sum_{j=1}^{p-1} \zeta_p^{ij} = \sum_{j=1}^{p-1} \zeta_p^j = -1$ und daher $z_i = x - y$. □

Bemerkung 7.5 *Mit derselben Strategie erhält man den Gewichtszähler von $C^\perp$ aus dem von C durch geeignete Variablensubstitution auch für allgemeinere Ringe (z.B. $\mathbb{F}_q$, $q = p^f$, aber auch $\mathbb{Z}/p^m\mathbb{Z}$).*

Beispiel 7.6 *Für $p = 2$ liest sich die MacWilliams Identität als*

$$p_{C^\perp}(x_0, x_1) = \frac{1}{|C|} p_C(x_0 + x_1, x_0 - x_1)$$

und für $p = 3$ erhält man

$$p_{C^\perp}(x_0, x_1, x_2) = \frac{1}{|C|} p_C(x_0 + x_1 + x_2, x_0 + \omega x_1 + \omega^2 x_2, x_0 + \omega^2 x_1 + \omega x_2)$$

wobei $\omega = \zeta_3 = \frac{-1+\sqrt{-3}}{2}$ eine primitive dritte Einheitswurzel ist.

Bemerkung 7.7 *Gewichtszähler selbstdualer Codes.*
Ist $C = C^\perp \leq \mathbb{F}_p^N$ so ist $|C| = p^{N/2}$. Dann liest sich Folgerung 7.4 als

$$h_C(x, y) = h_{C^\perp}(x, y) = h_C((x + (p-1)y)/\sqrt{p}, (x - y)/\sqrt{p})).$$

Das Polynom $h_C(x,y)$ ist also invariant unter der Variablensubstitution $x \mapsto \frac{1}{\sqrt{p}}(x+(p-1)y)$, $y \mapsto \frac{1}{\sqrt{p}}(x-y)$, als Matrix $\frac{1}{\sqrt{p}}\begin{pmatrix} 1 & p-1 \\ 1 & -1 \end{pmatrix}$. Dies schränkt die Menge der möglichen Gewichtszähler selbstdualer Codes ein, sie liegen alle in dem Teilraum der unter dieser Variablensubstitution invarianten Polynome.
Ist $p = 2$, so kann man noch mehr sagen. Jedes Codewort c eines selbstdualen Code $C = C^\perp \leq \mathbb{F}_2^N$ erfüllt natürlich $c \cdot c = 0$, also ist die Anzahl der Einsen in $c \in C$ immer gerade und somit $w(c) \in 2\mathbb{Z}$. Also ist $p_C(x_0,x_1) = p_C(x_0,-x_1)$ und p_C invariant unter der Gruppe von Variablensubstitutionen

$$\langle \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \rangle =: G_I \cong D_{16}.$$

Für doppelt gerade Codes gilt sogar $w(c) \in 4\mathbb{Z}$ und somit $p_C(x_0,x_1) = p_C(x_0,ix_1)$. Der Gewichtszähler eines binären selbstdualen doppelt geraden (oder auch Typ II) Codes ist also invariant unter

$$\langle h := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, d := \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \rangle =: G_{II}$$

einer Gruppe der Ordnung 192.

Folgerung 7.8 *Ist $C = C^\perp \leq \mathbb{F}_2^N$ doppelt gerade, so ist N durch 8 teilbar.*

Beweis. Es ist $(hd)^3 = \zeta_8 I_2 \in G_{II}$. Jedes unter G_{II} invariante homogene Polynom p vom Grad N erfüllt also

$$p(x_0,x_1) = p(\zeta_8 x_0, \zeta_8 x_1) = \zeta_8^N p(x_0,x_1).$$

Daher ist sein Grad N durch 8 teilbar. □

Mit Hilfe der Invariantentheorie erhält man den folgenden Satz, den ich nur zitieren möchte (vgl. z.B. Sturmfels):

Satz 7.9 *(I) Ist $p(x_0,x_1)$ ein unter G_I invariantes Polynom so ist p ein Polynom in $f := x_0^2 + x_1^2 = p_{\langle(1,1)\rangle}$ und $g := p_{e_8} = x_0^8 + 14x_0^4x_1^4 + x_1^8$. oder alternativ in f und*

$$\delta_I := \frac{1}{4}(f^4 - g) == x_0^6x_1^2 - 2x_0^4x_1^4 + x_0^2x_1^6 = x_0^2x_1^2(x_0^2 - x_1^2)^2.$$

(II) Ist $p(x_0,x_1)$ ein unter G_{II} invariantes Polynom so ist p ein Polynom in $g := p_{e_8} = x_0^8 + 14x_0^4x_1^4 + x_1^8$ und $\delta_{II} := x_0^4x_1^4(x_0^4 - x_1^4)^4$.

Folgerung 7.10 *(Gleason) Ist $C = C^\perp \leq \mathbb{F}_2^N$, $N = 8a + 2b$ mit $0 \leq b \leq 3$ so gibt es eindeutig bestimmte Zahlen $k_i \in \mathbb{Z}$, $i = 0,\ldots,a$ mit $k_0 = 1$ so daß*

$$p_C(x_0,x_1) = \sum_{i=0}^{a} k_i f^{4(a-i)+b} \delta_I^i.$$

Ist C zusätzlich doppelt gerade, so ist $N = 24a + 8b$ mit $0 \leq b \leq 2$ durch 8 teilbar und es gibt eindeutig bestimmte Zahlen $l_i \in \mathbb{Z}$ $(i = 0,\ldots,a)$ mit $l_0 = 1$ so daß

$$p_C(x_0,x_1) = \sum_{i=0}^{a} l_i g^{3(a-i)+b} \delta_{II}^i.$$

Definition 7.11 *Ein binärer doppelt gerader selbstdualer Code $C = C^\perp \leq \mathbb{F}_2^N$ mit $N = 24a + 8b$ heißt* extremal*, falls*

$$d(C) = \min\{\mathrm{wt}(c) \mid 0 \neq c \in C\} \geq 4a + 4.$$

Bemerkung 7.12 *Ist C ein extremaler Code, so ist*

$$p_C(1, x) = 1 + A^*_{4a+4}x^{4a+4} + \ldots + A^*_{4a+4}x^{N-4a-4} + x^N$$

eindeutig bestimmt.

Beweis. $p_C(1, x)$ ist Linearkombination von $g^{3(a-i)+b}\delta^i_{II}(1, x) = x^{4i}(1+\ldots)$ $i = 0, \ldots, a)$. Also bestimmen die $a + 1$ Gleichungen $A_0 = 1$ und $A_d = 0$ für $d = 4, 8, \ldots, 4a$ die Koeffizienten l_i in Gleason's Satz eindeutig. Damit ist p_C eindeutig bestimmt. Weiter gilt $A_d = A_{N-d}$, da die Abbildung $c \mapsto c + \mathbf{1}$ eine Bijektion zwischen den Mengen der Codeworte von Gewicht d und $N - d$ herstellt. □

Folgerung 7.13 *Ist $C = C^\perp \leq \mathbb{F}_2^N$ doppelt gerade so ist $d(C) \leq 4\lfloor \frac{N}{24} \rfloor + 4$.*

Zum Beweis müssen wir zeigen, dass die Anzahl A_{4a+4} von Codeworten von Gewicht $4a + 4$ in einem extremalen Code nicht 0 ist. Das geht entweder durch explizite Berechnung von A^*_{4a+4} mit Hilfe der Formel von Bürmann und Lagrange,

$$\begin{array}{lll} A^*_{4a+4} = & \binom{N}{5}\binom{5a-2}{a-1}/\binom{4a+4}{5} & \text{falls } N = 24a \\ A^*_{4a+4} = & \frac{1}{4}N(N-1)(N-2)(N-4)\frac{(5a)!}{a!(4a+4)!} & \text{falls } N = 24a+8 \\ A^*_{4a+4} = & \frac{3}{2}N(N-2)\frac{(5a+2)!}{a!(4a+4)!} & \text{falls } N = 24a+16 \end{array}$$

oder mit Hilfe von endlichen Blockdesigns, wie wir es im nächsten Abschnitt sehen werden.

7.2 Binäre Codes und Blockdesigns.

Definition 7.14 *Eine Menge $\mathcal{D} = B_1, \ldots, B_v$ von k-elementigen Teilmengen $B_i \subset \{1, \ldots, N\}$ (den* Blöcken*) heißt ein t-(N, k, λ)* Blockdesign*, falls jede t-elementige Teilmenge von $\{1, \ldots, N\}$ in genau λ Blöcken enthalten ist.*
Ein Steiner-System *der Stärke t ist ein $t-(N, k, 1)$-Design.*

Satz 7.15 *Ist $\mathcal{D}$ ein t-(N, k, λ) Design, so gilt*

$$v = |\mathcal{D}| = \lambda\binom{N}{t}/\binom{k}{t}.$$

Beweis. Bezeichnet $\Omega_t := \{T \subset \{1, \ldots, N\} \mid |T| = t\}$ so ist $|\Omega_t| = \binom{N}{t}$ und daher

$$\lambda\binom{N}{t} = \sum_{T\in\Omega_t} |\{B \in \mathcal{D} \mid T \subset B\}| = \sum_{B\in\mathcal{D}} |\{T \in \Omega_t \mid T \subset B\}| = |\mathcal{D}|\binom{k}{t}.$$

□

Folgerung 7.16 *Ist $\mathcal{D}$ ein t-(N,k,λ_t) Design und ein $t-1$-(N,k,λ_{t-1}), so gilt*

$$\lambda_t(N-t+1) = \lambda_{t-1}(k-t+1).$$

Definition 7.17 *(***Bezeichnungen***) Sei $C \leq \mathbb{F}_2^N$ ein Code, $\dim(C) = k$, und $C^\perp$ der duale Code. Sei $d := d(C)$ und $d' = d(C^\perp)$. Bezeichne weiter $C_i := \{c \in C \mid \mathrm{wt}(c) = i\}$ und $A_i := |C_i|$. sowie $0 < \tau_1 < \ldots < \tau_s \leq N$ die Gewichte der Vektoren $\neq 0$ in C bzw. $C^\perp$, so dass*

$$p_C(1,y) = 1 + \sum_{i=1}^{s} A_{\tau_i} y^{\tau_i}$$

Da $\mathbb{F}_2^N$ nur ein Wort vom Gewicht N enthält (nämlich $\mathbf{1}$), gilt $A_N = 0$ oder $A_N = 1$. Wir setzen

$$\overline{s} = |\{1 \leq i \leq N-1 \mid A_i \neq 0\}|$$

Wir Identifizieren $\mathbb{F}_2^N$ mit $\mathcal{P}ot(\{1,\ldots,N\})$ indem wir jeden Vektor mit seinem Träger identifizieren. Dann ist

$$C_{\tau_i} := \{c \in C \mid \mathrm{wt}(c) = \tau_i\}$$

eine Teilmenge von Ω_{τ_i}, der Menge der τ_i-elementigen Teilmengen von $\{1,\ldots,N\}$.

Für $0 < t < d'$ sei $u \in \mathbb{F}^N$ vom Gewicht $\mathrm{wt}(u) = t$ beliebig. Wir setzen

$$\lambda_{\tau_i}(u) := |\{c \in C_{\tau_i} \mid u \subset c\}|.$$

Dann gilt

Lemma 7.18 *Die Zahlen $\lambda_{\tau_i}(u)$ erfüllen die folgenden $d'-t$ Gleichungen:*

$$\sum_{i=1}^{\overline{s}} \binom{\tau_i - t}{j} \lambda_{\tau_i}(u) = (2^{k-t-j} - A_N)\binom{N-t}{j} \quad \textit{für } 0 \leq j \leq d'-1-t.$$

Beweis. Für $0 \leq j \leq d'-1-t$ sei

$$M_j := \{(v,c) \in \mathbb{F}_2^N \times C \mid \mathrm{wt}(v) = t+j, u \subset v \subset c, c \neq \mathbf{1}\}.$$

Wir benutzen Bemerkung 2.4, um die Kardinalität von M_j zu bestimmen. Da $t+j \leq d'-1$ ist nämlich $d(C^\perp) > t+j$. Also ist die Projektion auf je $t+j$ Spalten von C der gesamte $\mathbb{F}_2^{t+j}$. Insbesondere gibt es genau 2^{k-t-j} Codeworte, die an beliebigen $t+j$ vorgegebenen Stellen eine 1 haben. Also ist $|M_j| = (2^{k-t-j} - A_N)\binom{N-t}{j}$. Andererseits ist

$$M_j = \bigcup_{i=1}^{\overline{s}} \{(v,c) \in \mathbb{F}_2^N \times C_{\tau_j} \mid \mathrm{wt}(v) = t+j, u \subset v \subset c\}.$$

und daher

$$|M_j| = \sum_{i=1}^{\overline{s}} \lambda_{\tau_i}(u)\binom{\tau_i - t}{j}.$$

□

Lemma 7.19 *Sind* $0 < \tau_1 < \ldots < \tau_s \leq N$ *und*

$$T := \begin{pmatrix} 1 & \tau_1 & \binom{\tau_1}{2} & \ldots & \binom{\tau_1}{s} \\ 1 & \tau_2 & \binom{\tau_2}{2} & \ldots & \binom{\tau_2}{s} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \tau_s & \binom{\tau_s}{2} & \ldots & \binom{\tau_s}{s} \end{pmatrix}$$

so ist T *ist invertierbar mit* $T^{-1} = (f_{ij})$ *wo*

$$f_i(x) := \prod_{j=1, j\neq i}^{s} \frac{\tau_j - x}{\tau_j - \tau_i} = \sum_{j=0}^{s-1} f_{ij} \binom{x}{j}$$

wobei $\binom{x}{j} = x(x-1)\cdots(x-j+1)/(j!)$.

Beweis.

$$\sum_{j=0}^{s-1} f_{ij} \binom{\tau_n}{j} = f_i(\tau_n) = \delta_{in}.$$

□

Satz 7.20 *Sei* $1 \leq t \leq d' - \overline{s}$ *und* $\tau_i \geq t$ *für alle* i *und* $\lambda_{\tau_i}^{(t)} := \lambda_{\tau_i}(1^t, 0^{N-t})$. *Dann ist* C_{τ_i} *ein* t-$(N, \tau_i, \lambda_{\tau_i}^{(t)})$-*Blockdesign.*

Beweis. $A_N = 0$ oder 1 hängt nur von dem gegebenen Code C ab. Lemma 7.18 liefert also ein lineares Gleichungssystem an die $\lambda_{\tau_i}(u)$ mit Matrix $T' = (\binom{\tau_i - t}{j})_{i,j} \in \mathbb{Z}^{\overline{s} \times d'-1-t}$. Nach Lemma 7.19 hat diese Matrix Rang $\overline{s}$ da die $\tilde{\tau}_i := \tau_i - t$ die Voraussetzungen von Lemma 7.19 erfüllen. Also sind die $\lambda_{\tau_i}(u)$ eindeutig bestimmt und unabhängig von $u \in \Omega_t$ und damit ist C_{τ_i} ein t-$(N, \tau_i, \lambda_{\tau_i}^{(t)})$-Blockdesign. □

Um die $\lambda_{\tau_i} := \lambda_{\tau_i}^{(t)}$ zu bestimmen, lösen wir das lineare GLS

$$(\lambda_{\tau_1}, \ldots, \lambda_{\tau_{\overline{s}}}) T' = (2^{k-t} - A_N, (2^{k-t-1} - A_N)\binom{N-t}{1}, \ldots, (2^{k-d'+1} - A_N)\binom{N-t}{d'-t-1})$$

mit Hilfe von Lemma 7.19 indem wir nur die ersten $\overline{s}$ Gleichungen betrachten. Wir finden

$$(\lambda_{\tau_1}, \ldots, \lambda_{\tau_{\overline{s}}}) = (2^{k-t} - A_N, (2^{k-t-1} - A_N)\binom{N-t}{1}, \ldots, (2^{k-t-\overline{s}+1} - A_N)\binom{N-t}{\overline{s}-1})\tilde{T}^{-1}$$

mit $\tilde{T} = (\binom{\tau_i - t}{j})_{i,j} \in \mathbb{Z}^{\overline{s} \times \overline{s}}$ und $\tilde{T}^{-1} = \tilde{f}_{ij}$ wobei

$$\tilde{f}_i(x) = f_i(x+t) = \prod_{j=1, j\neq i}^{\overline{s}} \frac{\tau_j - t - x}{\tau_j - \tau_i} = \sum_{j=0}^{\overline{s}-1} \tilde{f}_{ij} \binom{x}{j} = \sum_{j=0}^{\overline{s}-1} f_{ij} \binom{x+t}{j}.$$

Also

$$\lambda_{\tau_i} = \sum_{j=0}^{\overline{s}-1} (2^{k-t-j} - A_N)\binom{N-t}{j} \tilde{f}_{ij} = 2^{k-N} \sum_{j=0}^{\overline{s}-1} (2^{N-t-j} - 2^{N-k} A_N)\binom{N-t}{j} \tilde{f}_{ij}.$$

Nun ist

$$2^{N-t-j}\binom{N-t}{j} = \sum_{n=0}^{N-t-j}\binom{N-t-j}{n}\binom{N-t}{j} = \sum_{n=j}^{N-t}\binom{N-t}{n}\binom{n}{j}$$

und daher

$$\lambda_{\tau_i} = 2^{k-N}\sum_{m=0}^{N}\binom{N-t}{m}\sum_{j=0}^{\overline{s}-1}\tilde{f}_{ij}\binom{m}{j} - A_N\sum_{j=0}^{\overline{s}-1}\tilde{f}_{ij}\binom{N-t}{j} =$$

$$2^{k-N}\sum_{m=0}^{N-t}\binom{N-t}{m}\tilde{f}_{\tau_i}(m) - A_N\tilde{f}_{\tau_i}(N-t) =$$

$$2^{k-N}\sum_{r=t}^{N}\binom{N-t}{r-t}f_{\tau_i}(r) - A_N f_{\tau_i}(N) =$$

Setzt man

$$S_i(x) := \prod_{j\neq i, j=1}^{\overline{s}}(\tau_j - x) =: S(x)/(\tau_i - x)$$

so ergibt sich $f_{\tau_i}(x) = S_i(x)/S_i(\tau_i)$ und daher

$$\lambda_{\tau_i}S_i(\tau_i) = -A_N S_i(N) + 2^{k-N}\sum_{r=t}^{N}\binom{N-t}{r-t}S_i(r).$$

Also haben wir gesehen:

Lemma 7.21 *Unter den Voraussetzungen von Satz 7.20 gilt*

$$\lambda_{\tau_i}^{(t)}S_i(\tau_i) = -A_N S_i(N) + 2^{k-N}\sum_{r=t}^{N}\binom{N-t}{r-t}S_i(r).$$

Zusammen mit Folgerung 7.16 ergibt sich daraus folgende Identität:

Folgerung 7.22 *Es gelten wieder die Voraussetzungen von Satz 7.20. Dann ist für* $2 \leq t \leq d' - \overline{s}$

$$A_N S(N) = 2^{k-N}\sum_{r=t-1}^{N}\binom{N-t+1}{r-t+1}S(r).$$

Beweis. C_{τ_i} ist dann ein t-design und ein $(t-1)$-design. Nach Folgerung 7.16 ergibt sich daraus die Gleichheit

$$\lambda_{\tau_i}^{(t)}(N-t+1) = \lambda_{\tau_i}^{(t-1)}(\tau_i - t + 1).$$

$$(N-t+1)A_N S(N)/(N-\tau_i) + (N-t+1)2^{k-N}\textstyle\sum_{r=t}^{N}\binom{N-t}{r-t}S(r)/(\tau_i - r)$$
$$= (\tau_i - t + 1)A_N S(N)/(N-\tau_i) + (\tau_i - t + 1)2^{k-N}\textstyle\sum_{r=t-1}^{N}\binom{N-t+1}{r-t+1}S(r)/(\tau_i - r)$$

Also

$$A_N S(N) = (\tau_i - t + 1)2^{k-N}\textstyle\sum_{r=t-1}^{N}\binom{N-t+1}{r-t+1}S(r)/(\tau_i - r) - (N-t+1)2^{k-N}\sum_{r=t}^{N}\binom{N-t}{r-t}S(r)/(\tau_i - r)$$
$$= 2^{k-N}\textstyle\sum_{r=t-1}^{N}\binom{N-t+1}{r-t+1}S(r)\frac{\tau_i - t + 1 - (r-t+1)}{\tau_i - r}$$

□

7.3 Extremale Codes und Blockdesigns

Satz 7.23 *Sei $C = C^\perp \leq \mathbb{F}_2^N$ ein doppelt gerader Code der Länge $N = 24a + 8b$ mit $d(C) \geq 4a + 4$. Dann ist $d(C) = 4a + 4$ und für die Anzahl A^*_{4a+4} von Codeworten von Gewicht $4a + 4$ gilt*

$$\begin{aligned} A^*_{4a+4} = &\ \tbinom{N}{5}\tbinom{5a-2}{a-1}/\tbinom{4a+4}{5} && \text{falls } N = 24a \\ A^*_{4a+4} = &\ \tfrac{1}{4}N(N-1)(N-2)(N-4)\tfrac{(5a)!}{a!(4a+4)!} && \text{falls } N = 24a+8 \\ A^*_{4a+4} = &\ \tfrac{3}{2}N(N-2)\tfrac{(5a+2)!}{a!(4a+4)!} && \text{falls } N = 24a+16 \end{aligned}$$

Weiter ist C_{4a+4} ein $5-2b$-Design.

Beweis. Es ist $d = d' = 4a + 4$ und

$$\overline{s} \leq |\{4a+4, 4a+8, \ldots, N-(4a+4) = 20a-4+8b\}| = 4a-1+2b$$

. Also ist C_{τ_i} ein Design der Stärke

$$d' - \overline{s} = 4a + 4 - (4a - 1 + 2b) = 5 - 2b (= 5, 3, 1).$$

Die Formel beweisen wir nur in dem Fall, dass $N = 24a$. Lemma 7.21 liefert

$$\lambda^{(t)}_{\tau_i} S_i(\tau_i) = -A_N S_i(N) + 2^{k-N} \sum_{r=t}^{N} \binom{N-t}{r-t} S_i(r).$$

Hier ist $A_N = 1$ und für $\tau_i = 4a + 4$ ist

$$\begin{aligned} S_i(4a+4) = &\ 4 \cdot 8 \cdots (20a - 4 - (4a+4)) = && 4^{4a-2}(4a-2)! \\ S_i(N) = &\ (-1)^{4a-2}(4a+4)\cdot(4a+8)\cdots(20a-8) = && 4^{4a-2}\tfrac{(5a-2)!}{a!} \end{aligned}$$

also ergibt sich für $t = 4$ und $\tau_i = 4a + 4$

$$\lambda^{(4)}_{4a+4} 4^{4a-2}(4a-2)! = -4^{4a-2}\frac{(5a-2)!}{a!} + 2^{-12a}\sum_{r=4}^{24a}\binom{24a-4}{r-4}\frac{S(r)}{4a+4-r}.$$

mit $S(r) = \prod_{i=1}^{4a-1}(4a + 4i - r)$. Es gilt

- $\frac{S(r-4)-S(r)}{16a-4} = \frac{S(r)}{4a+4-r}$
- $\sum_{r=4}^{24a}\binom{24a-4}{r-4}S(r-4) = -\sum_{l=4}^{24a}\binom{24a-4}{l-4}S(l)$
- $\frac{1}{2^{12a}}\sum_{r=4}^{24a}\binom{24a-4}{r-4}S(r) = S(24a) = -4^{4a-1}\frac{(5a-1)!}{a!}$

Denn: $S(r-4) = S(r)\frac{20a-r}{4a+4-r} = S(r) + \frac{(20a-r)-(4a+4-r)}{4a+4-r}S(r)$ woraus sich die erste Gleichung ergibt.
Für die 2. Gleichung bemerkt man zunächst

$$S(r) = (-1)^{4a-1}S(24a-r) = -S(24a-r)$$

und daher

$$\sum_{l=4}^{24a}\binom{24a-4}{l-4}S(l) = -\sum_{l=4}^{24a}\binom{24a-4}{24a-l}S(24a-l) = -\sum_{r=0}^{24a-4}\binom{24a-4}{r}S(r).$$

Die letzte Gleichung ist Folgerung 7.22, da C_{4a+4} sowohl ein 4-design als auch ein 5-design ist.
Also ist

$$2^{-12a}\sum_{r=4}^{24a}\binom{24a-4}{r-4}\frac{S(r)}{4a+4-r} = 2^{-12a}\sum_{r=4}^{24a}\binom{24a-4}{r-4}\frac{S(r-4)-S(r)}{16a-4}$$

$$= -2^{-12a}\frac{1}{8a-2}\sum_{r=4}^{24a}\binom{24a-4}{r-4}S(r) = -\frac{S(24a)}{8a-2} = 4^{4a-1}\frac{(5a-1)!}{a!(8a-2)}$$

und daher

$$\lambda^{(4)}_{4a+4}4^{4a-2}(4a-2)! = -4^{4a-2}\frac{(5a-2)!}{a!} + 4^{4a-1}\frac{(5a-1)!}{a!(8a-2)}$$

bzw.

$$\lambda^{(4)}_{4a+4} = \frac{(6a-1)(5a-2)!}{a!(4a-1)!}.$$

Daraus ergibt sich dann

$$\lambda^{(5)}_{4a+4} = |\mathcal{D}|\binom{4a+4}{5}/\binom{24a}{5} = \lambda^{(4)}_{4a+4}\binom{24a}{4}/\binom{24a}{5}\binom{4a+4}{5}/\binom{4a+4}{4} = \frac{4a}{24a-4}\lambda^{(4)}_{4a+4} = \binom{5a-2}{a-1}$$

und die Anzahl von Worten von Gewicht $4a+4$ ist dann

$$\lambda^{(5)}_{4a+4}\binom{24a}{5}/\binom{4a+4}{5}$$

wie angegeben. □

Mit denselben Methoden lässt sich A^*_r berechnen für $r = 4a+8, \ldots$. Insbesondere findet man:

Satz 7.24 *Sei $C = C^\perp \leq \mathbb{F}_2^N$, $N = 24a$, $d(C) = 4a+4$. Dann bildet C_{τ_i} ein t-$(N, \tau_i, \lambda^{(t)}_{\tau_i})$-design für $1 \leq t \leq 5$ und der Parameter $\lambda^{(4)}_{4a+8}$ ist gegeben als*

$$\lambda^{(4)}_{4a+8} = \frac{6a-1}{a}\binom{5a-2}{a-1}\left(\binom{20a-4}{4}/\binom{4a+4}{4} - (4a-1)\right) + \binom{5a-1}{a+1} - \binom{5a-3}{a-1}.$$

Insbesondere ist $A^*_{4a+8} < 0$ für genügend grosses a. ($a \geq 154$ tuts, d.h. wenn ein solcher Code existiert, dann ist seine Länge $\leq 24 \cdot 153 = 3672$. Man kennt bisher aber nur zwei extremale selbstduale Codes in durch 24 teilbarer Länge, den Golay Code in Länge 24 und den erweiterten quadratischen Rest Code in Länge 48. Es ist bewiesen, dass diese die einzigen solchen Codes in Länge 24 bzw. 48 sind.)

Beweis. Übung □

Dieser Satz zeigt dass es nur endlich viele extremale Codes gibt, in Dimensionen die Vielfache von 24 sind. Analoge Resultate kann man auch für $N = 24a + 8$ und $N = 24a + 16$ erhalten und sieht so:

Satz 7.25 *Es gibt nur endlich viele extremale Codes.*

7.4 Der binäre Golay Code und das Leech Gitter.

Satz 7.26 *Sei $C \leq \mathbb{F}_2^{24}$, $\dim(C) = 12$, $d(C) \leq 8$. Dann ist C ein extremaler doppelt gerader selbstdualer Code. Weiter gibt es bis auf Äquivalenz höchstens einen solchen Code C.*

Beweis. Sei C' der Code der Länge 23, der aus C entsteht, indem man eine Spalte wegläßt. Dann ist $|C'| = 2^{12}$, da sich verschiedene Codeworte von C an mehr als nur einer Stelle unterscheiden und der Minimalabstand von C' ist gleich 7. Insbesondere sind die Kugeln mit Radius 3 um die Codeworte von C' disjunkt. Da

$$2^{12}(1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}) = 2^{23}$$

ist der Code C' ein perfekter Code. Daraus ergeben sich die Anzahlen

$$\begin{array}{llll} A'_0 = & A'_{23} = & 1 \\ A'_7 = & A'_{16} = & \binom{23}{4}/\binom{7}{4} = 253 \\ A'_{11} = & A'_{12} & 1288 \\ A'_8 = & A'_{15} = & (\binom{23}{5} - A_7\binom{7}{5})/\binom{8}{5} = 506. \end{array}$$

Dies ist unabhängig davon, welche Stelle von $\{1, \ldots, 24\}$ man wegläss t. Also sind die Gewichte von C' immer $\equiv_4 -1, 0$ und daher $\mathrm{wt}(C) \subset 4\mathbb{Z}$ und

$$p_C(1, y) = 1 + 759y^8 + 2576y^{12} + 759y^{16} + y^{24}.$$

Also ist C doppelt gerade und insbesondere $C \subset C^\perp$. Aus Dimensionsgründen gilt die Gleichheit. Sei $u \in C$ vom Gewicht 12. Sei C_u der Code der Länge 12, der aus C entsteht, indem alle Spalten weggelassen werden, wo $u_i = 1$. $C_u = \mathrm{Bild}(\pi_u)$. Dann ist $\ker(\pi_u) = \{u, 0\}$ also ist C_u gerade, hat Länge 12 und Dimension 11. Damit ist C_u der gerade Teilcode von $\mathbb{F}_2^{12}$ und nach geeigneter Umordnung der Spalten hat C eine Erzeugermatrix der Form

$$\mathcal{G} := \left(\begin{array}{c|c|c|c} 1^{11} & 1 & 0 & 0^{11} \\ \hline A & 0_{11} & 1_{11} & I_{11} \end{array}\right)$$

mit $A \in \mathbb{F}_2^{11\times 11}$ die folgenden beiden Eigenschaften hat:

- Jede Zeile in A hat Gewicht ≥ 6.
- Je zwei Zeilen von A haben Abstand ≥ 6.

Da jede Zeile von $\mathcal{G}$ Abstand ≥ 8 von u (der 1. Zeile von $\mathcal{G}$) hat, hat jede Zeile von A Gewicht 6. Darau sieht man auch, dass je 2 Zeilen von A genau Abstand 6 haben.

Ende am 25.6.

Jedes Paar von Zeilen hat also genau 2 Nullen gemeinsam. Gibt man umgekehrt 2 beliebige Positionen aus den $\binom{11}{2}$ möglichen vor, so hat eines der $\binom{11}{2}$ Paare von Zeilen genau dort die gemeinsamen Nullen. Denn wenn diese Paar von Nullen in 3 Zeilen von A so hat A ŒZeilen der Form

$$\begin{array}{cccccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \end{array}$$

wobei sich die letzte Zeile aus der Voraussetzung ergibt, dass die letzten beiden Positionen 0 sind und der Abstand von den anderen beiden Zeilen gleich 6. Dann liefert aber die Summe der entsprechenden Zeilen in $\mathcal{G}$ ein Wort vom Gewicht 4. Also ist $(J - A)$ die Inzidenzmatrix eines $2-(11,5,2)$-Designs, welches nach Übungsaufgabe eindeutig bestimmt ist. □

Satz 7.27 *Es gibt einen extremalen doppeltgeraden selbstdualen binären Code $\mathcal{G}_{24}$ der Länge 24. Dieser heißt der* Golay Code *der Länge 24.*

Beweis. Wir geben J.H. Conway's Konstruktion des Golay Codes aus dem Hexacode, $h_6 \leq \mathbb{F}_4^6$ mit Erzeugermatrix

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

an. Es gilt $h_6 = \overline{h_6}^{\perp}$ (Hermitesch selbstdual) wobei $\overline{\ }$ der nichttriviale Galoisautomorphismus von $\mathbb{F}_4$ ist ($\overline{x} = x^2$). Da $x\overline{x} = 1$ für $x \in \mathbb{F}_4, x \neq 0$, sind die Hamming Gewichte aller Codeworte in h_6 gerade. Insbesondere hat h_6 kein Wort von Gewicht 3 oder 5. Die Worte c vom Gewicht 2 in h_6 sind Linearkombinationen von 2 Erzeugern. Aus Symmetriegründen können wir annehmen, dass $c = b_1 + ab_2$ ist mit $a \in \{0, 1, \omega, \omega^2\}$. Diese Worte haben aber alle Gewicht 4, also ist $d(h_6) = 4$. Der Hamming Gewichtszähler von h_6 ist

$$h_{h_6} = x^6 + 45x^2y^4 + 18y^6.$$

(Die Worte vom Gewicht ≤ 5 sind von der Form $ab_i + bb_j$ mit $1 \leq i < j \leq 3$ und $(a, b) \in \mathbb{F}_4^2 - \{0\}$. Davon gibt es $3 \cdot (16 - 1) - 9 = 36$ Stück. Von den Linearkombinationen von 3 Basisvektoren mit Koeffizienten $\neq 0$, also $ab_1 + bb_2 + cb_3$ mit $a, b, c \in \mathbb{F}_4 - \{0\}$ haben 18 Gewicht 6 und 9 Gewicht 4.)

Identifiziert man $\mathbb{F}_2^{24}$ mit $\mathbb{F}_2^{4\times 6}$ in der offensichtlichen Weise so ist

$$\mathcal{G}_{24} = \{(x_{ij}) \in \mathbb{F}_2^{4\times 6} \mid \begin{array}{l} \sum_{i=1}^4 x_{ij} = \sum_{j=1}^6 x_{1j} \quad \text{für alle } j = 1, \ldots, 6 \\ x_2 + \omega x_3 + \overline{\omega} x_4 \in h_6 \end{array} \}.$$

Wir zeigen dazu, dass der in der Menge beschriebene lineare Code Dimension 12 hat und Minimalabstand ≥ 8.

Die $\mathbb{F}_2$-lineare Abbildung

$$\mathbb{F}_2^3 \to \mathbb{F}_4,\ x \mapsto x_1 + \omega x_2 + \overline{\omega} x_3$$

hat Kern $\langle (1,1,1) \rangle = \{(0,0,0),(1,1,1)\}$. Also gibt es zu jedem $c \in h_6$ genau 2^6 Matrizen $(X_{ij}) \in \mathbb{F}_2^{3\times 6}$ mit $X_1 + \omega X_2 + \omega^2 X_3 = c$. Die Urbilder werden genau durch die Spaltensummen $\in \mathbb{F}_2^6$ unterschieden. Wählt man sich also eine beliebige erste Zeile $(x_{11}, \ldots, x_{16}) \in \mathbb{F}_2^6$ und ein beliebiges Wort $c \in h_6$ so enthält $\mathcal{G}_{24}$ genau eine Matrix (x_{ij}) mit dieser ersten Zeile und so dass $x_2 + \omega x_3 + \overline{\omega} x_4 = c$. Also ist $|\mathcal{G}_{24}| = 2^6 \cdot 4^3 = 2^{12}$.

Zum Minimalgewicht: Sei $X := (x_{ij}) \in \mathcal{G}_{24}$. Ist $\sum_{j=1}^6 x_{1j}$ gerade und $c \neq 0$, so ist $\mathrm{wt}(c) \geq 4$ und X hat mindestens 4 Spalten $\neq 0$, in denen dann 2 oder 4 Einsen stehen müssen. Daher $\mathrm{wt}(X) \geq 2 \cdot 4 = 8$. Ist $c = 0$ und die erste Zeile nicht 0, so enhält diese mindestens 2 Einsen. Die zugehörigen Spalten sind dann aber $(1,1,1,1)^{tr}$ also $\mathrm{wt}(X) \geq 8$. Ist $\sum_{j=1}^6 x_{1j}$ ungerade so steht in jeder Spalte mindestens eine 1, da die Spaltensummen alle ungerade sein müssen. Also ist $\mathrm{wt}(X) \geq 6$. Ist $\mathrm{wt}(X) = 6$, so ist $c \in h_6$ ein Wort vom Gewicht 5, was nicht existiert. □

Definition 7.28 *(Leech Gitter) Sei*

$$M := L_{\mathcal{G}_{24}} = \{\sum_{i=1}^{24} a_i x_i \mid (a_1 + 2\mathbb{Z}, \ldots, a_{24} + 2\mathbb{Z}) \in \mathcal{G}_{24} i\}$$

wobei $(x_1, \ldots, x_{24})$ eine OG-Basis ist mit $(x_i, x_i) = 1/2$ das Codegitter (vgl. Definition 2.13) zu $\mathcal{G}_{24}$. Dann ist $\min(M) = 2$ und $S(M) = \{\pm 2x_1, \ldots, \pm 2x_{24}\}$. Sei $M_0 := \{m \in M \mid (m, \sum_{i=1}^{24} x_i) \in 2\mathbb{Z}\} \leq M$ und $M_1 := \{m \in M \mid (m, \sum_{i=1}^{24} x_i) \in 1 + 2\mathbb{Z}\} \subset M$ und setze

$$\Lambda_{24} := M_0 \cup (\frac{1}{2} \sum_{i=1}^{24} x_i + M_1).$$

Λ_{24} *heißt das* Leech Gitter. *,*

Satz 7.29 Λ_{24} *ist ein gerades unimodulares Gitter mit* $\min(\Lambda_{24}) = 4$.

Beweis. Es ist klar, dass M_0 ein Teilgitter vom Index 2 in dem geraden unimodularen Gitter M ist. Da $S(M) \not\subset M_0$, ist $\min(M_0) \geq 4$. Die Elemente $y := \frac{1}{2} \sum_{i=1}^{24} x_i + m$ mit $m \in M_1$ erfüllen

- $(y,y) = \frac{12}{4} + (\sum_{i=1}^{24} x_i, m) + (m,m) \in 2\mathbb{Z}$.
- $y = \sum a_i x_i$ mit allen $a_i \in \frac{1}{2} + \mathbb{Z}$.
- $(y,y) \geq 3$.
- $y_1 + y_2 = \sum_{i=1}^{24} x_i + m_1 + m_2 \in M_0$ für $y_1, y_2 \in \frac{1}{2} \sum_{i=1}^{24} x_i + M_1)$.

Also ist Λ_{24} ein gerades Gitter und $\min(\Lambda_{24}) \geq 4$. Da M_0 ein Teilgitter von Index 2 in Λ_{24} ist, ist Λ_{24} unimodular. □

Vektoren der Quadratlänge 4 in Λ_{24}:

wo	Typ	Anzahl	
$M_0:$	$\pm 1^8 0^{16}$	$759 \cdot 2^7 =$	97152
	$\pm 2^2 0^{22}$	$4\binom{24}{2} =$	1104
$\frac{1}{2}\sum x_i + M_1:$	$(\pm 1/2)^{23} \pm 3/2$	$24 \cdot 2^1 2 =$	98304
			196560

8 Thetareihen von Gittern.

Definition 8.1 *Sei L ein ganzes Gitter in $(\mathbb{R}^n, (,))$. Die formale Potenzreihe*

$$\Theta_L := \sum_{\ell \in L} q^{(\ell,\ell)} = \sum_{m=0}^{\infty} a_m q^m \in \mathbb{C}[[q]]$$

mit $a_m = |L_{=m}|$ heißt Theta-Reihe *von L. Analog definiert man für jede (geeignete) Teilmenge $T \subset \mathbb{R}^n$ (z.B. $T = v + L$, eine Restklasse nach einem Gitter L) die Theta-Reihe $\Theta_T := \sum_{t \in T} q^{(t,t)}$.*

Beispiel 8.2 $\Theta_{\mathbb{Z}} = \sum_{a \in \mathbb{Z}} q^{a^2} = 1 + 2\sum_{n=1}^{\infty} q^{n^2}$.
Sind L, M Gitter, so gilt

$$\Theta_{L \perp M} = \Theta_L \Theta_M.$$

Ist $a \in \{0, \ldots, p-1\}$ so sei $\theta_{a,p} := \sum_{z \in \mathbb{Z}, z \equiv_p a} q^{z^2/p}$. Ist $e \in \mathbb{R}^n$ ein Vektor mit $(e,e) = 1/p$ so ist $\theta_{a,p} = \Theta_{ae + \langle pe \rangle_{\mathbb{Z}}}$.

Satz 8.3 *Sei $C \leq \mathbb{F}_p^N$ ein Code und $L_C \leq \mathbb{R}^N$ das zugehörige Codegitter. Dann ist*

$$\Theta_{L_C} = p_C(\theta_{0,p}, \theta_{1,p}, \ldots, \theta_{p-1,p}).$$

Beweis. Sei $M := \langle x_1, \ldots, x_N \rangle$ mit $(x_i, x_j) = 1/p\delta_{ij}$, $pM \subset L_C \subset M$ genauer

$$L_C = \{\sum a_i x_i \mid (a_1 + p\mathbb{Z}, \ldots, a_N + p\mathbb{Z}) \in C = \dot{\cup}_{c \in C} \sum c_i x_i + pM.$$

Also ist

$$\Theta_{L_C} = \sum_{c \in C} \Theta_{\sum c_i x_i + pM} = \sum_{c \in C} \prod_{i=1}^{N} \theta_{c_i,p}.$$

□

Beispiel 8.4 *Sei $p = 2$ und*

$$A := \theta_{0,2} = 1 + 2\sum_{a=1}^{\infty} q^{2a^2},\ B := \theta_{1,2} = \sum_{a=0}^{\infty} 2q^{(2a+1)^2/2}.$$

Dann ist

$$\Theta_{E_8} = \Theta_{L_{e_8}} = p_{e_8}(A, B) = A^8 + 14A^4B^4 + B^8.$$

$A = 1 + 2q^2 + 2q^8 + \ldots$, *also* $A^4 = 1 + 8q^2 + 4 \cdot 6q^4 + \ldots$ *und* $A^8 = 1 + 16q^2 + 4 \cdot 28q^4 + \ldots$. *Weiter ist* $B = 2q^{1/2} + 2q^{9/2} + \ldots$ *und daher* $B^4 = 16q^2 + 4 \cdot 16q^6 + \ldots$ *und* $B^8 = 2^8q^4 + \ldots$. *Daher ist*

$$\Theta_{E_8} = 1 + (16 + 14 \cdot 16)q^2 + (112 + 14 \cdot 128 + 256)q^4 + \ldots = 1 + 240q^2 + 2160q^4 + \ldots.$$

Ende am 29.6.

Lemma 8.5 *Sei L ein Gitter. Setzt man $q = \exp(\pi i z)$ mit $z \in \mathbb{H} := \{z \in \mathbb{C} \mid \Im(z) > 0\}$ so ist die Reihe $\Theta_L : \mathbb{H} \to \mathbb{C}$ absolut und uniform konvergent auf jedem Streifen $\Im(z) \geq v_0 > 0$ und somit eine holomorphe Funktion.*

Beweis. Sei $L = \mathbb{Z}^n M$ für ein $M \in \mathrm{GL}_n(\mathbb{R})$ und $\epsilon := \min_{xx^{tr}=1} xMM^{tr}x^{tr}$. Dann ist $\epsilon > 0$ und $xMM^{tr}x^{tr} \geq \epsilon xx^{tr}$ für alle $x \in \mathbb{R}^n$. Daher erhält man

$$\sum_{\ell \in L} |\exp(\pi i z(\ell, \ell))| = \sum_{x \in \mathbb{Z}^n} |\exp(\pi i z(xM, xM))| \leq \sum_{x \in \mathbb{Z}^n} \exp(-\pi v_0 \epsilon(x, x)) = (\sum_{r=-\infty}^{\infty} \exp(-\pi v_0 \epsilon r^2))^n < \infty.$$

□

Bemerkung 8.6 *Ist L ganz, so ist $\Theta_L(z+2) = \Theta_L(z)$ für alle $z \in \mathbb{H}$ und ist L sogar gerade, so gilt $\Theta_L(z+1) = \Theta_L(z)$.*

Satz 8.7 *(Poisson Summations Formel) Sei $f : \mathbb{R}^n \to \mathbb{C}$ eine Funktion, die die Bedingungen (V1), (V2), (V3) erfüllt. Dann ist für jedes volle Gitter $\Gamma \leq \mathbb{R}^n$*

$$\sum_{x \in \Gamma} f(x) = \det(\Gamma)^{-1/2} \sum_{y \in \Gamma^\#} \hat{f}(y)$$

wobei

$$\hat{f}(y) = \int_{\mathbb{R}^n} f(x) \exp(-2\pi i x y^{tr}) dx$$

die Fourier-Transformierte *von f ist und die Bedingungen (V1), (V2), (V3) wie folgt sind:*

(V1) $\int_{\mathbb{R}^n} |f(x)| dx < \infty$ *(damit $\hat{f}$ existiert).*

(V2) Die Reihe

$$F(u) := \sum_{x \in \Gamma} f(x + u)$$

konvergiert absolut und uniform auf jedem Kompaktum (damit $F(u)$ stetig ist).

(V3) Die Reihe $\sum_{y\in\Gamma^\#}\hat{f}(y)$ konvergiert absolut.

Beweis. Wir beweisen den Satz zunächst für $\Gamma=\mathbb{Z}^n$.
Die Funktion $F(u):=\sum_{x\in\mathbb{Z}^n}f(x+u)$ ist nach Voraussetzung (V2) stetig und periodisch in u, $F(u+x)=F(u)$ für $x\in\mathbb{Z}^n$. Also hat F eine Fourier-Entwicklung

$$F(u)=\sum_{y\in\mathbb{Z}^n}\exp(2\pi i(u,y))a(y)$$

wobei $a(y)=\int_{[0,1]^n}F(t)\exp(-2\pi i(t,y))dt$. Wir zeigen, $\hat{f}(y)=a(y)$. Dann gilt nämlich wegen (V3), dass

$$F(0)=\sum_{x\in\mathbb{Z}^n}f(x)=\sum_{y\in\mathbb{Z}^n}\hat{f}(y).$$

Es ist für $y\in\mathbb{Z}^n$

$$\begin{aligned}a(y)&=\textstyle\int_{[0,1]^n}\sum_{x\in\mathbb{Z}^n}f(x+t)\exp(-2\pi i(t,y))dt\\&=\textstyle\sum_{x\in\mathbb{Z}^n}\int_{[0,1]^n}f(x+t)\exp(-2\pi i((x+t),y))dt\\&=\textstyle\sum_{x\in\mathbb{Z}^n}\int_{x+[0,1]^n}f(t)\exp(-2\pi i(t,y))dt=\hat{f}(y).\end{aligned}$$

Im allgemeinen Fall ist $\Gamma=\mathbb{Z}^nM$ mit $M\in\mathrm{GL}_n(\mathbb{R})$ und $\Gamma^\#=\mathbb{Z}^nM^{-tr}$. Also ist

$$\sum_{x\in\Gamma}f(x)=\sum_{x\in\mathbb{Z}^n}f(xM)=\sum_{x\in\mathbb{Z}^n}f_M(x)=\sum_{y\in\mathbb{Z}^n}\hat{f}_M(y)$$

wobei

$$\hat{f}_M(y)=\int_{\mathbb{R}^n}f(tM)\exp(-2\pi i(t,y))dt=\frac{1}{|\det(M)|}\int_{\mathbb{R}^n}f(t)\exp(-2\pi i(tM^{-1},y))dt=\det(\Gamma)^{-1/2}\hat{f}(yM^{-tr}$$

□

Satz 8.8 *(Theta Transformationsformel) Es gilt für ein volles Gitter $L\leq\mathbb{R}^n$*

$$\Theta_L(-1/z)=(z/i)^{n/2}\det(L)^{-1/2}\Theta_{L^\#}(z).$$

Beweis. Beide Seiten sind holomorphe Funktionen auf $\mathbb{H}$. Daher genügt es die Identität für $z=it$ mit $t>0$ nachzuweisen. Die Fouriertransformierte von $f(x)=\exp(\frac{-\pi}{t}(x,x))$ ist $\hat{f}(y)=t^{n/2}\exp(-\pi t(y,y))$ (Übung). Daher erhalten wir mithilfe von Poisson Summation:

$$\begin{aligned}&\Theta_L(\tfrac{-1}{it})=\textstyle\sum_{x\in L}\exp(\frac{-\pi}{t}(x,x))=\\&\det(L)^{-1/2}\textstyle\sum_{y\in L^\#}t^{n/2}\exp(-\pi t(y,y))=t^{n/2}\det(L)^{-1/2}\Theta_{L^\#}(it).\end{aligned}$$

□

Bemerkung 8.9 *Die Gruppe*

$$\mathrm{SL}_2(\mathbb{Z}) := \langle S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$$

operiert auf der oberen Halbebene durch Möbiustransformationen:

$$\gamma z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} z := \frac{az+b}{cz+d}.$$

Insbesondere ist

$$Tz = z + 1 \text{ und } Sz = \frac{-1}{z}.$$

Definition 8.10 *Sei $k \in 2\mathbb{Z}_{\geq 0}$. Eine holomorphe Funktion $f : \mathbb{H} \to \mathbb{C}$ heißt* Modulform vom Gewicht *k falls*

(i) $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ *für alle* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ *und*

(ii) f *hat eine Potenzreihenentwicklung* $f(z) = \sum_{n=0}^{\infty} a_n \exp(2\pi i n z)$.

Bemerkung 8.11 *Eine holomorphe Funktion $f : \mathbb{H} \to \mathbb{C}$ ist genau dann eine Modulform, falls $f(z) = f(z+1)$ und $f(-1/z) = z^k f(z)$ und die wegen der ersten Bedingung existierende Fourierentwicklung $f(z) = \sum_{-\infty}^{\infty} a_n \exp(2\pi i n z)$ die Bedingung $a_n = 0$ für $n < 0$ erfüllt.*

Satz 8.12 *Ist $L \leq \mathbb{R}^n$ ein gerades unimodulares Gitter, so ist n durch 8 teilbar.*

Beweis. Sei L so ein Gitter. Angenommen n ist nicht durch 8 teilbar. Indem wir L durch $L \perp L$ oder $L \perp L \perp L \perp L$ ersetzen können wir annehmen, dass $n \equiv_8 4$ ist. Dann ist

$$\Theta_L(-1/z) = (-1)^{n/4} z^{n/2} \Theta_L(z) = -z^{n/2} \Theta_L(z).$$

Also ist

$$\Theta_L((TS)z) = -z^{n/2} \Theta_L(z).$$

Da $(TS)z = (z-1)/z$ und $(TS)^2 z = 1/(1-z)$ ist, ergibt sich daraus

$$\begin{aligned} &\Theta_L((TS)^3 z) = \Theta_L((TS)(TS)^2 z) = -(1/(1-z))^{n/2} \Theta_L((TS)^2 z) \\ &= z^{-n/2} \Theta_L((TS)z) = -\Theta_L(z) \end{aligned}$$

ein Widerspruch da $(TS)^3 = I_2$. □

Satz 8.13 *Ist $L \leq \mathbb{R}^n$ ein gerades unimodulares Gitter, so ist Θ_L eine Modulform vom Gewicht $n/2$.*

Beweis. Sei $f := \Theta_L$. Dann ist $f(z) = f(z+1)$, da L ein gerades Gitter ist und f hat eine Fourierentwicklung wie in 8.10 (ii). Wegen der Theta Transformaionsformel ist $f(-1/z) = z^{n/2} f(z)$ (da n durch 8 teilbar ist), also ist f eine Modulform vom Gewicht $n/2$. □

Bemerkung 8.14 *Bezeichne*

$$\mathcal{M}(\mathrm{SL}_2(\mathbb{Z})) := \bigoplus_{k=0}^{\infty} \mathcal{M}_k$$

den Ring der Modulformen wobei $\mathcal{M}_k$ den $\mathbb{C}$-Vektorraum der Modulformen vom Gewicht k bezeichnet. Für $f \in \mathcal{M}_k$ und $g \in \mathcal{M}_l$ ist $fg \in \mathcal{M}_{k+l}$, also ist $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$ eine $\mathbb{Z}$-graduierte $\mathbb{C}$-Algebra.

Satz 8.15 *(ohne Beweis) $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}[E_4, E_6]$, wo*

$$E_4 = \theta_{E_8} = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^{2n} \in \mathcal{M}_4 \text{ und } E_6 = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^{2n} \in \mathcal{M}_6$$

die Eisensteinreihen bezeichnen. Dabei ist $\sigma_t(n) = \sum_{0<d|n} d^t$ die Summe der t-ten Potenzen der Teiler von n.

Beweis. Ein Beweis findet man in Ebeling, Abschnitte 2.5 und 2.6. □

Folgerung 8.16 *Sei*

$$\Delta := \frac{1}{1728}(E_4^3 - E_6^2) = q^2 \prod_{i=1}^{\infty} (1 - q^{2i})^{24} \in \mathcal{M}_{12}.$$

Ist $L \leq \mathbb{R}^n$ ein gerades unimodulares Gitter mit $n = 24a + 8b$, so gibt es Zahlen $c_i \in \mathbb{Q}$ mit

$$\Theta_L = \sum_{i=0}^{a} c_i E_4^{n/8-3i} \Delta^i.$$

Definition 8.17 *Eine Modulform f vom Gewicht k heißt* Spitzenform *, falls $f = \sum_{n=1}^{\infty} q^{2n}$. Bezeichnung: $f \in \mathcal{S}_k$.*

Bemerkung 8.18 *$\mathcal{S} := \bigoplus_{k=1}^{\infty} \mathcal{S}_k = \Delta\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$ ist das von Δ erzeugte Hauptideal in $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$.*

8.1 Extremale gerade unimodulare Gitter

Bemerkung 8.19 *Der Raum $\mathcal{M}_{12a+4b}$ $(0 \leq b \leq 2)$ enthält genau eine* extremale Modulform

$$f^*_{12a+4b} = 1 + 0q^2 + \ldots + 0q^{2a} + a^*_{2a+2} q^{2a+2} + \ldots = 1 + \sum_{i=a+1}^{\infty} a^*_{2i} q^{2i}.$$

Beweis. f ist ein Polynom in E_4 und Δ. $f = \sum_{i=0}^{a} c_i E_4^{3a+b-3i} \Delta^i$. Die $a + 1 = \dim(\mathcal{M}_{12a+4b})$ Bedingungen, dass die Koeffizienten von q^{2i} gleich 0 sind $(1 \leq i \leq a)$ und der von q^0 gleich 1 sind linear unabhängig und bestimmen daher die Koeffizienten c_i eindeutig. □

Satz 8.20 *(ohne Beweis) Man kann zeigen, dass der Koeffizient a^*_{2a+2} in der extremalen Modulform von Null verschieden ist.*

Beweis. C.L. Siegel, Berechnung von Zetafunktionen an ganzzahligen Stellen. Nachr. Akad. Wiss. Göttingen, 87-102 (1969). □

Folgerung 8.21 *Sei $L \leq \mathbb{R}^{24a+8b}$ ein gerades unimodulares Gitter mit $0 \leq b \leq 2$. Dann ist $\min(L) \leq 2 + 2a$. Ist $\min(L) = 2a + 2$, so heißt L* extremal.

Die Thetareihe Θ_L eines extremalen Gitters L ist genau die extremale Modulform und insbesondere eindeutig bestimmt. Man kann wieder beweisen, dass für großes Gewicht k, ($k > 20500$) der Koeffizient a^*_{2a+4} in der extremalen Modulform negativ wird (Mallows, Odlysko, Sloane: Upper bounds for modulare forms, lattices and codes, J. Algebra 68-76 (1975)). Also gibt es wieder nur endlich viele extremale gerade unimodulare Gitter. In durch 24 teilbaren Dimensionen kennt man bisher 4 solcher Gitter, das Leech Gitter Λ_{24} und 3 gerade unimodulare Gitter in Dimension 48 mit Minimum 6, P_{48p}, P_{48q} und P_{48n}. Ebenso wie bei Codes ist 72 die erste Dimension, in der man nicht weiss, ob ein extremales Gitter existiert.

Ende am 3.7.07

8.2 Theta Reihen mit harmonischen Koeffizienten und Designs.

Definition 8.22 *Sei L ein ganzes Gitter, $p \in \mathbb{C} \otimes \mathrm{Harm}_d$ ein harmonisches Polynom. Dann ist*

$$\Theta_{L,p} := \sum_{x \in L} p(x) q^{(x,x)} = \sum_{n=0}^{\infty} \Big(\sum_{x \in L_{=n}} p(x) \Big) q^n$$

die Theta-Reihe von *L zum Polynom p. Hier ist*

$$L_{=n} := \{\ell \in L \mid (\ell, \ell) = n\}.$$

Bemerkung 8.23 *Die Formeln in Abschnitt 6.1 haben nicht wesentlich benutzt, dass die Polynome reelle Koeffizienten haben. So gilt z.B. auch für $\alpha \in \mathbb{C}^n$*

$$\Delta(\rho_\alpha^m) = m(m-1)(\alpha, \alpha)\rho_\alpha^{m-2}$$

wobei $\rho_\alpha(x) = \sum \alpha_i x_i$ wie üblich. Läßt man $\alpha \in \mathbb{C}^n$ zu, so gibt es für $n \geq 2$ (was wir auch im folgenden stets annehmen) unendlich viele isotrope Vektoren $\alpha \in \mathbb{C}^n$ (d.h. $(\alpha, \alpha) = 0$). Für diese ist dann $\rho_\alpha^m \in \mathbb{C} \otimes \mathrm{Harm}_m$.

Satz 8.24 $\mathbb{C} \otimes \mathrm{Harm}_{n,d} = \langle \rho_\alpha^d \mid \alpha \in \mathbb{C}^n, (\alpha, \alpha) = 0 \rangle$.

Beweis. $\supseteq$ ist klar. Um die Umkehrung beweisen wir analog zu Folgerung 6.6. Dazu setzen wir das Skalarprodukt

$$[f, g] := \sum_{i \in T_d} \binom{|i|}{i}^{-1} a_i b_i$$

auf $\mathcal{F}_{n,d}$ zu einem Hermiteschen Skalarprodukt auf $\mathbb{C} \otimes \mathcal{F}_{n,d} = \mathbb{C}[X_1, \ldots, X_n]_d$ fort, durch

$$[f, g] := \sum_{i \in T_d} \binom{|i|}{i}^{-1} a_i \overline{b_i}$$

für $f, g \in \mathbb{C}[X_1, \ldots, X_n]_d$. Wie in Lemma 6.5 zeigt man, dass für $f \in \mathbb{C} \otimes \mathcal{F}_{n,d}$ und $\alpha \in \mathbb{C}^n$ gilt

$$[f, \rho_\alpha^d] = f(\overline{\alpha}).$$

Da mit α auch $\overline{\alpha}$ isotrop ist, genügt es also zu zeigen, dass jedes harmonische Polynom f mit $f(\alpha) = 0$ für alle isotropen $\alpha \in \mathbb{C}^n$ das Nullpolynom ist. Es ist dann aber $f(\alpha) = 0$ wennimmer $\omega(\alpha) = 0$ ist. Also ist f durch ω teilbar. Nach Bemerkung 6.12 ist dann aber $f = 0$. □

Satz 8.25 *(Theta-Transformationsformel) Sei $p \in \mathbb{C} \otimes \mathrm{Harm}_{2d}$, $L \leq \mathbb{R}^n$. Dann ist*

$$\Theta_{L,p}(\frac{-1}{z}) = (\frac{z}{i})^{n/2+2d}(-1)^d \det(L)^{-1/2} \Theta_{L^\#,p}.$$

Beweis. Es ist $\Theta_{L,p_1+p_2} = \Theta_{L,p_1} + \Theta_{L,p_2}$. Also genügt es die Gleichung für Erzeuger von $\mathbb{C} \otimes \mathrm{Harm}_{2d}$ nachzurechnen, d.h. für $p = \rho_\alpha^{2d}$ mit $\alpha \in \mathbb{C}^n$ isotrop. Für

$$f(x) = (\alpha, x)^{2d} \exp(\pi i \frac{-1}{z}(x, x))$$

ist die Fourier Transformierte

$$\hat{f}(y) = (\alpha, y)^{2d}(-1)^d (\frac{z}{i})^{n/2+2d} \exp(\pi i z(y, y)).$$

(Übung). Nach der Poisson Summations Formel folgt dann

$$\sum_{x \in L} (\alpha, x)^{2d} \exp(\pi i \frac{-1}{z}(x, x)) = \det(L)^{-1/2} \sum_{y \in L^\#} (\alpha, y)^{2d}(-1)^d (\frac{z}{i})^{n/2+2d} \exp(\pi i z(y, y))$$

woraus sich die Behauptung ergibt. □

Satz 8.26 *$p \in \mathrm{Harm}_{2d}$, $L \leq \mathbb{R}^n$ gerade unimodular. Dann ist*

$$\Theta_{L,p} \in \mathcal{M}_{n/2+2d}(\mathrm{SL}_2(\mathbb{Z})).$$

Beweis. Klar ist $\Theta_{L,p}(z+1) = \Theta_{L,p}(z)$ für jedes gerade Gitter L. Da n durch 8 teilbar ist, ist $\frac{z}{i}^{n/2+2d}(-1)^d = z^{n/2+2d}$ also $\Theta_{L,p}(-1/z) = z^{n/2+2d}\Theta_{L,p}(z)$. □

Satz 8.27 *Sei $L \leq \mathbb{R}^{24a+8b}$ ein extremales gerades unimodulares Gitter mit $0 \leq b \leq 2$. Dann bilden alle nichtleeren Schichten*

$$L_{=v} := \{\ell \in L \mid (\ell, \ell) = v\}$$

sphärische $11 - 4b$-Designs. Ist $b = 0$ oder $b = 1$, so ist L stark perfekt.

Beweis. Sei p ein harmonisches Polynom homogen vom Grad $10-4b$. Dann ist

$$\Theta_{L,p} = 0 + 0q^2 + \ldots + 0q^{2a} + *q^{2a+2} + \ldots \in \mathcal{M}_{12a+4b+10-4b} = \mathcal{M}_{12a+10}$$

durch Δ^{a+1} teilbar. Δ^{a+1} hat aber Gewicht $12a+12$. Also ist $\Theta_{L,p} = 0$ und damit gilt (Koeffizientenvergleich bei q^v) für jedes $v \in \mathbb{N}$

$$\sum_{\ell \in L_{=v}} p(\ell) = 0.$$

□

Folgerung 8.28 *Sei $L \leq \mathbb{R}^{24a+8b}$ ein extremales gerades unimodulares Gitter mit $b = 0$ oder $b = 1$. Dann ist L stark perfekt und insbesondere extrem.*

8.3 Die Klassifikation der 24-dimensionalen geraden unimodularen Gitter

Satz 8.29 *Sei $L \leq \mathbb{R}^n$ ein gerades unimodulares Gitter, $n = 8, 16, 24$ und $L_2 := \{\ell \in L \mid (\ell, \ell) = 2\}$ sein Wurzelsystem. Dann gilt entweder $L_2 = \emptyset$ oder L_2 enthält eine Basis von $\mathbb{R}^n$. Weiter haben die irreduziblen Komponenten des von L_2 erzeugten Wurzelgitters alle die gleiche Coxeter Zahl $h = \frac{|L_2|}{n}$.*

Beweis. Sei $p := P_\alpha^{(2)} := \rho_\alpha^2 - \frac{(\alpha,\alpha)}{n}\omega \in \mathrm{Harm}_2$ mit $0 \neq \alpha \in \mathbb{R}^n$ beliebig. Dann ist

$$\Theta_{L,p} \in \mathcal{S}_{n/2+2} = \{0\}$$

da $n/2 + 2 = 6, 10, 14$ ist. Insbesondere gilt

$$\sum_{x \in L_2} (x, \alpha)^2 = \frac{2|L_2|(\alpha, \alpha)}{n}$$

und L_2 ist ein sphärisches 2-Design. Daher ist entweder $L_2 = \emptyset$ oder $L_2^\perp = \{0\}$. Ausserdem gilt für jede irreduzible Komponente R von L_2 und $\alpha \in \langle R \rangle_\mathbb{R}$, dass

$$\sum_{x \in L_2} (x, \alpha)^2 = \sum_{x \in R} (x, \alpha)^2 = 2h(\alpha, \alpha) = \frac{2|L_2|(\alpha, \alpha)}{n}$$

wobei h die Coxeter Zahl von R ist (vgl. Satz 6.40 (c)). □

Folgerung 8.30 *Sei L ein gerades unimodulares Gitter der Dimension n und $R = \langle L_2 \rangle_\mathbb{Z}$ sein Wurzelteilgitter.*

$n = 8$ *Dann ist $L = R \cong \mathbb{E}_8$.*

$n = 16$ *Dann ist entweder $L = R \cong \mathbb{E}_8 \perp \mathbb{E}_8$ oder $R \cong \mathbb{D}_{16}$ und $L \cong \mathbb{D}_{16}^+$.*

$n = 24$ *Dann ist R entweder gleich 0 oder eines 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. Für $n = 8$ und $n = 16$ sind die Gitter L extremal. Insbesondere ist $|L_2| = 240$ bzw. 480 eindeutig bestimmt. $\mathbb{E}_8$ bze. $2\mathbb{E}_8$ und $\mathbb{D}_{16}$ sind die einzigen Wurzelgitter der Dimension 8 bzw. 16 mit dieser Anzahl von Wurzeln. Die Gitter $\mathbb{E}_8$ und $\mathbb{E}_8 \perp \mathbb{E}_8$ sind schon unimodular. Ist L gerade, unimodular mit $L_2 = \mathbb{D}_{16}$, so ist $\mathbb{D}_{16} \leq L \leq \mathbb{D}_{16}^{\#}$. Da $\mathbb{D}_{16}^{\#}/\mathbb{D}_{16} \cong C_2 \times C_2$ ist, findet man genau 3 Obergitter. Diese sind alle unimodular, eines davon ist $\mathbb{Z}^{16}$ (also nicht gerade), die anderen beiden sind beide isometrisch zu $\mathbb{D}_{16}^{+}$.
Für $n = 24$ ist die im Satz angegebene Liste die Liste aller möglichen Wurzelsysteme vom Rang 24, deren irreduzible Komponenten alle die gleiche Coxeterzahl haben. □

irreduzible Wurzelgitter

Gitter L	$\lvert R(L)\rvert$	$h(L)$	$\det(L)$	$L^{\#}/L$	Dimension n
$\mathbb{A}_n$	$n(n+1)$	$n+1$	$n+1$	$\mathbb{Z}/(n+1)\mathbb{Z}$	≥ 1
$\mathbb{D}_n$	$2n(n-1)$	$2(n-1)$	4	$\mathbb{Z}/4\mathbb{Z}$	≥ 4, ungerade
$\mathbb{D}_n$	$2n(n-1)$	$2(n-1)$	4	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	≥ 4, gerade
$\mathbb{E}_6$	72	12	3	$\mathbb{Z}/3\mathbb{Z}$	6
$\mathbb{E}_7$	126	18	2	$\mathbb{Z}/2\mathbb{Z}$	7
$\mathbb{E}_8$	240	30	1	1	8

mögliche Wurzelsysteme R eines 24-dimensionalen geraden unimodularen Gitters

R	$h(R_i)$	$\lvert R\rvert$	R	$h(R_i)$	$\lvert R\rvert$
$\emptyset$		0	$24\mathbb{A}_1$	2	48
$12\mathbb{A}_2$	3	72	$8\mathbb{A}_3$	4	96
$6\mathbb{A}_4$	5	120	$4\mathbb{A}_6$	7	168
$3\mathbb{A}_8$	9	216	$2\mathbb{A}_{12}$	13	312
$\mathbb{A}_{24}$	25	600	$6\mathbb{D}_4$	6	144
$4\mathbb{D}_6$	10	240	$3\mathbb{D}_8$	14	336
$2\mathbb{D}_{12}$	22	528	$\mathbb{D}_{24}$	46	1106
$4\mathbb{E}_6$	12	288	$3\mathbb{E}_8$	30	720
$4\mathbb{A}_5 + \mathbb{D}_4$	6	144	$2\mathbb{A}_7 + 2\mathbb{D}_5$	8	192
$2\mathbb{A}_9 + \mathbb{D}_6$	10	240	$\mathbb{A}_{15} + \mathbb{D}_9$	16	384
$\mathbb{E}_8 + \mathbb{D}_{16}$	30	720	$2\mathbb{E}_7 + \mathbb{D}_{10}$	18	432
$\mathbb{E}_7 + \mathbb{A}_{17}$	18	432	$\mathbb{E}_6 + \mathbb{D}_7 + \mathbb{A}_{11}$	12	288

Satz 8.31 *Zu jedem der 23 in Folgerung 8.30 angegebene Wurzelgitter R vom Rang 24 gibt es bis auf Isometrie genau ein gerades unimodulares Gitter L mit $\langle L_2\rangle_{\mathbb{Z}} = R$.*

Der Beweis basiert auf der folgenden Beobachtung: Ist $R \leq L = L^{\#} \leq R^{\#}$, L gerade, so ist $L/R \leq R^{\#}/R$ eine isotrope Untergruppe der Diskriminantengruppe.

Definition 8.32 *Sei R ein gerades Gitter. Dann induziert das Skalarprodukt eine symmetrische Bilinearform*

$$b_R : R^{\#}/R \times R^{\#}/R \to \mathbb{Q}/\mathbb{Z}, (x+R, y+R) \mapsto (x,y) + \mathbb{Z}$$

sowie eine quadratische Form

$$q_R : R^{\#}/R \to \mathbb{Q}/2\mathbb{Z}, x + R \mapsto (x,x) + 2\mathbb{Z}.$$

Die endliche abelsche Gruppe $(R^{\#}/R, b_R, q_R)$ zusammen mit diesen Formen nennen wir Diskriminantengruppe. *Eine Untergruppe $U \leq R^{\#}/R$ heißt* isotrop, *falls $q_R(U) = \{0\}$ und $b_R(u,u') = 0$ für alle $u, u' \in U$. Die* Orthogonalgruppe *einer Untergruppe $U \leq R^{\#}/R$ ist*

$$U^{\perp} := \{v \in R^{\#}/R \mid b_R(v,u) = 0 \text{ für alle } u \in U\}.$$

Bemerkung 8.33 *Nach dem Homomorphiesatz entsprechen sich Untergruppen $U \leq R^{\#}/R$ und Zwischengitter $R \leq L \leq R^{\#}$. Dabei ist L gerade, genau dann wenn L/R isotrop und $(L/R)^{\perp} = L^{\#}/R$. Insbesondere entsprechen den geraden unimodularen Obergittern L von R genau die isotropen selbstorthogonalen Untergruppen $U = U^{\perp}$ von $R^{\#}/R$.*

Da $R^{\#}/R$ immer endlich ist, ist der Beweis von Satz 8.31 ein algorithmisch sehr leicht lösbares Problem. Man bestimmt alle isotropen $U = U^{\perp} \leq R^{\#}/R$ und deren Urbilder $L = L^{\#}$, gerade und prüft dann, welche L genau R als Wurzelgitter haben.

Beispiel 8.34 *Sei $R = \mathbb{A}_{24}$. Dann ist $\mathbb{A}_{24}^{\#}/\mathbb{A}_{24} \cong C_{25}$ zyklisch, hat also genau eine isotrope Untergruppe $U = U^{\perp}$. Sei L das entsprechende gerade unimodulare Gitter. Dann erzeugt L_2 ein irreduzibles Wurzelgitter, das $\mathbb{A}_{24}$ enthält, also entweder $= \mathbb{A}_{24}$ ist oder $= L$. Letzter Fall ist ausgeschlossen, da es kein irreduzibles unimodulares Wurzelgitter der Dimension 24 gibt.*

Beispiel 8.35 *Sei $R = 24\mathbb{A}_1$. Dann ist $R^{\#}/R \cong C_2^{24}$ und jedes gerade unimodulare Obergitter L von R entspricht einem doppelt geraden, selbstdualen Code $L/R =: C \leq \mathbb{F}_2^{24}$. Damit das Wurzelteilgitter von L gleich R ist, darf C keine Worte vom Gewicht 4 enthalten. Also ist $d(C) = 8$ und wegen Satz 7.26 und 7.27 ist also C der Golay Code und daher L bis auf Isometrie eindeutig bestimmt.*

Beispiel 8.36 *Sei $R = 2\mathbb{D}_{12}$. Dann ist $\mathbb{D}_{12} \leq \mathbb{Z}^{12} = \langle e_1, \ldots, e_{12} \rangle$ mit ON-Basis $(e_1, \ldots, e_{12})$ und $\mathbb{D}_{12}^{\#}/\mathbb{D}_{12} = \langle e_1 + \mathbb{D}_{12} =: x_1, \frac{1}{2}\sum_{i=1}^{12} e_i + \mathbb{R}_{12} = x_2 \rangle$. Es ist $b(x_1, x_2) = \frac{1}{2}$ und $q(x_1) = q(x_2) = 1 = q(x_1 + x_2)$. Setzt man $x3 := x_1 + x_2$, und bezeichnen x_i' die entsprechenden Vektoren in der 2. Komponente, so sind die isotropen Vektoren in $R^{\#}/R$ gleich $x_i + x_j'$ mit $1 \leq i, j \leq 3$. Es gibt einen Automorphismus von D_{12}, der die Klassen x_2 und x_3 vertauscht. Da $\mathbb{D}_{12}^{\#}/\mathbb{D}_{12}$ keine isotropen Vektor $\neq 0$ enthält ist L/R ein volles subdirektes Produkt (die Projektion auf jede Komponente ist surjektiv). Also können wir Œ annehmen, dass $x_1 + x_j'$ und $x_2 + x_k'$ in L/R liegen. Da $b(x_1 + x_j', x_2 + x_k') = \frac{1}{2} + b(x_j', x_k')$ ist, muss also $b(x_j', x_k') = \frac{1}{2}$*

sein, was einfach nur bedeutet, dass $j \neq k$. Man findet bis auf Operation von $\mathrm{Aut}(\mathbb{D}_{12} \perp \mathbb{D}_{12})$, *(also Vertauschen der beiden Komponenten und unabhängigem Vertauschen von x_2, x_3 und x_2', x_3') dass*

$$L/R = \langle x_1 + x_1', x_2 + x_2' \rangle \text{ oder } \langle x_1 + x_2', x_2 + x_1' \rangle.$$

Im ersten Fall liegt $e_1 + e_1' \in L_2$ und daher wird das Wurzelsystem von L größer (gleich $\mathbb{D}_{24}$). Das andere Gitter L ist gerade, unimodular mit Wurzelsystem $2\mathbb{D}_{12}$.

Übung: $R = \mathbb{D}_{24}$ liefert $L = \mathbb{D}_{24}^+ = \langle \mathbb{D}_{24}, \frac{1}{2}\sum e_i \rangle$, $R = \mathbb{E}_8 + \mathbb{D}_{16}$ liefert $L = \mathbb{E}_8 + \mathbb{D}_{16}^+$. Wie sehen die geraden unimodularen Obergitter von $R = 2\mathbb{A}_{12}$, $4\mathbb{A}_6$ und $2\mathbb{E}_7 + \mathbb{D}_{10}$ aus?

Folgerung 8.37 *Sei $C = C^\perp \leq \mathbb{F}_2^{24}$ doppelt gerade. Dann ist das Codegitter L_C eines der 9 unimodularen geraden Gitter mit Wurzelteilgitter*

$$24\mathbb{A}_1, 6\mathbb{D}_4, 4\mathbb{D}_6, 3\mathbb{D}_8, 2\mathbb{D}_{12}, \mathbb{D}_{24}, 3\mathbb{E}_8, \mathbb{E}_8 + \mathbb{D}_{16}, 2\mathbb{E}_7 + \mathbb{D}_{10}.$$

Beweis. Das Wurzelteilgitter R von L_C muss das Wurzelsystem $24\mathbb{A}_1$ enthalten. Insbesondere sind alle irreduziblen Komponenten von R nach Satz 2.20 von der Form $\mathbb{A}_1$, $\mathbb{D}_n$ mit $n \geq 4$ gerade, $\mathbb{E}_7$ oder $\mathbb{E}_8$. Geht man durch die Liste der möglichen Wurzelsysteme gerader unimodularer Gitter in Dimension 24 in Satz 8.31, so findet man genau die 9 angegebenen Wurzelsysteme. □

Bemerkung 8.38 *Es gibt genau 9 selbstduale doppelt gerade Codes der Länge 24 und diese liefern genau die 9 verschiedenen Codegitter von Folgerung 8.37. Jedoch folgt im allgemeinen nicht aus $L_C \cong L_{C'}$, dass $C \cong C'$.*

8.4 Eindeutigkeit des Leech Gitters.

Satz 8.39 *Sei $L \leq \mathbb{R}^{24}$ ein extremales gerades unimodulares Gitter. Dann ist $L \cong \Lambda_{24}$.*

Definition 8.40 *(M. Kneser) Seien $L, M \leq \mathbb{R}^n$ volle Gitter. Dann heissen L und M* benachbart*, falls*

$$[L : L \cap M] = [M : L \cap M] = 2.$$

Lemma 8.41 *Sei L ein gerades unimodulares Gitter und M ein gerader Nachbar von L. Dann gibt es $u \in L$ mit $(u, u) \in 8\mathbb{Z}$ und*

$$M = L^u = L_u \dot\cup (\frac{u}{2} + L_u)$$

wobei $L_u = \{\ell \in L \mid (u, \ell) \in 2\mathbb{Z}\}$. Umgekehrt ist jedes solche L^u ein gerader unimodularer Nachbar von L.

Beweis. Sei M so ein gerader Nachbar. Dann ist M ganz und $\det(M) = \det(L) = 1$, also M unimodular. Das Teilgitter $L_1 := M \cap L$ ist der Kern eines Epimorphismus von $\varphi : L \to \mathbb{Z}/2\mathbb{Z}$. Da L frei abelsche Gruppe ist, gibt es $\tilde{\varphi} \in \mathrm{Hom}(L, \mathbb{Z})$ mit $\varphi(\ell) = \tilde{\varphi}(\ell) + 2\mathbb{Z}$ für alle $\ell \in L$. Also gibt es ein $v \in L^{\#} = L$ so dass $\varphi(\ell) = (v, \ell) + 2\mathbb{Z}$, also $L_1 = L_v$. Klar ist $L_v = L_w$ genau dann wenn $v + w \in 2L$. Die unimodularen Gitter zwischen $L_1^{\#}$ und L_1 sind gerade von der Form $M = L_1 \dot{\cup} x + L_1$ für ein $x \in L_1^{\#} \subset \frac{1}{2}L$. Also ist $x = \frac{u}{2}$ für ein $u \in L - 2L$. Da M gerade ist, ist $\frac{1}{4}(u, u) \in 2\mathbb{Z}$ also $(u, u) \in 8\mathbb{Z}$. Da M ganz ist, ist $\frac{1}{2}(u, y) \in \mathbb{Z}$ für alle $y \in L_1$. Also ist $L_1 = L_u$ und $M = L^u$. □

Beweis. (von Satz 8.39) Sei $L \leq \mathbb{R}^{24}$ ein extremales gerades unimodulares Gitter. Dann ist $\Theta_L = \Theta_{\Lambda_{24}}$, insbesondere gibt es ein $u \in L$ mit $(u, u) = 8$. Wir betrachten das Gitter $M := L^u$. Dann ist M ein gerades unimodulares Gitter mit $\min(M) = 2$, da $\frac{u}{2} \in M_{=2}$.

Behauptung: Das Wurzelsystem von M ist $24\mathbb{A}_1$. Denn sonst gibt es $x, y \in M_{=2}$ mit $(x, y) = 1$. Da x und y nicht in L_u liegen gilt $x - y \in L_u$ ein Widerspruch da $(x - y, x - y) = 2 < \min(L_u)$.

Also ist $M = L_{\mathcal{G}_{24}}$ das Codegitter zum Golay Code.

Wir wissen also, dass L ein Nachbar von $M := L_{\mathcal{G}_{24}}$ ist. Es gibt also ein $u \in M$ mit $L = M^u = M_1 \cup (\frac{u}{2} + M_1)$ wo $M_1 = \{x \in M \mid (x, u) \in 2\mathbb{Z}\}$. Dann ist $u = \sum_{i=1}^{24} u_i e_i$ für die Orthogonalbasis $(e_1, \ldots, e_{24})$ mit $(e_i, e_i) = 1/2$. Da $\min(M_1) \geq \min(L) = 4$ ist, sind alle u_i ungerade (da $2e_i \notin M_1$). Die Spiegelung σ_i entlang $2e_i$ ist ein Automorphismus von M und bildet e_j auf $(-1)^{\delta_{ij}} e_j$ ab. Also können wir Œ annehmen dass $u_i \equiv 1 \pmod 4$ für alle i. Da $4e_i + 4e_j \in 2M_1$ und insbesondere $8e_i \in 2M_1$ können wir weiter annehmen dass $u_i = 1$ für alle $2 \leq i \leq 24$ und $u_1 \in \{1, 5\}$. Ist $u = \sum_{i=1}^{24} e_i$, so ist $(u/2, u/2) = 3$ ein Widerspruch dazu, dass L gerade ist. Also ist $u = 5e_1 + \sum_{i=2}^{24} e_i$ und dass Gitter $L = M^u$ genau das in 7.28 konstruierte Gitter. □

8.5 Ungerade unimodulare Gitter.

Bemerkung 8.42 *Ist L ein ganzes Gitter, so ist die quadratische Form $L \to \mathbb{Z}/2\mathbb{Z}, v \mapsto (v,v) + 2\mathbb{Z}$ eine lineare Abbildung. Insbesondere gibt es für unimodulare Gitter $L = L^\#$ ein $c \in L$ mit $(v,v) \equiv_2 (c,v)$ für alle $v \in L$. Der Vektor c ist modulo $2L$ eindeutig bestimmt.*

Definition 8.43 *Sei $L = L^\#$ ein unimodulares Gitter. Dann heißt jeder Vektor $c \in L$ mit $(c,v) \equiv_2 (v,v)$ für alle $v \in L$ ein* charakteristischer Vektor *von L und die Klasse $c + 2L$ die* kanonische Klasse *von L.*

Bemerkung 8.44 *Sind c und $c' = c + 2v$ zwei charakteristische Vektoren des unimodularen Gitters L, so ist*

$$(c',c') = (c,c) + 4(c,v) + 4(v,v) \equiv_8 (c,c).$$

Die Normen von charakteristischen Vektoren sind also kongruent modulo 8.

Beispiel: $L = \mathbb{Z}^n$ hat charakteristischen Vektor $c = \sum_{i=1}^n e_i$ mit Norm $(c,c) = n$. Also haben alle charakteristischen Vektoren von $\mathbb{Z}^n$ Norm $\equiv_8 n$.

Bemerkung 8.45 *(a) Ein unimodulares Gitter L ist gerade, genau dann wenn 0 ein charakteristischer Vektor ist.*
(b) Sei $M = M^\#$ ein ungerades unimodulares Gitter und $M_0 := \{m \in M \mid (m,m) \in 2\mathbb{Z}\}$ sein gerades Teilgitter. *Ist $c \in M$ ein charakteristischer Vektor, so ist $\frac{c}{2} \in M_0^\# = M \dot\cup (\frac{c}{2} + M)$. Die Menge aller halben charakteristischen Vektoren ist also genau $M_0^\# - M$. Diese Menge nennt man auch den* Schatten *von M .*

Satz 8.46 *Sei $M = M^\# \leq \mathbb{R}^n$ und c ein charakteristischer Vektor von M. Dann ist die Theta Reihe des Schattens von M gleich*

$$\Theta'_M := \Theta_{c/2+M} = \Theta_{M_0^\#} - \Theta_M = (z/i)^{-n/2}\Theta_M(1 - \frac{1}{z}).$$

Weiter gilt

$$\Theta'_M(z+1) = \exp(\pi i n/4)\Theta'_M(z).$$

Beweis. Es ist

$$\Theta_{M_0}(z) = \frac{1}{2}(\Theta_M(z) + \Theta_M(1+z))$$

und daher nach der Theta-Transformationsformel

$$\Theta_{M_0^\#}(z) = \det(M_0)^{1/2}(z/i)^{-n/2}\frac{1}{2}(\Theta_M(\frac{-1}{z}) + \Theta_M(1 - \frac{1}{z})) = \Theta_M(z) + (z/i)^{-n/2}\Theta_M(1 - \frac{1}{z})$$

woraus die erste Behauptung folgt. Es gilt also

$$\Theta_M((TS(z))) = (z/i)^{n/2}\Theta'_M(z)$$

und daher (da $TST = ST^{-1}S$)

$$(\frac{z+1}{i})^{n/2}\Theta'_M(z+1) = \Theta_M(TS(z+1)) = \Theta_M(TST(z)) = \Theta_M(ST^{-1}S(z))$$

$$= \big(\frac{T^{-1}S(z)}{i}\big)^{n/2}\Theta_M(T^{-1}S(z)) == \big(\frac{-1/z-1}{i}\big)^{n/2}\Theta_M(TS(z)) = \big(\frac{(z+1)i}{z}\big)^{n/2}(z/i)^{n/2}\Theta'_M(z)$$

also

$$\Theta'_M(z+1) = i^{n/2}\Theta'_M(z).$$

□

Folgerung 8.47 *Ist c ein charakteristischer Vektor eines n-dimensionalen Gitters M, so ist $(c,c) \equiv_8 n$.*

Beweis. Es ist

$$\Theta'_M(z+1) = \sum_{\frac{c'}{2} \in \frac{c}{2}+M_0} \exp(\pi i/4(c',c')(z+1)) = \exp(\pi i/4(c,c))\Theta'_M(z) = \exp(\pi i/4)^n\Theta'_M(z).$$

Also ist $(c,c) \equiv_8 n$. □

Folgerung 8.48 *Sei M ein ungerades unimodulares Gitter der Dimension n und M_0 sein gerades Teilgitter. Dann gilt:*
(a) Ist n ungerade, so ist $M_0^\#/M_0 \cong C_4$ und ist n gerade, so ist $M_0^\#/M_0 \cong C_2 \times C_2$.
(b) Ist n durch 4 teilbar so sind die 3 Gitter zwischen $M_0^\#$ und M_0 alle unimodular.
(c) Ist n sogar durch 8 teilbar, so sind die beiden Gitter $\neq M$ zwischen $M_0^\#$ und M_0 gerade und unimodular.

Beweis. Sei c ein charakteristischer Vektor. Dann ist $M_0^\# = M \dot\cup \frac{c}{2} + M$. Ist n ungerade, so ist (c,c) auch ungerade und daher hat $\frac{c}{2} + M_0$ Ordnung 4 in $M_0^\#/M_0$.
Sei nun n gerade und $u \in M - M_0$. Dann sind M, $X := \langle \frac{c}{2}, M_0\rangle$, $Y := \langle u + \frac{c}{2}, M_0\rangle$ die 3 Gitter zwischen M_0 und $M_0^\#$. Insbesondere ist $M_0^\#/M_0 \cong C_2 \times C_2$.
Außerdem ist

$$(u + \frac{c}{2}, u + \frac{c}{2}) = \frac{1}{4}(c,c) + (u,c) + (u,u) \equiv \frac{1}{4}(c,c) \pmod{2\mathbb{Z}}.$$

Also sind die Gitter X, Y ganz, genau dann wenn $\frac{1}{4}(c,c)$ ganz ist, also n durch 4 teilbar und gerade, genau dann wenn n durch 8 teilbar ist. □

Beispiel:
Sei $M = \mathbb{Z}^n = \langle e_i \mid 1 \le i \le n\rangle$, $M_0 = \mathbb{D}_n$. Dann hat $\mathbb{D}_n$ genau dann 2 weitere unimodulare Obergitter

$$\mathbb{D}_n^+ := \langle e_i + e_j, \frac{1}{2}\sum_{k=1} e_k \mid 1 \le i,j \le n\rangle \text{ und } \mathbb{D}_n^- := \langle e_i + e_j, \frac{1}{2}\sum_{k=1} e_k - e_1 \mid 1 \le i,j \le n\rangle$$

wenn n durch 4 teilbar ist. Die Spiegelung entlang e_1 bildet $\mathbb{D}_n^+$ auf $\mathbb{D}_n^-$ ab. Die beiden Gitter sind gerade, genau dann wenn n durch 8 teilbar ist. Es ist $\mathbb{D}_8^+ \cong \mathbb{E}_8$.

Folgerung 8.49 *Ist n durch 8 teilbar, so stehen die Paare (L_1, L_2) benachbarter gerader unimodularer Gitter in Bijektion zu den ungeraden unimodularen Gittern.*

Beispiel. Die ungeraden unimodularen Gitter in Dimension 8 sind alle isometrisch zu $\mathbb{Z}^8$.

Beweis. Das einzige gerade unimodulare Gitter in Dimension 8 ist $\mathbb{E}_8$. Wir müssen jetzt alle Nachbarn von $\mathbb{E}_8$ finden. $\mathrm{Aut}(\mathbb{E}_8) \cong 2.O_8^+(2)$ operiert transitiv auf den Klassen $v + 2\mathbb{E}_8$ in $\mathbb{E}_8/2\mathbb{E}_8$ mit $4 \mid (v, v)$. Also hat $\mathbb{E}_8$ genau einen Nachbarn, das zugehörige ungerade Gitter muss dann das bekannte unimodulare Gitter $\mathbb{Z}^8$ sein. □

Beispiel Es gibt 6 ungerade unimodulare Gitter in Dimension 16. L_{16} (mit Minimum 2), $\mathbb{Z} \perp L_{15}$, $\mathbb{Z}^2 \perp L_{14}$, $\mathbb{Z}^4 \perp \mathbb{D}_{12}^+$, $\mathbb{Z}^8 \perp \mathbb{E}_8$ und $\mathbb{Z}^{16}$.

Beweis. $\mathrm{Aut}(\mathbb{E}_8)$ hat ein Bahn auf den isotropen Klassen $v + 2\mathbb{E}_8$ mit $(v, v) \in 4\mathbb{Z}$ und eine Bahn auf den anisotropen Klassen $w + 2\mathbb{E}_8$ mit $(w, w) \equiv_4 2$. Die isotropen Klassen von $\mathbb{E}_8 \perp \mathbb{E}_8/2(\mathbb{E}_8 \perp \mathbb{E}_8)$ (modulo der Operation der Automorphismengruppe) werden vertreten durch $(v, 0)$, (v, v) und (w, w), liefern Nachbarn $\mathbb{E}_8 \perp \mathbb{E}_8$, $\mathbb{E}_8 \perp \mathbb{E}_8$, $\mathbb{D}_{16}^+$, und ungerade Nachbarn $\mathbb{Z}^8 \perp \mathbb{E}_8$, $\mathbb{Z}^2 \perp L_{14}$, bzw. L_{16}. Das Gitter $\mathbb{D}_{16}^+$ hat 4 Nachbarn (modulo der Operation der Automorphismengruppe), einer davon ist $\mathbb{E}_8 \perp \mathbb{E}_8$ und liefert das ungerade Gitter L_{16}, die anderen 3 sind isometrisch zu $\mathbb{D}_{16}^+$ und liefern die 3 Gitter $\mathbb{Z} \perp L_{15}$, $\mathbb{Z}^4 \perp \mathbb{D}_{12}^+$ sowie $\mathbb{Z}^{16}$. □

Bemerkung 8.50 *Dieselbe Strategie hat R. Borcherds benutzt, um die ungeraden unimodularen Gitter in Dimension 24 zu klassifizieren. Es gibt insgesamt 297 unimodulare Gitter in Dimension 24, 24 davon sind gerade, 273 sind ungerade. Enthält ein unimodulares Gitter M einen Vektor v mit $(v, v) = 1$, so ist $M = \langle v \rangle \perp M' \cong \mathbb{Z} \perp M'$ für ein unimodulares Gitter M'. Zählt man nur die ungeraden unimodularen Gitter, die keinen Vektor der Norm 1 enthalten, so findet man $273 - 117 = 156$ ungerade unimodulare Gitter in Dimension 24 mit Minimum 2 oder Minimum 3. Nur eines dieser Gitter hat Minimum 3, das sogenannte* ungerade Leech-Gitter *O_{24} dessen gerade Nachbarn beide isometrisch zum Leech-Gitter Λ_{24} sind.*
In Dimension 25 gibt es 665 unimodulare Gitter. In grösseren Dimensionen sind diese noch nicht klassifiziert.

Index