

Additive Zerlegungen von Gittern

Additive decompositions of lattices

BACHELORARBEIT

vorgelegt der
FAKULTÄT FÜR MATHEMATIK, INFORMATIK
UND NATURWISSENSCHAFTEN

angefertigt am
LEHRSTUHL B FÜR MATHEMATIK
RWTH AACHEN UNIVERSITY

von
SIMON EISENBARTH
aus Odenthal

betreut von
PROF. DR. WILHELM PLESKEN

im September 2014

Inhaltsverzeichnis

1 Grundlagen und Notation	5
1.1 Gitter	5
1.2 Zusammenhang von Gittern und quadratischen Formen	8
2 Einbettung euklidischer Gitter in $\mathbb{Z}_{\text{orth}}^k$	10
2.1 Der Algorithmus SIB	10
2.2 Transversalen der Automorphismengruppe auf den Einbettungen	15
3 Additive Zerlegungen von Gittern	20
3.1 Grundlagen	20
3.2 Ergebnisse	26
3.2.1 Teilgitter von E_6 , E_7 und E_8	27
3.2.2 Konstruktion von Blockformen	30
3.2.3 Obergitter additiv unzerlegbarer Gitter	36
3.2.4 Skalierung von Basisvektoren	37
3.2.5 Konstruktion von Gittern mit gegebener Determinante	38
3.2.6 Teilgitter additiv unzerlegbarer Gitter	39
4 Anhang	41

Einleitung

Ganzzahlige Gitter stehen im engen Zusammenhang zu ganzzahligen quadratischen Formen. Eine quadratische Form, die als Summe zweier positiv semidefiniter, ganzzahliger quadratischer Formen ungleich Null geschrieben werden kann, heißt additiv zerlegbar. Dies kann benutzt werden um die additive Zerlegbarkeit von Gitter zu untersuchen, da die Isometrieklassen additiv unzerlegbarer, ganzzahliger Gitter zu den $GL_n(\mathbb{Z})$ -Bahnen auf der Menge der additiv unzerlegbaren, ganzzahligen quadratischen Formen in Bijektion stehen. Es existieren bis auf Isometrie für jede Dimension n nur endlich viele additiv unzerlegbare, ganzzahlige Gitter. C. Ko zeigte bereits 1942, dass jedes solche Gitter bis zur Dimension 8 isometrisch zu \mathbb{Z} , E_6 , E_7 oder E_8 ist (vgl. [Ko37], [Ko39], [Ko42b], [Ko42a]). J. Opgenorth zeigte 1992, dass es in Dimension 9 nur 2 Isometrieklassen additiv unzerlegbarer Gitter gibt. In den Dimensionen 10 und 11 fand er 7 bzw. 13 solcher Isometrieklassen und bewies, dass bis Determinante 100 keine weiteren existieren. In dieser Arbeit werden additiv unzerlegbare, ganzzahlige Gitter in höheren Dimensionen berechnet, wobei der Schwerpunkt in Dimension 12 liegt.

Die Arbeit gliedert sich in 4 Kapitel:

Im ersten Kapitel werden die wichtigsten Definitionen und Begriffe aus der Gittertheorie eingeführt. Zusätzlich wird der Zusammenhang zwischen n -dimensionalen ganzzahligen Gittern und n -dimensionalen ganzzahligen quadratischen Formen beschrieben.

Im zweiten Kapitel wird der Algorithmus aus [Ple95] von W. Plesken vorgestellt. Für eine ganzzahlige Matrix $A \in \mathbb{Z}^{n \times n}$, welche symmetrisch und positiv definit ist, lassen sich hiermit alle $k \in \mathbb{N}$ und alle $X \in \mathbb{Z}^{n \times k}$ finden mit $A = XX^{\text{tr}}$. Interpretiert man A als ganzzahliges Gitter, so bilden die Zeilen einer Lösung dieser Gleichung die Basis eines Teilgitters des k -dimensionalen orthonormalen Standardgitters, welches zu A isometrisch ist. Häufig liefert der Algorithmus allerdings verschiedene Basen für dasselbe Teilgitter. Es zeigt sich, dass die Automorphismengruppe von A auf den gefundenen Lösungen operiert und die Bahnen aus genau den Matrizen bestehen, deren Zeilen dasselbe \mathbb{Z} -Erzeugnis haben. Mit Hilfe von Stabilisator Ketten wird der Algorithmus so verändert, dass direkt ein Vertretersystem ausgegeben wird. In die schon bestehende Implementierung des Algorithmus wurde die Option eingefügt, zusätzlich bei der Berechnung der Lösungen die Automorphismengruppe zu benutzen.

Im dritten Kapitel wird die additive Zerlegung von ganzzahligen Gittern betrachtet. Zu-

sätzlich zu den schon bekannten Kriterien wird eine Methode entwickelt, wie man das duale Gitter benutzen kann, um zu zeigen, dass ein Gitter additiv zerlegbar ist. Positiv semidefinite, symmetrische, ganzzahlige Matrizen A , für die $A - YY^{\text{tr}}$ indefinit ist für jedes $Y \in \mathbb{Z}^n$, werden Blockformen genannt. In der Implementierung von dem in Kapitel 2 beschriebenen Algorithmus wurde zusätzlich die Möglichkeit eingefügt, für ein gegebenes A alle möglichen Blockformen der Gestalt $A - XX^{\text{tr}}$ auszugeben. Hiermit ist es möglich aus schon bekannten Gittern additiv unzerlegbare Gitter zu konstruieren, die genaue Vorgehensweise wird ebenfalls in diesem Kapitel beschrieben. Insgesamt wurden 68 additiv unzerlegbare Gitter gefunden, davon alleine 29 in Dimension 12. Im vierten Kapitel sind Gram-Matrizen aller gefunden additiv unzerlegbaren Gitter angegeben.

Mein Dank gilt Herrn Professor Dr. W. Plesken für die Themenstellung und die sehr gute Betreuung, insbesondere in den letzten Wochen vor der Abgabe, Herrn Martin Leuner für die Hilfestellung bei der Implementierung der Algorithmen und nicht zuletzt meinem Vater, der mir das Studium der Mathematik ermöglicht hat.

1 Grundlagen und Notation

1.1 Gitter

In diesem Abschnitt werden grundlegende Definitionen und Begriffe aus der Gittertheorie eingeführt, welche im Folgenden benutzt werden.

Definition 1.1 (i) Sei $E = (\mathcal{V}, \phi)$ ein euklidischer Vektorraum. (L, ϕ) heißt Gitter in \mathcal{V} , falls ein linear unabhängiges Tupel $B = (b_1, \dots, b_n) \in \mathcal{V}^n$ existiert, mit

$$L = \langle b_1, \dots, b_n \rangle_{\mathbb{Z}} = \left\{ \sum_{i=1}^n a_i b_i \mid a_i \in \mathbb{Z} \right\}.$$

L ist also ein freier \mathbb{Z} -Modul in \mathcal{V} . B heißt dann Gitterbasis und $n = \dim(L, \phi)$ die Dimension von (L, ϕ) . (L, ϕ) heißt volles Gitter in \mathcal{V} , falls B eine Basis von \mathcal{V} ist.

(ii) Die Matrix $\mathcal{G}(B) = (\phi(b_i, b_j))_{1 \leq i, j \leq n} \in \mathbb{R}^{n \times n}$ heißt Gram-Matrix von (L, ϕ) bezüglich der Basis B .

Lemma 1.2 Sei (L, ϕ) ein Gitter mit Gitterbasis B . Die Determinante $\det(L, \phi) := \det(\mathcal{G}(B))$ ist unabhängig von der Gitterbasis und heißt die Determinante des Gitters (L, ϕ) .

BEWEIS Sei $B' = (b'_1, \dots, b'_n)$ eine weitere Gitterbasis von (L, ϕ) . Dann gilt $\mathcal{G}(B') = {}_B \text{id}_{B'} \mathcal{G}(B) ({}_{B'} \text{id}_B)^{\text{tr}}$. Da sowohl ${}_B \text{id}_{B'}$ und $({}_{B'} \text{id}_B)^{-1} = {}_{B'} \text{id}_B$ ganzzahlige Matrizen sind, gilt $\det({}_B \text{id}_{B'}) = \pm 1$, also $\det(\mathcal{G}(B')) = \det(\mathcal{G}(B))$. \square

Lemma 1.3 Sei (L, ϕ) ein volles Gitter in (\mathcal{V}, ϕ) mit Gitterbasis B . Für jedes $s \in \mathbb{R}$ ist dann

$$L_{\leq s} := \{l \in L \mid \phi(l, l) \leq s\}$$

eine endliche Menge.

BEWEIS Sei $\|\cdot\|_\infty$ eine Norm auf \mathcal{V} definiert durch $\|v\|_\infty = \max_{i=1,\dots,n} |a_i|$ für $v = \sum_{i=1}^n a_i b_i, a_i \in \mathbb{R}$. Da \mathcal{V} ein euklidischer Vektorraum ist, sind je zwei Normen äquivalent, d.h. es existiert ein $C \in \mathbb{R}$ mit $\|v\|_\infty \leq C\sqrt{\phi(v,v)}$ für alle $v \in \mathcal{V}$. Für $l \in L, l = \sum_{i=1}^n z_i b_i, z_i \in \mathbb{Z}$ mit $\phi(l,l) \leq s$ gilt also $z_i \leq C\sqrt{s}$. Es existieren also höchstens $(2C\sqrt{s+1})^n$ solcher Gittervektoren l . \square

Insbesondere folgt aus diesem Lemma, dass ein Gitter kürzeste Vektoren $\neq 0$ besitzt. Dies motiviert die folgenden Definitionen:

Definition 1.4 Für ein Gitter (L, ϕ) definiere

$$\min(L, \phi) := \min\{\phi(l, l) \mid l \in L - \{0\}\}.$$

Dann heißt

$$\text{Min}(L, \phi) := \{l \in L \mid \phi(l, l) = \min(L)\}$$

die Menge der kürzesten Vektoren in L .

Bemerkung 1.5 Seien $(L, \phi), (L', \phi)$ Gitter mit Gitterbasen B bzw. C . (L', ϕ) heißt Teilgitter von (L, ϕ) , wenn L' ein \mathbb{Z} -Teilmodul von L ist. Dann gilt $\mathcal{G}(C) = {}_C \text{id}_B \mathcal{G}(B) ({}_C \text{id}_B)^{\text{tr}}$ und $[L : L'] = |\det({}_C \text{id}_B)| = \sqrt{\frac{\det(L')}{\det(L)}}$.

Definition 1.6 Sei (L, ϕ) ein volles Gitter in (\mathcal{V}, ϕ) mit Gitterbasis B .

- (i) Sei $L^\# := \{v \in \mathcal{V} \mid \Phi(v, l) \in \mathbb{Z} \text{ für alle } l \in L\}$. Dann ist $(L^\#, \phi)$ ebenfalls ein volles Gitter in (\mathcal{V}, ϕ) , das zu (L, ϕ) duale Gitter.
- (ii) Falls $L \subseteq L^\#$ gilt, heißt (L, ϕ) ganz. Gilt sogar Gleichheit, so heißt (L, ϕ) unimodular.

Bemerkung 1.7 (i) Die Dualbasis $B^\# := (b_1^\#, \dots, b_m^\#)$ von B bezüglich ϕ ist eine Gitterbasis von $(L^\#, \phi)$.

- (ii) Es gilt ${}_B {}^* \text{id}_B = \mathcal{G}(B)$, also insbesondere $\mathcal{G}(B^\#) = \mathcal{G}(B)^{-1}$ und $\det(L^\#, \phi) = \det(L, \phi)^{-1}$.
- (iii) Falls (L, ϕ) ein ganzes Gitter ist, ist die Faktorgruppe $L^\# / L$ eine endliche abelsche Gruppe der Ordnung $\det(L, \phi)$ und $\mathcal{G}(B)$ ist eine Relationenmatrix dieser abelschen Gruppe. Falls $(d_1, \dots, d_n) \in \mathbb{Z}^n$ die Invariantenteiler von $\mathcal{G}(B)$ sind, gilt $L^\# / L \cong \mathbb{Z} / d_1 \mathbb{Z} \oplus \dots \oplus \mathbb{Z} / d_n \mathbb{Z}$.

BEWEIS Sei $v \in \mathcal{V}$. Dann gilt $\phi(l, v) \in \mathbb{Z}$ für alle $l \in L$ genau dann, wenn $a_i = \phi(b_i, v) \in \mathbb{Z}$ gilt für $1 \leq i \leq n$. Dies ist wiederum äquivalent dazu, dass $v = \sum a_i b_i^*$ gilt. Also ist das duale Gitter genau das von der dualen Basis erzeugte Gitter. Für $v = b_j$ erhält

man $b_j = \sum \phi(b_i, b_j) b_i^*$ für $1 \leq j \leq n$, also gilt ${}_B \text{id}_B = \mathcal{G}(B)$. Somit gilt $\mathcal{G}(B^*) = {}_B \text{id}_{B^*} = ({}_B \text{id}_B)^{-1} = \mathcal{G}(B)^{-1}$. $\mathcal{G}(B)$ ist eine Relationenmatrix von $L^\# / L$, denn es gilt $B^* \mathcal{G}(B) = B$. Damit ist $\det(L, \phi) = |L^\# / L|$ und die Elementarteiler von $\mathcal{G}(B)$ geben den Isomorphietyp der endlich abelschen Gruppe $L^\# / L$ an. \square

Definition 1.8 (Isometrie von Gittern) (i) Zwei Gitter (L, ϕ) und (L', ϕ') heißen isometrisch, falls eine \mathbb{Z} -lineare Abbildung $\alpha : L \rightarrow L', l \mapsto l\alpha$ existiert mit $\phi(l_1, l_2) = \phi'(l_1\alpha, l_2\alpha)$ für alle $l_1, l_2 \in L$. Dann heißt α Isometrie, im Fall $(L, \phi) = (L', \phi')$ heißt α Automorphismus.

(ii) Die Menge aller Automorphismen von (L, ϕ) bildet die Automorphismengruppe $\text{Aut}(L, \phi)$ von (L, ϕ) .

Bemerkung 1.9 Für jedes Gitter (L, ϕ) ist $\text{Aut}(L, \phi)$ eine endliche Gruppe.

BEWEIS Sei $B = (b_1, \dots, b_n)$ eine Gitterbasis von (L, ϕ) und sei $\alpha \in \text{Aut}(L, \phi)$. Dann gilt $b_i\alpha \in L_{\leq s}$ für jeden Basisvektor b_i und $s = \max\{\phi(b_j, b_j) \mid j = 1, \dots, n\}$. Da ein Automorphismus eindeutig durch die Bilder der Basisvektoren bestimmt ist, gilt $|\text{Aut}(L, \phi)| \leq |L_{\leq s}|^n$. \square

Definition 1.10 Ein Gitter (L, ϕ) heißt orthogonal zerlegbar, falls Teilgitter (L_1, ϕ) , (L_2, ϕ) von (L, ϕ) existieren mit $L_i \neq \{0\}$, $\phi(L_1, L_2) = \{0\}$ und $\langle L_1, L_2 \rangle_{\mathbb{Z}} = L$.

Satz 1.11 (M. Eichler, M. Kneser) Jedes Gitter (L, ϕ) besitzt eine bis auf Reihenfolge eindeutige Zerlegung in orthogonal unzerlegbare Teilgitter $(L_1, \phi), \dots, (L_k, \phi)$.

Dieser Satz wurde erstmals 1952 von M. Eichler in [Eic52] bewiesen. M. Kneser gab in [Kne54] einen alternativen Beweis an, mit dem diese Zerlegung konstruktiv bestimmt werden konnte.

Satz 1.12 ([Opg92], Satz 1.1.6) Sei (L, ϕ) ein ganzzahliges Gitter und sei p eine Primzahl. Die Teilgitter (M, ϕ) von (L, ϕ) vom Index p stehen in Bijektion zu den eindimensionalen Teilräumen von $(\mathbb{Z}/p\mathbb{Z})^{1 \times n}$. Insbesondere ist ihre Anzahl $(p^n - 1)/(p - 1)$.

BEWEIS Ist M ein \mathbb{Z} -Teilmodul von L vom Index p , so induziert der natürliche Homomorphismus $L \rightarrow L/M$ einen Epimorphismus von L auf $\mathbb{Z}/p\mathbb{Z}$, da L/M eine additive Gruppe der Ordnung p ist. Andererseits hat jeder Epimorphismus $L \rightarrow \mathbb{Z}/p\mathbb{Z}$ ein Teilgitter vom Index p als Kern.

Sei $B = (b_1, \dots, b_n)$ eine Basis von L und sei für $l \in L$ mit $l = a_1 b_1 + \dots + a_n b_n$ ${}_B l = (a_1, \dots, a_n)$. $\text{Hom}(\mathbb{Z}^n, \mathbb{Z}/p\mathbb{Z})$ ist isomorph zu $(\mathbb{Z}/p\mathbb{Z})^{1 \times n}$ und jeder Homomorphismus $\kappa : L \rightarrow \mathbb{Z}/p\mathbb{Z}$ lässt sich schreiben als

$$\kappa_{B,a} : L \rightarrow \mathbb{Z}/p\mathbb{Z}, l \mapsto {}_B l a^{\text{tr}} + p\mathbb{Z}$$

für ein $a \in (\mathbb{Z}/p\mathbb{Z})^{1 \times n}$. Klar ist: $\kappa_{B,a}$ ist genau dann ein Epimorphismus, wenn a nicht der Nullvektor ist, und $\kappa_{B,a}$ und $\kappa_{B,b}$ besitzen genau dann den gleichen Kern, wenn gilt: $b = ca$ für ein $c \in \mathbb{Z}/p\mathbb{Z} - \{0 + p\mathbb{Z}\}$. Daraus folgt die Behauptung. \square

Bemerkung 1.13 Sei (L, ϕ) ein ganzzahliges Gitter mit Gitterbasis $B = (b_1, \dots, b_n)$ und sei (M, ϕ) ein Teilgitter vom Index p . Dann gilt $M = \text{Kern}(\kappa_{B,a})$ für ein $a = (\bar{a}_1, \dots, \bar{a}_n) \in (\mathbb{Z}/p\mathbb{Z})^{1 \times n}$. Sei i der kleinste Index mit $\bar{a}_i \neq \bar{0}$. Dann gilt o.B.d.A. $\bar{a}_i = \bar{1}$, d.h. $a = (\bar{0}, \dots, \bar{0}, \bar{1}, \bar{a}_{i+1}, \dots, \bar{a}_n)$. Damit folgt

$$\text{Kern}(\kappa_{B,a}) = \langle b_1, \dots, b_{i-1}, pb_i, b_{i+1} - a_{i+1}b_i, \dots, b_n - a_nb_i \rangle_{\mathbb{Z}}.$$

Inbesondere sind diese n Vektoren eine Gitterbasis von (M, ϕ) .

Bemerkung 1.14 Sei (L, ϕ) ein ganzzahliges Gitter, $\alpha \in \text{Aut}(L, \phi)$ und $\epsilon : L \rightarrow \mathbb{Z}/p\mathbb{Z}$ ein Epimorphismus. Dann ist die Komposition $\alpha\epsilon$ ebenfalls ein Epimorphismus von L auf $\mathbb{Z}/p\mathbb{Z}$, wobei ϵ und $\alpha\epsilon$ isometrische Kerne haben. $\text{Aut}(L, \phi)$ operiert auf der Menge aller Epimorphismen von L auf $\mathbb{Z}/p\mathbb{Z}$, wobei Epimorphismen, die in einer Bahn unter $\text{Aut}(L, \phi)$ liegen, isometrische Kerne haben. Möchte man die Isometrieklassen aller Teilgitter von Index p bestimmen, genügt es, nur die Kerne von Vertretern der Bahnen von $\text{Aut}(L, \phi)$ auf der Menge aller Epimorphismen zu betrachten. Allerdings können Teilgitter, welche Kerne von Epimorphismen sind, die nicht in einer Bahn liegen, trotzdem isometrisch sein.

1.2 Zusammenhang von Gittern und quadratischen Formen

Definition 1.15 Sei R ein Teilring eines Körpers \mathbb{K} der Charakteristik $\neq 2$.

(i) Eine quadratische Form f in n Variablen ist eine Funktion

$$f : R^n \rightarrow \mathbb{K}, x = (x_1, \dots, x_n) \mapsto \sum_{i,j=1}^n f_{ij}x_ix_j = (x_1, \dots, x_n)F(x_1, \dots, x_n)^{\text{tr}}$$

mit $f_{ij} = f_{ji} \in \mathbb{K}$ für $1 \leq i, j \leq n$ und $F = (f_{ij})_{1 \leq i, j \leq n}$. Im Fall $\mathbb{K} = \mathbb{Q}$ heißt f rationale quadratische Form. Sind die Koeffizienten f_{ij} aus \mathbb{Z} , so heißt f ganzzahlig.

(ii) Eine quadratische Form heißt positiv definit bzw. positiv semidefinit, falls $\mathbb{K} \leq \mathbb{R}$ und die Matrix F positiv definit bzw. positiv semidefinit ist.

(iii) Zwei quadratische Formen f und g heißen R -äquivalent, falls ein $T \in \text{GL}_n(R)$ existiert mit $g(xT) = f(x)$ für alle $x \in R^n$.

Sei nun (L, ϕ) ein Gitter mit Gitterbasis $B = (b_1, \dots, b_n)$ und Gram-Matrix $A = \mathcal{G}(B)$. Dann definiert (L, ϕ) eine positiv definite quadratische Form für $\mathbb{K} = \mathbb{R}$ und $R = \mathbb{Z}$

durch

$$\mathbb{Z}^n \rightarrow \mathbb{R}, (a_1, \dots, a_n) \mapsto \phi\left(\sum_{i=1}^n a_i b_i, \sum_{i=1}^n a_i b_i\right) = (a_1, \dots, a_n) A (a_1, \dots, a_n)^{\text{tr}}.$$

Quadratische Formen, die zu isometrischen Gittern gehören, sind \mathbb{Z} -äquivalent. Andererseits definieren isometrische Gitter \mathbb{Z} -äquivalente quadratische Formen. Es existiert also eine 1-1-Zuordnung zwischen den \mathbb{Z} -Äquivalenzklassen positiv definiten quadratischer Formen und den Isometrieklassen von Gittern. Eine symmetrische und positiv definite Matrix $A \in \mathbb{R}^{n \times n}$ definiert eine quadratische Form und somit auch eine Isometrieklasse von Gittern. Diese besteht aus ganzzahligen Gittern genau dann, wenn die Matrix A ganzzahlig ist. Die Begriffe aus der Gittertheorie übertragen sich:

$$\begin{aligned} \min(A) &:= \min\{vAv^{\text{tr}} \mid v \in \mathbb{Z}^{1 \times n}\} \\ \text{Min}(A) &:= \{v \in \mathbb{Z}^{1 \times n} \mid vAv^{\text{tr}} = \min(A)\} \\ \text{Aut}(A) &:= \{B \in \text{GL}_n(\mathbb{Z}) \mid BAB^{\text{tr}} = A\} \end{aligned}$$

Bemerkung 1.16 Sei (L, ϕ) ein Gitter mit Gitterbasis B und Gram-Matrix $A = \mathcal{G}(B)$. Dann gilt:

- (i) $\min(L, \phi) = \min(A)$.
- (ii) Es gilt $a_1 b_1 + \dots + a_n b_n \in \text{Min}(L, \phi)$ genau dann, wenn $(a_1, \dots, a_n) \in \text{Min}(A)$ gilt.
- (iii) Es gilt $\alpha \in \text{Aut}(L, \phi)$ genau dann, wenn ${}_B \alpha_B \in \text{Aut}(A)$ gilt.
- (iv) (L, ϕ) ist orthogonal zerlegbar genau dann, wenn ein $g \in \text{GL}_n(\mathbb{Z})$ existiert, so dass gAg^{tr} eine Blockdiagonalmatrix ist.

2 Einbettung euklidischer Gitter in

$\mathbb{Z}_{\text{orth}}^k$

2.1 Der Algorithmus SIB

In diesem Abschnitt wird der Algorithmus aus [Ple95] vorgestellt, der für ein symmetrisches, positiv definites $A \in \mathbb{Z}^{n \times n}$ alle $k \in \mathbb{N}$ und alle $X \in \mathbb{Z}^{n \times k}$ findet mit $A = XX^{\text{tr}}$. Hiermit kann für ein ganzes Gitter (L, ϕ) entschieden werden, ob, und wenn ja wie, es sich in $\mathbb{Z}_{\text{orth}}^k$ (dem Gitter \mathbb{Z}^k mit dem Standardskalarprodukt) für ein $k \in \mathbb{N}$ einbetten lässt. Falls $B = (b_1, \dots, b_n)$ eine Gitterbasis von (L, ϕ) ist, bilden die Zeilen von jedem $X \in \mathbb{Z}^{n \times k}$ mit $\mathcal{G}(B) = XX^{\text{tr}}$ die Gitterbasis von einem Teilgitter von $\mathbb{Z}_{\text{orth}}^k$, welches isometrisch zu (L, ϕ) ist. Der Algorithmus hat allerdings noch andere Anwendungen, welche später diskutiert werden. Die Sätze und Beweise wurden ebenfalls aus [Ple95] übernommen.

Bemerkung 2.1 Sei $\gamma_k := \{X = (X_1, \dots, X_k) \in \mathbb{Z}^{n \times k} \mid X_i \neq 0, XX^{\text{tr}} = A\}$ und $\gamma := \bigcup_{k \in \mathbb{N}} \gamma_k$. Dann gilt:

(i) γ ist eine endliche Menge.

(ii) γ ist abgeschlossen unter Vorzeichenänderung und Vertauschen der Spalten.

BEWEIS (i) Sei $X \in \gamma$. Dann gilt $X_{i,-} X_{i,-}^{\text{tr}} = A_{i,i}$ für jede Zeile von X . Die Matrix

$$B = \begin{pmatrix} \underbrace{1 \ \dots \ 1}_{A_{1,1}} & & & & \\ & \underbrace{1 \ \dots \ 1}_{A_{2,2}} & & & \\ & & \ddots & & \\ & & & & \underbrace{1 \ \dots \ 1}_{A_{n,n}} \end{pmatrix} \in \mathbb{Z}^{n \times \text{Spur}(A)}$$

hat maximale Spaltenanzahl, sodass $B_{i,-} B_{i,-}^{\text{tr}} = A_{i,i}$ ist für $i = 1, \dots, n$. Für $X = (X_1, \dots, X_k) \in \gamma$ gilt also $k \leq \text{Spur}(A)$ und $X_{i,j} \leq \sqrt{A_{i,i}}$. Da alle $X_{i,j}$ ganzzahlig sind,

folgt die Behauptung.

(ii) Für $X = (X_1, \dots, X_k) \in \gamma$ gilt $A = \sum_{i=1}^k X_i X_i^{\text{tr}}$, daraus folgt die Behauptung. \square

Um Trivialitäten zu vermeiden, wird verlangt, dass keine Spalte 0 ist. Meistens ist man nur an den Spalten einer Lösung interessiert, nicht aber an deren Vorzeichen oder Reihenfolge. Im Folgenden werden also zwei Lösungen $X, X' \in \gamma$ als gleich angesehen, wenn sie bis auf Reihenfolge und Vorzeichen die gleichen Spalten haben.

Bemerkung 2.2 Sei $A \in \mathbb{R}^{n \times n}$ symmetrisch und positiv definit. Für $X \in \mathbb{R}^{n \times k}$, definiere $P = P_X = X^{\text{tr}} A^{-1} X \in \mathbb{R}^{k \times k}$. Dann sind die folgenden Aussagen äquivalent:

(i) $A = X X^{\text{tr}}$.

(ii) $P^2 = P$ und $\text{Spur}(P) = n$.

(iii) $I_k - P$ ist positiv semidefinit mit Rang $k - n$.

BEWEIS (i) \Rightarrow (ii): Es gilt $P^2 = (X^{\text{tr}} A^{-1} X)(X^{\text{tr}} A^{-1} X) = X^{\text{tr}} A^{-1} A A^{-1} X = P$. Also ist $\text{Spur}(P) = \text{Rang}(P) = \text{Rang}(X)$, da A^{-1} positiv definit ist. Nach (i) gilt allerdings $\text{Rang}(X) = n$.

(ii) \Rightarrow (iii): P hat die Eigenwerte 0 und 1 mit Vielfachheiten $k - n$ und n . Also hat $I_k - P$ die Eigenwerte 1 und 0 mit Vielfachheiten $k - n$ und n . Da nach (ii) $(I_k - P)^2 = I_k - P$ ist, gilt $\text{Rang}(I_k - P) = \text{Spur}(I_k - P) = k - \text{Spur}(P) = k - n$.

(iii) \Rightarrow (i): Seien a_1, \dots, a_k die Eigenwerte von P . Aus $\text{Rang}(I_k - P) = k - n$ folgt, dass $I_k - P$ n -mal den Eigenwert 0 hat, also existieren genau n a_i mit $1 - a_i = 0$. Sei o.B.d.A. $a_1 = \dots = a_n = 1$. Da $\text{Rang}(P) \leq n$ ist, gilt $a_{n+1} = \dots = a_k = 0$, also ist $(I_k - P)^2 = I_k - P$ und $P^2 = P$ und $\text{Rang}(X) = \text{Rang}(P)$, insbesondere $XP = X$. Es ist $A - X X^{\text{tr}} = 0$ äquivalent zu $(A - X X^{\text{tr}})A^{-1} = 0$, was wiederum äquivalent ist zu $(A - X X^{\text{tr}})A^{-1}X = 0$ (da X injektiv). Da $(A - X X^{\text{tr}})A^{-1}X = X - X X^{\text{tr}} A^{-1} X = X - XP$ gilt folgt die Behauptung. \square

Korollar 2.3 Sei $A \in \mathbb{Z}^{n \times n}$ symmetrisch und positiv definit. Jede Spalte X_i einer Lösung $X \in \gamma$ erfüllt

$$X_i^{\text{tr}} A^{-1} X_i \leq 1.$$

BEWEIS Aus $A = X X^{\text{tr}}$ folgt mit Bemerkung 2.2 $(I_k - P)_{i,i} \geq 0$, also ist $X_i^{\text{tr}} A^{-1} X_i = P_{i,i} \leq 1$. \square

Da A symmetrisch und positiv definit ist, gilt dies für A^{-1} ebenfalls, kann also als Gram-Matrix eines Gitters (L, ϕ) aufgefasst werden. Nach Bemerkung 1.16 ist also $\{Y \in \mathbb{Z}^{n \times 1} \mid Y^{\text{tr}} A^{-1} Y \leq 1\}$ eine endliche Menge. Hiermit ist es bereits möglich die Grundidee des Algorithmus' zu formulieren. Vorher ist allerdings etwas Notation notwendig.

Notation (i) Für festes $A \in \mathbb{Z}^{n \times n}$ symmetrisch und positiv definit sei $cc = (X_i)_{i=1}^m$ eine Familie von $X_i \in \mathbb{Z}^{n \times 1}$ mit $X_i^{\text{tr}} A^{-1} X_i \leq 1$ und $X_i \neq \pm X_j$ für alle $1 \leq i < j \leq m$.

(ii) Für festes cc und $\iota = (\iota_1, \dots, \iota_m) \in \mathbb{Z}_{\geq 0}^m$ sei

$$\begin{aligned} |\iota| &= \sum_{j=1}^m \iota_j \\ f(\iota) &= \left(\underbrace{X_1, \dots, X_1}_{\iota_1}, \dots, \underbrace{X_m, \dots, X_m}_{\iota_m} \right) \in \mathbb{Z}^{n \times |\iota|} \\ G(\iota) &= I_{|\iota|} - f(\iota) A^{-1} f(\iota) \in \mathbb{Q}^{|\iota| \times |\iota|} \end{aligned}$$

(iii) $\iota \in \mathbb{Z}_{\geq 0}^m$ heißt zulässig, falls $G(\iota)$ positiv semidefinit ist.

(iv) Definiere eine partielle Ordnung \geq_{tot} auf $\mathbb{Z}_{\geq 0}^m$ durch

$$(\tau_1, \dots, \tau_m) \geq_{\text{tot}} (\iota_1, \dots, \iota_m)$$

genau dann wenn $\tau_k \geq \iota_k$ für alle $k = 1, \dots, m$.

„cc“ steht hierbei für Spaltenkandidaten („column candidates“). Falls alle Lösungen $X \in \gamma$ berechnet werden sollen, kommt jedes $X_i \in \mathbb{Z}^{n \times 1}$, $X_i \neq 0$ mit $X_i^{\text{tr}} A^{-1} X_i \leq 1$ bis auf Vorzeichen genau einmal in cc vor. Je nach Anwendung des Algorithmus' kann die Liste aber weiter eingeschränkt werden, Beispiele hierfür werden am Ende des Abschnittes diskutiert. Nach Bemerkung 2.2 und Korollar 2.3 ist jede Lösung $X \in \gamma$ von der Form $X = f(\iota)$ für ein $\iota \in \mathbb{Z}_{\geq 0}^m$ mit $G(\iota)$ positiv semidefinit und vom Rang $|\iota| - n$. Zulässigkeit lässt sich auch anders charakterisieren, wie die folgende Bemerkung zeigt.

Bemerkung 2.4 Seien A, X, P wie in Bemerkung 2.2. Dann sind folgende Aussagen äquivalent:

- (i) $A - XX^{\text{tr}}$ ist positiv semidefinit
- (ii) $P - P^2$ ist positiv semidefinit
- (iii) $I_k - P$ ist positiv semidefinit

BEWEIS (i) \Rightarrow (ii): Falls $A - XX^{\text{tr}}$ positiv semidefinit ist, existiert ein $Y \in \mathbb{R}^{n \times s}$ (für

$s = \text{Rang}(A - XX^{\text{tr}})$ mit $A - XX^{\text{tr}} = YY^{\text{tr}}$. Damit folgt

$$\begin{aligned}
& P - (X^{\text{tr}}A^{-1}Y)(X^{\text{tr}}A^{-1}Y)^{\text{tr}} \\
&= P - (X^{\text{tr}}A^{-1}Y)(Y^{\text{tr}}A^{-1}X) \\
&= P - X^{\text{tr}}A^{-1}(A - XX^{\text{tr}})A^{-1}X \\
&= P - \underbrace{X^{\text{tr}}A^{-1}AA^{-1}X}_{=P} + \underbrace{X^{\text{tr}}A^{-1}XX^{\text{tr}}A^{-1}X}_{=P^2} \\
&= P^2
\end{aligned}$$

Also ist $P - P^2$ positiv semidefinit, da $(X^{\text{tr}}A^{-1}Y)(X^{\text{tr}}A^{-1}Y)^{\text{tr}}$ positiv definit ist.

(ii) \Rightarrow (iii): Die Eigenwerte von P sind nicht-negativ und nach (ii) kleiner oder gleich 1, damit folgt (iii).

(iii) \Rightarrow (i): Sei $A = gg^{\text{tr}}$ für ein $g \in \text{GL}(n, \mathbb{R})$. Dann ist jeder Eigenwert von $g^{-1}(A - XX^{\text{tr}})g^{-\text{tr}} = I_k - (g^{-1}X)(g^{-1}X)^{\text{tr}}$ entweder gleich 1 oder Eigenwert von $I_k - (g^{-1}X)^{\text{tr}}(g^{-1}X) = I_k - X^{\text{tr}}A^{-1}X = I_k - P$, was positiv semidefinit ist. Also ist $A - XX^{\text{tr}}$ positiv semidefinit. \square

Mit dieser Bemerkung wird klar, dass

$$\{Y \in \mathbb{Z}^{n \times 1} \mid Y^{\text{tr}}A^{-1}Y \leq 1\} = \{Y \in \mathbb{Z}^{n \times 1} \mid A - YY^{\text{tr}} \text{ positiv semidefinit}\}$$

gilt. Außerdem ist $\iota \in \mathbb{Z}_{\geq 0}^m$ zulässig, genau dann wenn $A - f(\iota)f(\iota)^{\text{tr}}$ positiv semidefinit ist. Jedes ι mit $f(\iota) = X \in \gamma$ ist \geq_{tot} -maximal zulässig, im Allgemeinen gilt die Umkehrung aber nicht. In Kapitel 3 werden Matrizen $A' = A - f(\iota)f(\iota)^{\text{tr}}$ mit einem \geq_{tot} -maximal zulässigem ι betrachtet, also positiv semidefinite Matrizen A' , für die die Menge $\{Y \in \mathbb{Z}^{n \times 1} \mid A' - YY^{\text{tr}} \text{ positiv semidefinit}\}$ leer ist.

Nun ist es möglich eine Grundversion des Algorithmus' zur Bestimmung von γ anzugeben:

Algorithmus 2.5 (SIB) Sei $A \in \mathbb{Z}^{n \times n}$ symmetrisch und positiv definit.

Schritt 1: Berechne die Spaltenkandidaten $cc = (X_i)_{i=1}^m$. Sei $\iota = (\iota_1, \dots, \iota_m) = (0, \dots, 0) \in \mathbb{Z}_{\geq 0}^m$ und $l = 1$.

Schritt 2: Falls möglich, erhöhe ι_k um 1, wobei $k \geq l$ minimal ist so dass das resultierende ι zulässig bleibt, setze l auf k und führe Schritt 2 mit den neuen Parametern ι und l aus. Fahre sonst mit Schritt 3 fort.

Schritt 3: Überprüfe ob $f(\iota)f(\iota)^{\text{tr}} = A$ gilt und verringere ι durch

- (i) Falls $\iota_l \neq 0$ und $l < m$ ist, verringere ι_l und danach l jeweils um 1. Fahre dann mit Schritt 2 fort.
- (ii) Falls $\iota_l \neq 0$ und $l = m$ ist, sei k maximal mit $\iota_k \neq 0$ und $k < m$, verringere ι_k um 1, setze ι_m auf 0 und l auf $k + 1$.

(iii) Falls $\iota_l = 0$ ist, sei k maximal mit $\iota_k \neq 0$, verringere ι_k um 1 und setze l auf $k + 1$. Fahre dann mit Schritt 2 fort. Falls kein solches k existiert, terminiere.

„Falls möglich“ in Schritt 2 bedeutet, dass kein Kriterium zu dem Schluss führt, dass kein $\tau \in \mathbb{Z}_{\geq 0}^m$ existiert mit $f(\tau) \in \gamma$ und welches in lexikographischer Ordnung kleiner als ι ist (meistens sogar $\iota \leq_{\text{tot}} \tau$). Diese Kriterien (und auch die Laufzeit des Algorithmus') hängen stark von einer geeigneten Sortierung der Vektoren in cc ab:

Sei $cc = (X_i)_{i=1}^m$ und $X_i = (x_{i1}, \dots, x_{in})^{\text{tr}}$ ein Spaltenkandidat. Definiere

$$A(r, s) := \{X_i \mid x_{ir} \cdot x_{is} \neq 0\}$$

für $1 \leq r \leq s \leq n$. Wähle eine Anordnung der X_i , so dass $\{X_1, \dots, X_{|A(r,s)|}\} = A(r, s)$ gilt, wobei r, s so gewählt werden, dass $|A(r, s)|$ minimal ist. Bezeichne dieses (r, s) mit (r_1, s_1) und definiere für $(r, s) \neq (r_1, s_1)$

$$A^1(r, s) := \{X_i \mid X_i \notin A(r_1, s_1), x_{ir} \cdot x_{is} \neq 0\}$$

und wähle (r_2, s_2) wieder so, dass $|A^1(r_1, s_1)|$ minimal ist unter allen $|A^1(r, s)|$. Wenn man dies fortsetzt erhält man eine Partition von cc in

$$A(r_1, s_1), A^1(r_2, s_2), A^2(r_3, s_3), \dots$$

welche, nach geeigneter Umsortierung, aus aufeinander folgenden Vektoren aus cc besteht. Damit kann man folgendes Kriterium formulieren: Falls der Positionsindex l in Schritt 2 von Algorithmus 2.5 größer ist als der größte Index in $A^{i+1}(r_i, s_i)$, muss der Eintrag (r_i, s_i) von $A - f(l)f(l)^{\text{tr}}$ entweder 0 sein oder kein $\tau \geq_{\text{tot}} \iota$ führt zu einer Lösung $f(\tau) \in \gamma$.

Die so definierte Ordnung von cc lässt noch Freiheiten innerhalb der $A^{i+1}(r_i, s_i)$ zu. Hier ist es sinnvoll die X_k so anzuordnen, dass $X_k^{\text{tr}} A^{-1} X_k$ monoton fallend ist für $k \in A^{i+1}(r_i, s_i)$.

Beispiel 2.6 Sei

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

eine Gram-Matrix des Wurzelgitters E_8 . Es existiert keine Einbettung von E_8 in ein $\mathbb{Z}_{\text{orth}}^k$, da die Menge $\{Y \in \mathbb{Z}^{n \times 1} \mid Y^{\text{tr}} A^{-1} Y \leq 1\}$ leer ist. Die Gleichung $XX^{\text{tr}} = 2A$ liefert 2025 Lösungen $X \in \mathbb{Z}^{8 \times k}$ mit $k = 8$ für alle X . $XX^{\text{tr}} = 3A$ liefert 11200 Lösungen die alle in $\mathbb{Z}^{8 \times 12}$ liegen.

Beispiel 2.7 Sei $M := \{1, \dots, 10\}$. Gesucht sind Teilmengen $S_1, \dots, S_5 \subseteq M$ mit $|S_i \cap S_j| = A_{ij}$ für

$$A = \begin{pmatrix} 3 & 1 & 1 & 0 & 2 \\ 1 & 2 & 0 & 1 & 0 \\ 1 & 0 & 2 & 0 & 2 \\ 0 & 1 & 0 & 1 & 0 \\ 2 & 0 & 2 & 0 & 3 \end{pmatrix}.$$

Die Gleichung $XX^{\text{tr}} = A$ mit $X \in \{0, 1\}^{5 \times k}$ und $k \leq 10$ liefert als einzige Lösung

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

Die Mengen S_i können nun abgelesen werden, in dem man ein beliebiges 5-elementiges Tupel $M' \in M^5$ wählt und die Zeilen von X als ihre charakteristische Funktion interpretiert. Die Wahl $M' = (1, 2, 3, 4, 5)$ liefert zum Beispiel

$$S_1 = \{1, 2, 3\}, S_2 = \{1, 4\}, S_3 = \{2, 5\}, S_4 = \{4\}, S_5 = \{2, 3, 5\}.$$

2.2 Transversalen der Automorphismengruppe auf den Einbettungen

Interpretiert man eine symmetrische und positiv definite Matrix $A \in \mathbb{Z}^{n \times n}$ als Gram-Matrix eines ganzzahligen Gitters (L, ϕ) , liefert der Algorithmus SIB Basen von Teilgittern in $\mathbb{Z}_{\text{orth}}^k$, welche zu (L, ϕ) isometrisch sind. Dass die Lösungen nur bis auf Vertauschen und Vorzeichenänderung der Spalten berechnet werden, bedeutet, dass Einbettungen, welche durch Drehungen und Spiegelungen ineinander hervorgehen, nicht doppelt berechnet werden. Allerdings kann es vorkommen, dass das \mathbb{Z} -Erzeugnis der Zeilen bei einigen Lösungen gleich ist, dass SIB also verschiedene Basen für die gleichen Gitter berechnet. Im Folgenden wird eine Methode beschrieben, wie die Gruppe $\text{Aut}(A)$ ausgenutzt werden kann, für jede mögliche Einbettung nur eine einzige Basis zu berechnen. Zusätzlich soll erreicht werden, dass weniger $\iota \in \mathbb{Z}_{\geq 0}^m$ auf Zulässigkeit geprüft werden müssen, insbesondere soll also nicht im Nachhinein entschieden werden, ob zwei berechnete Basen das selbe \mathbb{Z} -Erzeugnis haben.

Sei im Folgenden $A \in \mathbb{Z}^{n \times n}$ symmetrisch und positiv definit und sei $cc = (X_i)_{i=1}^m$ die Familie aller $X_i \in \mathbb{Z}^{n \times 1}$ mit $X_i^{\text{tr}} A^{-1} X_i \leq 1$ und $X_i \neq \pm X_j$ für alle $1 \leq i < j \leq m$.

Bemerkung 2.8 (i) Sei $C := \{Y \in \mathbb{Z}^{n \times 1} \mid Y^{\text{tr}} A^{-1} Y \leq 1\}$. Die Gruppen $\{\pm I_n\}$ und $\text{Aut}(A)$ operieren auf C durch Multiplikation von links. Da beide Operationen vertauschen, operiert $\text{Aut}(A)$ auf $C/\{\pm I_n\}$, also auch auf der Transversalen cc .

(ii) $\text{Aut}(A)$ operiert auf \underline{m} durch die Identifikation $X_i \leftrightarrow i$ für alle $X_i \in cc$. Dadurch operiert $\text{Aut}(A)$ auf $\mathbb{Z}_{\geq 0}^m$ durch

$$\text{Aut}(A) \times \mathbb{Z}_{\geq 0}^m \rightarrow \mathbb{Z}_{\geq 0}^m, (B, (\iota_1, \dots, \iota_m)) \mapsto (\iota_{\overline{B}^{-1}(1)}, \dots, \iota_{\overline{B}^{-1}(m)}).$$

(iii) $\text{Aut}(I_k)$ operiert auf $cc^k \subseteq \mathbb{Z}^{n \times k}$ durch

$$\text{Aut}(I_k) \times cc^k \rightarrow cc^k, (M, X) \mapsto XM.$$

$\text{Aut}(A)$ operiert auf cc^k durch

$$\text{Aut}(A) \times cc^k \rightarrow cc^k, (B, X) \mapsto BX.$$

Da beide Operationen vertauschen, operiert $\text{Aut}(A)$ auf $cc^k / \text{Aut}(I_k)$, also auch auf der Transversalen $\text{Bild}(f) \cap \mathbb{Z}^{n \times k}$.

(iv) $\text{Aut}(I_k)$ operiert auf $\gamma_k \subseteq \mathbb{Z}^{n \times k}$ durch

$$\text{Aut}(I_k) \times \gamma_k \rightarrow \gamma_k, (M, X) \mapsto XM.$$

$\text{Aut}(A)$ operiert auf γ_k durch

$$\text{Aut}(A) \times \gamma_k \rightarrow \gamma_k, (B, X) \mapsto BX.$$

Da beide Operationen vertauschen, operiert $\text{Aut}(A)$ auf $\gamma_k / \text{Aut}(I_k)$, also auch auf der Ausgabe von SIB als Transversale dieser Operation.

(v) f ist eine $\text{Aut}(A)$ -ähnliche Abbildung zwischen $\mathbb{Z}_{\geq 0}^m$ und $\text{Bild}(f)$.

Lemma 2.9 Die Zeilen von zwei Matrizen $X, X' \in \gamma$ haben genau dann das gleiche \mathbb{Z} -Erzeugnis, wenn sie in einer Bahn unter $\text{Aut}(A)$ liegen.

BEWEIS Falls X und X' in einer Bahn unter $\text{Aut}(A)$ liegen, existiert ein $B \in \text{Aut}(A)$ mit $BX = X'$. Da aber $B \in \text{GL}_n(\mathbb{Z})$ gilt, haben die Zeilen von X und X' das gleiche \mathbb{Z} -Erzeugnis. Andererseits folgt aus der Gleichheit der \mathbb{Z} -Erzeugnisse, dass ein $B \in \text{GL}_n(\mathbb{Z})$ existiert mit $BX = X'$. Dann gilt allerdings $A = X'X'^{\text{tr}} = (BX)(BX)^{\text{tr}} = BXX^{\text{tr}}B^{\text{tr}} = BAB^{\text{tr}}$, also ist $B \in \text{Aut}(A)$. \square

Ziel ist nun also, dass der Algorithmus für alle $k \in \mathbb{N}$ mit $\gamma_k \neq \emptyset$ eine Transversale der Operationen von $\text{Aut}(A)$ auf $\gamma_k / \text{Aut}(I_k)$ ausgibt, ohne natürlich erst die gesamte Lösungsmenge und dann die Bahnen zu bestimmen.

Satz 2.10 Seien $\iota, \tau \in \mathbb{Z}_{\geq 0}^m$ und sei $B \in \text{Aut}(A)$. Dann gilt:

- (i) ι ist zulässig genau dann, wenn $B\iota$ zulässig ist.
- (ii) Es gilt $\tau \geq_{\text{tot}} \iota$ genau dann, wenn $B\tau \geq_{\text{tot}} B\iota$ gilt.
- (iii) Es gilt $\tau \geq_{\text{tot}} \iota$ mit $A = f(\tau)f(\tau)^{\text{tr}}$ genau dann, wenn $B\tau \geq_{\text{tot}} B\iota$ mit $A = f(B\tau)f(B\tau)^{\text{tr}}$ gilt.

BEWEIS (i) Sei ι zulässig. Per Definition ist dann $A - f(\iota)f(\iota)^{\text{tr}}$ positiv semidefinit. Nach dem Sylvesterschem Trägheitssatz ist dies äquivalent dazu, dass $B(A - f(\iota)f(\iota)^{\text{tr}})B^{\text{tr}}$ positiv semidefinit ist. Durch die Operation von $\text{Aut}(A)$ ist dies wiederum äquivalent dazu dass $A - f(B\iota)f(B\iota)^{\text{tr}}$ positiv semidefinit ist.

(ii) $\text{Aut}(A)$ operiert durch Permutation der Einträge.

(iii) Es gilt $f(B\iota) = Bf(\iota)$. Durch (ii) und der Operation auf den Lösungen folgt die Behauptung. \square

Die wesentliche Aussage ist: Angenommen SIB testet ein $\iota \in \mathbb{Z}_{\geq 0}^m$ auf Zulässigkeit. Falls ein $\tau \in \text{Aut}(A)\iota$ existiert, welches SIB bereits auf Zulässigkeit geprüft hat, folgt bereits, dass alle Lösungen $f(\iota') \in \gamma$ mit $\iota' \geq_{\text{tot}} \iota$ in den selben Bahnen liegen wie die Lösungen $f(\tau') \in \gamma$ mit $\tau' \geq_{\text{tot}} \tau$. Da die τ' aber schon berechnet wurden, kann ι als nicht zulässig gewertet werden. Gesucht ist also eine Möglichkeit zu entscheiden, ob ein solches τ in der Bahn $\text{Aut}(A)\iota$ existiert. Sei \geq_{lex} die übliche Lexikographische Ordnung auf $\mathbb{Z}_{\geq 0}^m$. Da SIB alle $\iota \in \mathbb{Z}_{\geq 0}^m$ in lexikographischer Reihenfolge auf Zulässigkeit testet gilt also: $\tau \in \text{Aut}(A)\iota$ wird genau dann vor ι auf Zulässigkeit geprüft wenn $\tau >_{\text{lex}} \iota$ gilt.

Ob solch ein solches τ in der Bahn $\text{Aut}(A)\iota$ existiert kann natürlich mit dem Bahnenalgorithmus getestet werden, dies ist in der Regel allerdings zu aufwendig. Sinnvoller ist es die Bahn geordnet auszurechnen. Hierfür ist ein Resultat aus der Computeralgebra notwendig:

Bemerkung 2.11 (i) $\text{Aut}(A)$ operiert im Allgemeinen nicht treu auf cc . Es kann allerdings o.B.d.A. die Gruppe $G := \text{Bild}(\alpha)$ für

$$\alpha : \text{Aut}(A) \rightarrow S_{cc}, B \mapsto \overline{B}$$

betrachtet werden. Dann gilt $cc / \text{Aut}(A) = cc / G$, durch die in Bemerkung 2.8 definierten Operationen also auch $\underline{m} / \text{Aut}(A) = \underline{m} / G$ und $\mathbb{Z}_{\geq 0}^m / \text{Aut}(A) = \mathbb{Z}_{\geq 0}^m / G$. G operiert treu auf cc , \underline{m} und $\mathbb{Z}_{\geq 0}^m$.

(ii) Sei $U_0 = G$ wie in (i) definiert und sei $U_i = \text{Stab}_G(1, \dots, i)$ und R_i ein Vertretersystem von U_i in U_{i-1} für $i = 1, \dots, m$. Dann ist die Abbildung

$$R_1 \times \dots \times R_m \rightarrow G, (g_1, \dots, g_m) \mapsto g_1 \cdot \dots \cdot g_m$$

eine Bijektion.

Dadurch ist es möglich bei der Berechnung von $\text{Aut}(A)\iota = G\iota$ schrittweise die ersten i Einträge von ι zu fixieren.

Algorithmus 2.12 *Gegeben:* Eine Gruppe G definiert wie in Bemerkung 2.11 durch ein Vertretersystem R_1, \dots, R_m und ein $\iota \in \mathbb{Z}_{\geq 0}^m$.

Gesucht: Ist $\iota \geq_{\text{lex}}$ -maximal in $\text{Aut}(A)\iota$?

Algorithmus: Definiere $L := \{\iota\}$ und initialisiere die Liste $N := \emptyset$. Laufe nun schrittweise durch die Vertretersysteme R_1, \dots, R_m und wende für ein festes R_i alle $g \in R_i$ auf alle $\iota' \in L$ an. Falls der i . Eintrag von einem resultierenden Element größer ist als ι_i , ist ι nicht \geq_{lex} -maximal in $\text{Aut}(A)\iota$, ansonsten füge alle Elemente deren i . Eintrag gleich ι_i ist zu N hinzu. Ersetze danach L durch N und entferne alle Elemente aus N .

Ausgabe: Entweder wurde auf diese Weise ein $\tau \in \text{Aut}(A)\iota$ mit $\tau >_{\text{lex}} \iota$ gefunden oder ι ist \geq_{lex} -maximal in $\text{Aut}(A)\iota$.

Ein Programm, welches diesen Ansatz verfolgt, wurde von Martin Leuner und mir implementiert. Als Eingabe für die Automorphismengruppe dient die Ausgabe von CARAT.

Bemerkung 2.13 ([Ple95], 3.3 Remark) Für $A \in \mathbb{Z}^{n \times n}$ symmetrisch und positiv definit sei $\tilde{\gamma}_k = \gamma_k / \text{Aut}(I_k)$. Nach Bemerkung 2.8 operiert $\text{Aut}(A)$ auf $\tilde{\gamma}_k$. Für $X \in \gamma_k$ sei

$$S(X) = \{g \in \text{Aut}(A) \mid gX = Xm \text{ für ein } m \in \text{Aut}(I_k)\}$$

der Stabilisator von X $\text{Aut}(I_k) \in \tilde{\gamma}_k$. Dann gilt

$$|\tilde{\gamma}| = \sum_{X^\alpha \in T} |\text{Aut}(A) : S(X^\alpha)|,$$

wobei T ein Vertretersystem von $\tilde{\gamma}$ ist (beispielsweise die Ausgabe von SIB).

Im Fall $k = n$ ist $S(X)$ die größte Untergruppe von $\text{Aut}(A)$, welche gleichzeitig auf dem orthonormalem Obergitter $(\mathbb{Z}^{1 \times n} X^{-1}, \phi)$ von $(\mathbb{Z}^{1 \times n}, \phi|_{\mathbb{Z}^{1 \times n} \times \mathbb{Z}^{1 \times n}})$ operiert, wobei

$$\phi : \mathbb{Z}^{1 \times n} X^{-1} \times \mathbb{Z}^{1 \times n} X^{-1} \rightarrow \mathbb{Z}, (l_1, l_2) \mapsto l_1 A l_2^{\text{tr}}.$$

Allgemein besteht $S(X)$ aus genau den Automorphismen, die die Gitterbasis, welche aus den Zeilen von X besteht, durch Drehung und Spiegelung (also eine Umorientierung des Koordinatensystems) auf eine weitere Basis abbildet.

Beispiel 2.14 (Fortsetzung von Beispiel 2.6) (i) Um alle 2025 Lösungen der Gleichung $XX^{\text{tr}} = 2A$ zu finden, müssen 258520 $\iota \in \mathbb{Z}_{\geq 0}^{120}$ auf Zulässigkeit getestet werden. Insgesamt hat der Algorithmus eine Laufzeit von von 17,4s. Die Gruppe

$\text{Aut}(A)$ operiert transitiv auf den Lösungen. Um diese mit Hilfe der Automorphismengruppe zu finden werden nun nur noch 933 $\iota \in \mathbb{Z}_{\geq 0}^{120}$ auf Zulässigkeit getestet, zusätzlich werden 339 Tupel mit Algorithmus 2.12 getestet. Die Laufzeit verringert sich auf 1,1s.

- (ii) $\text{Aut}(A)$ operiert wieder transitiv auf den Lösungen von $XX^{\text{tr}} = 3A$. Anstatt 2200671 werden nun nur noch 1212 $\iota \in \mathbb{Z}_{\geq 0}^{120}$ auf Zulässigkeit getestet, zusätzlich werden 702 Tupel mit Hilfe der Automorphismengruppe getestet. Die Laufzeit verringert sich von 3m6,6s auf 1,4s.

In beiden Fällen operiert $\text{Aut}(A)$ transitiv auf cc. Dies hat zur Folge, dass von allen $\iota \in \mathbb{Z}_{\geq 0}^{120}$ mit $\iota_1 = 0$ nur diejenigen mit genau einem Eintrag 1 und sonst 0 auf Zulässigkeit getestet werden.

3 Additive Zerlegungen von Gittern

3.1 Grundlagen

Die Definitionen und Sätze dieses Kapitels sind überwiegend aus [Ple94] und [Opg92] übernommen. Beweise, welche sich in diesen Arbeiten befinden, wurden an den entsprechenden Sätzen gekennzeichnet.

Ein beliebiges Gitter (L, ϕ) mit Gram-Matrix $\mathcal{G}(B)$ ist isometrisch zu (\mathbb{Z}^n, ϕ') , wobei ϕ' die von $\mathcal{G}(B)$ induzierte quadratische Form ist. Betrachtet man also alle Isometrie-Klassen von Gittern, kann ohne Einschränkung $L = \mathbb{Z}^n$ angenommen werden. Alle symmetrischen Bilinearformen $\phi : L \times L \rightarrow \mathbb{Z}$ bilden eine additive Gruppe $\text{Bil}(L)$, welche zur Gruppe aller symmetrischen ganzzahligen Matrizen $\mathbb{Z}_{\text{sym}}^{n \times n}$ isomorph ist. In dieser sind die Halbgruppen $\text{Bil}_{>0}(L)$ und $\text{Bil}_{\geq 0}(L)$ der positiv definiten und positiv semidefiniten Bilinearformen enthalten, welche zu den Halbgruppen der symmetrisch positiv definiten bzw. positiv semidefiniten Matrizen $\mathbb{Z}_{\text{sym}, >0}^{n \times n}$ und $\mathbb{Z}_{\text{sym}, \geq 0}^{n \times n}$ korrespondieren. Zusammen mit einer positiv definiten Bilinearform $\phi \in \text{Bil}_{>0}(L)$ wird (L, ϕ) zu einem ganzzahligen Gitter, es werden nun aber auch semidefinite Gitter (L, ϕ) für $\phi \in \text{Bil}_{\geq 0}$ zugelassen. Diese gehören im Gegensatz zu positiv definiten Gittern nicht mehr zu euklidischen Räumen.

Eine \mathbb{Z} -lineare Abbildung $\alpha : (L, \phi) \rightarrow (L, \phi')$ heißt zulässig, falls $\alpha\phi' = \phi$ gilt, mit $\alpha\phi' : L \times L \rightarrow \mathbb{Z} : (l_1, l_2) \mapsto \phi'(l_1\alpha, l_2\alpha)$. Die Addition in $\text{Bil}(L)$ kann wie folgt interpretiert werden: Für $\phi, \phi_1, \phi_2 \in \text{Bil}(L)$ ist die Abbildung

$$(L, \phi) \rightarrow (L, \phi_1) \perp (L, \phi_2), l \mapsto (l, l)$$

genau dann zulässig, falls $\phi = \phi_1 + \phi_2$ gilt. Die Gruppe $\text{GL}_n(\mathbb{Z})$ operiert auf $\text{Bil}(L)$ durch

$$\text{GL}_n(\mathbb{Z}) \times \text{Bil}(L) \rightarrow \text{Bil}(L), (\alpha, \phi) \mapsto \alpha\phi.$$

Diese Operation ist verträglich mit der Addition in $\text{Bil}(L)$ und lässt die Mengen $\text{Bil}_{\geq 0}(L)$ und $\text{Bil}_{>0}(L)$ invariant.

Definition 3.1 (i) Sei $\phi \in \text{Bil}_{\geq 0}(L)$. Für $i = 1, \dots, k$ seien (L_i, ϕ_i) positiv definite ganzzahlige Gitter, und die \mathbb{Z} -linearen Abbildungen $\pi_i : L \rightarrow L_i$ seien nicht die Nullabbildung. Eine zulässige Abbildung

$$\pi_1 \oplus \dots \oplus \pi_k : (L, \phi) \rightarrow (L_1, \phi_1) \perp \dots \perp (L_k, \phi_k), l \mapsto (l\pi_1, \dots, l\pi_k)$$

heißt additive Zerlegung von (L, ϕ) . Falls eine solche Zerlegung existiert heißt (L, ϕ) additiv zerlegbar, sonst additiv unzerlegbar.

(ii) $A \in \mathbb{Z}_{\text{sym}, \geq 0}^{n \times n}$ heißt additiv zerlegbar, falls A als Summe von zwei positiv semidefiniten Matrizen $A_1, A_2 \in \mathbb{Z}_{\text{sym}, \geq 0}^{n \times n}$ ungleich der Nullmatrix geschrieben werden kann. Falls eine solche Zerlegung existiert heißt A additiv zerlegbar, sonst additiv unzerlegbar.

(iii) $\phi \in \text{Bil}_{\geq 0}(L)$ heißt Blockform, falls für jede \mathbb{Z} -lineare Abbildung $\alpha : L \rightarrow \mathbb{Z}$ ungleich der Nullabbildung die Differenz $\phi - \alpha 1 = \phi - \alpha^2$ nicht positiv semidefinit ist, wobei $1 : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, (a, b) \mapsto ab$.

(iv) $A \in \mathbb{Z}_{\text{sym}, \geq 0}^{n \times n}$ heißt Blockform, falls $A - YY^{\text{tr}}$ nicht positiv semidefinit ist für jedes $Y \in \mathbb{Z}^{n \times 1}$ ungleich dem Nullvektor.

Jedes additiv unzerlegbare Gitter und jede additiv unzerlegbare Matrix ist eine Blockform.

Bemerkung 3.2 Sei (L, ϕ) ein Gitter mit Gitterbasis B und sei $A = \mathcal{G}(B)$ eine Gram-Matrix von L . Dann gilt:

(i) (L, ϕ) ist genau dann additiv zerlegbar, wenn A additiv zerlegbar ist.

(ii) (L, ϕ) ist genau dann eine Blockform, wenn A eine Blockform ist.

Für ein positiv definites Gitter (L, ϕ) mit Gram-Matrix A ist nach Bemerkung 2.4 A genau dann eine Blockform, wenn die Menge $\{Y \in \mathbb{Z}^{n \times 1} \mid Y^{\text{tr}} A^{-1} Y \leq 1\}$ leer ist. Da A^{-1} allerdings eine Gram-Matrix des dualen Gitters $(L^\#, \phi)$ ist, gilt:

Lemma 3.3 Ein positiv definites Gitter (L, ϕ) ist genau dann eine Blockform, wenn $\min(L^\#, \phi) > 1$ ist.

Bemerkung 3.4 ([Opg92], Bemerkung 1.3.2) Sei $\phi \in \text{Bil}_{> 0}(L)$. Dann gilt:

(i) Falls (L, ϕ) orthogonal zerlegbar ist, dann ist (L, ϕ) additiv zerlegbar.

(ii) Falls $\det(L, \phi) = 1$ ist, dann ist (L, ϕ) genau dann orthogonal zerlegbar, falls es additiv zerlegbar ist.

BEWEIS (i) Folgt sofort aus Bemerkung 3.2 und Bemerkung 1.16.

(ii) Sei (L, ϕ) unimodular und orthogonal unzerlegbar. Angenommen es existiert eine additive Zerlegung $(L, \phi) \rightarrow (L_1, \phi_1) \perp \dots \perp (L_k, \phi_k)$. Dann ist das Bild \tilde{L} von L isometrisch zu L , also ist auch \tilde{L} orthogonal unzerlegbar und hat Determinante 1. Nach dem Satz über die eindeutige orthogonale Zerlegung von Gittern folgt nun $\tilde{L} \subset L_i$ für ein i , also nach Definition der additiven Zerlegung $k = 1$ und $L = L_1$. \square

Die Gruppe $\mathrm{GL}_n(\mathbb{Z})$ operiert auf $\mathbb{Z}_{\mathrm{sym}, \geq 0}^{n \times n}$ durch

$$\mathrm{GL}_n(\mathbb{Z}) \times \mathbb{Z}_{\mathrm{sym}, \geq 0}^{n \times n} \rightarrow \mathbb{Z}_{\mathrm{sym}, \geq 0}^{n \times n}, (g, A) \mapsto gAg^{\mathrm{tr}}.$$

Additive Zerlegbarkeit und Blockform sind Invarianten dieser Operation. Die Abbildung

$$\mathrm{Bil}_{\geq 0}(L) \rightarrow \mathbb{Z}_{\mathrm{sym}, \geq 0}^{n \times n}, \phi \mapsto (\phi(e_i, e_j))_{1 \leq i, j \leq n}$$

ist eine $\mathrm{GL}_n(\mathbb{Z})$ -Ähnlichkeit, wobei (e_1, \dots, e_n) die Standardbasis des \mathbb{Z}^n bezeichnet. Anstelle der Isometrieklassen n -dimensionaler, additiv unzerlegbarer Gitter kann man also die $\mathrm{GL}_n(\mathbb{Z})$ -Bahnen auf $\mathbb{Z}_{\mathrm{sym}, \geq 0}^{n \times n}$ betrachten. Die nächste Bemerkung zeigt, dass man hierbei ohne Einschränkung von positiv definiten Matrizen ausgehen kann.

Bemerkung 3.5 Sei $A \in \mathbb{Z}_{\mathrm{sym}, \geq 0}^{n \times n}$. Dann existiert ein $g \in \mathrm{GL}_n(\mathbb{Z})$ und ein $A' \in \mathbb{Z}^{\mathrm{Rang}(A) \times \mathrm{Rang}(A)}$ symmetrisch und positiv definit mit

$$gAg^{\mathrm{tr}} = \left(\begin{array}{c|c} A' & 0 \\ \hline 0 & 0 \end{array} \right).$$

Insbesondere ist A genau dann additiv unzerlegbar, wenn A' additiv unzerlegbar ist.

BEWEIS Sei $b = (b_1, \dots, b_n)$ ein Basisvektor von $\mathrm{Kern}(A) \leq \mathbb{Q}^{1 \times n}$. Dann gilt o.B.d.A. $b \in \mathbb{Z}^{1 \times n}$ und $gg^{\mathrm{T}}(b_1, \dots, b_n) = 1$. Mit Hilfe des ganzzahligen Gaußalgorithmus existiert ein $\tilde{g} \in \mathrm{GL}_n(\mathbb{Z})$ mit $\tilde{g}b = (0, \dots, 0, 1)$. Dann gilt

$$\tilde{g}A\tilde{g}^{\mathrm{tr}} = \left(\begin{array}{c|c} \tilde{A} & 0 \\ \hline 0 & 0 \end{array} \right)$$

mit $\tilde{A} \in \mathbb{Z}^{(n-1) \times (n-1)}$ symmetrisch und positiv semidefinit. Nun kann o.B.d.A. \tilde{A} betrachtet werden. Wenn man dies iterativ fortführt erhält man das gesuchte A' . \square

Satz 3.6 (vgl. [Mor37]) Für alle $n \in \mathbb{N}$ gibt es bis auf Isometrie nur endlich viele positiv definite, ganzzahlige Gitter (L, ϕ) vom Rang n , wobei ϕ eine Blockform ist. Insbesondere gibt es nur endlich viele Isometrieklassen n -dimensionaler positiv definiten, ganzzahliger, additiv unzerlegbarer Gitter, und deshalb gibt es unter der Operation von $\mathrm{GL}_n(\mathbb{Z})$ auch nur endlich viele Bahnen additiv unzerlegbarer Matrizen in $\mathbb{Z}_{\mathrm{sym}, \geq 0}^{n \times n}$.

BEWEIS Nach dem Satz von HERMITE (vgl. [PZ89], S. 197) existiert für jedes n eine Konstante κ_n , so dass für jedes n -dimensionale, positiv definite Gitter (L', ϕ') vom Rang n gilt:

$$\min(L', \phi') \leq \kappa_n \det(L', \phi').$$

Ein positiv semidefinites Gitter (L, ϕ) ist genau dann eine Blockform, wenn die Matrix $(\phi(e_i, e_j))_{1 \leq i, j \leq n}$ es ist. Nach Bemerkung 3.5 kann also ohne Einschränkung angenommen werden, dass (L, ϕ) positiv definit ist. Dann gilt $\min(L^\#, \phi) \leq \kappa_n \det(L^\#, \phi) = \kappa_n \det(L, \phi)^{-1}$, also ist $\min(L^\#, \phi) \det(L, \phi) \leq \kappa_n$. Falls $\det(L, \phi) \geq \kappa_n$ gilt, muss also $\min(L^\#, \phi) \leq 1$ gelten, insbesondere ist dann (L, ϕ) keine Blockform. Es existieren für eine gegebene Dimension und Determinante nur endlich viele Isometrieklassen von Gittern (vgl. [Sie56], Seite 67), daraus folgt die Behauptung. \square

Beispiel 3.7 *Bis Dimension 8 existieren nur 4 Isometrieklassen additiv unzerlegbarer Gitter: \mathbb{Z} und die Wurzelgitter E_6 , E_7 und E_8 (vgl. [Ko39], [Ko42b], [Ko42a]). In den Dimensionen 1 bis 5 existieren noch nicht einmal Blockformen, denn jedes (L, ϕ) mit $\dim(L, \phi) \leq 5$ lässt sich in $\perp_{i=1}^n \mathbb{Z}$ für ein $n \leq \dim(L, \phi) + 3$ einbetten (vgl. [Ko37]). Es muss also $\min(L^\#, \phi) \leq 1$ gelten, sonst würde der in Kapitel 3 beschriebene Algorithmus keine Einbettung finden.*

Der nächste Satz liefert ein hinreichendes Kriterium dafür, dass ein ein Gitter additiv unzerlegbar ist.

Satz 3.8 ([Opg92], Satz 1.3.9 bzw. [Ple94], Proposition III.3) *Sei (L, ϕ) ein positiv definites, ganzzahliges Gitter, so dass gilt:*

- (i) ϕ ist eine Blockform, d.h. $\min(L^\#, \phi) > 1$.
- (ii) Das Teilgitter $(\langle L_{\leq 3} \rangle_{\mathbb{Z}}, \phi)$ von (L, ϕ) , welches von allen $l \in L$ mit $\phi(l, l) \leq 3$ erzeugt wird, ist orthogonal unzerlegbar und $\dim(L, \phi) - \dim(\langle L_{\leq 3} \rangle_{\mathbb{Z}}, \phi) \leq 5$.

Dann ist (L, ϕ) additiv unzerlegbar.

BEWEIS Angenommen (L, ϕ) ist additiv zerlegbar. Dann gilt $\phi = \phi_1 + \phi_2$ mit $0 \neq \phi_i \in \text{Bil}_{\geq 0}(L)$ für $i = 1, 2$. Für ein $0 \neq x \in L$ mit $\phi(x, x) \leq 3$ muss dann gelten $\phi_1(x, x) = 0$ oder $\phi_2(x, x) = 0$. Denn anderenfalls wäre o.B.d.A. $\phi_1(x, x) = 1$, und in diesem Fall ist (L, ϕ_1) orthogonal zerlegbar mit $(\mathbb{Z}, 1)$ als orthogonalem Summanden, wobei $1 : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, (a, b) \mapsto ab$. Damit ist $\phi > \phi_1 \geq \delta^2$ für eine lineare Form δ auf L , was jedoch wegen Lemma 3.3 ein Widerspruch zu (i) ist. Sei also $0 \neq x_0 \in L$ mit $\phi(x_0, x_0) \leq 3$ und o.B.d.A. $\phi_1(x_0, x_0) = 0$. Dann ist $\phi_1(x, x) = 0$ für alle $x \in L$ mit $\phi(x, x) \leq 3$. Dies gilt für alle x mit $\phi(x_0, x) \neq 0$, da gelten muss

$$0 \leq \det \begin{pmatrix} \phi_1(x_0, x_0) & \phi_1(x_0, x) \\ \phi_1(x_0, x) & \phi_1(x, x) \end{pmatrix} = -\phi_1(x_0, x)^2,$$

also folgt $\phi_1(x_0, x) = 0$. Wenn man nun annimmt, dass $\phi_1(x, x) \neq 0$, dann muss gelten $\phi_2(x, x) = 0$, und dasselbe Argument liefert $\phi_2(x_0, x) = 0$. Das aber führt zum Widerspruch $0 \neq \phi(x_0, x) = \phi_1(x_0, x) + \phi_2(x_0, x) = 0 + 0$. Da $\langle L_{\leq 3} \rangle_{\mathbb{Z}}$ orthogonal unzerlegbar ist, gilt $\phi_1(x, x) = 0$ für alle $x \in L$ mit $\phi(x, x) \leq 3$. Also ist ϕ_1 gleich 0 auf $\langle L_{\leq 3} \rangle_{\mathbb{Z}}$ und auch auf $L' = L \cap \mathbb{Q}\langle L_{\leq 3} \rangle_{\mathbb{Z}}$. Aber nach Voraussetzung ist $\dim(L/L') \leq 5$, deshalb ist ϕ_1 die Summe von Quadraten von linearen Formen (vgl. [Ko37]). In diesem Fall aber wäre ϕ von der Form $\delta^2 + \phi'$ mit einer linearen Form δ auf L und $\phi' \in \text{Bil}_{\geq 0}(L)$, was wiederum einen Widerspruch zu (i) bedeutet. \square

Lemma 3.9 *Sei (L, ϕ) ein positiv definites, ganzzahliges Gitter mit Gitterbasis B und Gram-Matrix $A = \mathcal{G}(B)$. Dann gilt:*

- (i) *Falls (L, ϕ) additiv unzerlegbar ist, dann ist jedes Obergitter von (L, ϕ) , welches dieselbe Dimension hat, additiv unzerlegbar.*
- (ii) *Falls (L, ϕ) in ein orthogonal zerlegbares Gitter $(L', \phi') = (L_1, \phi_1) \perp \dots \perp (L_k, \phi_k)$ einbettet mit $\dim(L_i, \phi_i) < \dim(L, \phi)$ für $i = 1, \dots, k$, dann ist (L, ϕ) additiv zerlegbar.*

BEWEIS (i) Sei $(\tilde{L}, \tilde{\phi})$ ein Obergitter von (L, ϕ) mit Gitterbasis \tilde{B} und Gram-Matrix $\tilde{A} = \mathcal{G}(\tilde{B})$. Falls $(\tilde{L}, \tilde{\phi})$ additiv zerlegbar ist, existieren $\tilde{A}_1, \tilde{A}_2 \in \mathbb{Z}_{\text{sym}}^{n \times n}$ positiv semidefinit ungleich der Nullmatrix mit $\tilde{A} = \tilde{A}_1 + \tilde{A}_2$. Da $(\tilde{L}, \tilde{\phi})$ ein Obergitter von (L, ϕ) ist, gilt $A = (\text{Bid}_{\tilde{B}})\tilde{A}(\text{Bid}_{\tilde{B}})^{\text{tr}} = (\text{Bid}_{\tilde{B}})\tilde{A}_1(\text{Bid}_{\tilde{B}})^{\text{tr}} + (\text{Bid}_{\tilde{B}})\tilde{A}_2(\text{Bid}_{\tilde{B}})^{\text{tr}}$, also ist (L, ϕ) additiv zerlegbar.

(ii) Sei A_i eine Gram-Matrix von (L_i, ϕ_i) für $i = 1, \dots, k$ und sei B' eine Basis von (L', ϕ') mit $\mathcal{G}(B') = \text{Diag}(A_1, \dots, A_k)$. Da (L, ϕ) in (L', ϕ') einbettet, gilt

$$A = (\text{Bid}_{B'}) \text{Diag}(A_1, \dots, A_k) (\text{Bid}_{B'})^{\text{tr}}.$$

Falls (L, ϕ) additiv unzerlegbar ist, muss

$$(\text{Bid}_{B'}) \text{Diag}(0, \dots, 0, A_i, 0, \dots, 0) (\text{Bid}_{B'})^{\text{tr}} = 0$$

gelten für alle i mit genau einer Ausnahme. Dann würde aber (L, ϕ) in ein Gitter kleinerer Dimension einbetten. \square

Obergitter, die orthogonal zerlegbar sind, können mit Hilfe des dualen Gitters gesucht werden. Falls (L, ϕ) ein ganzzahliges Gitter ist, dann ist $L^\# / L$ eine endliche abelsche Gruppe der Ordnung $\det(L, \phi)$. (L', ϕ) ist genau dann ein ganzzahliges Gitter mit $L \leq L' \leq L^\#$, wenn $U = L' / L$ eine Untergruppe von $L^\# / L$ ist mit $\overline{\Phi}|_{U \times U} = \{\overline{0}\}$, wobei

$$\overline{\Phi} : L^\# / L \times L^\# / L \rightarrow \mathbb{Q} / \mathbb{Z}, (\overline{l_1}, \overline{l_2}) \mapsto \phi(l_1, l_2) + \mathbb{Z}.$$

Die Abbildung ist wohldefiniert, da (L, ϕ) ein ganzzahliges Gitter ist. Maximale Untergruppen in $L^\# / L$ mit dieser Eigenschaft können leicht konstruiert werden:

Lemma 3.10 Sei (L, ϕ) ein ganzzahliges Gitter und sei $V := \{\bar{l} \in L^\# / L \mid \phi(l, l) \in \mathbb{Z}\}$. Definiere einen Graphen $G = (V, E)$ auf V durch

$$E(\bar{l}_1, \bar{l}_2) = \begin{cases} 1 & \bar{l}_1 \neq \bar{l}_2 \text{ und } \phi(l_1, l_2) \in \mathbb{Z} \\ 0 & \text{sonst} \end{cases}$$

für alle $\bar{l}_1, \bar{l}_2 \in V$. Dann ist U genau dann eine maximale Untergruppe von $L^\# / L$ mit $\bar{\Phi}|_{U \times U} = \{\bar{0}\}$, wenn $(U, E|_{U \times U})$ ein maximal vollständiger Teilgraph von G ist.

BEWEIS „ \Leftarrow “: Sei $(U, E|_{U \times U})$ ein maximal vollständiger Teilgraph von G . Dann ist U nicht leer und für alle $\bar{l}, \bar{l}_1, \bar{l}_2 \in U$ gilt $\phi(l_1 - l_2, l) = \phi(l_1, l) - \phi(l_2, l) \in \mathbb{Z}$. Da $(U, E|_{U \times U})$ maximal vollständig ist, gilt also $\bar{l}_1 - \bar{l}_2 \in U$. Also ist U eine Untergruppe von $L^\# / L$, die offensichtlich maximal ist. Nach Konstruktion gilt $\bar{\Phi}|_{U \times U} = \{\bar{0}\}$.

„ \Rightarrow “: Sei U eine maximale Untergruppe von $L^\# / L$ mit $\bar{\Phi}|_{U \times U} = \{\bar{0}\}$. Dann gilt $\phi(l_1, l_2) \in \mathbb{Z}$ für alle $\bar{l}_1, \bar{l}_2 \in U$, also ist $(U, E|_{U \times U})$ ein vollständiger Teilgraph von G . Falls dieser echt in einem vollständigem Teilgraphen von G liegen würde, wäre U nicht maximal. \square

Die maximal vollständigen Teilgraphen können mit dem Bron-Kerbosch-Algorithmus gefunden werden (vgl. [TTT06]). Fügt man zu die Zeilen einer Gram-Matrix zu einer solchen maximalen Untergruppe hinzu und berechnet eine \mathbb{Z} -Basis, erhält man die Basis eines maximal ganzzahligen Gitters (L', ϕ) mit $L \leq L' \leq L^\#$. Falls dieses orthogonal zerlegbar ist, dann ist L additiv zerlegbar.

Beispiel 3.11 In der Notation von [CS99], Kapitel 6, S. 159, sind alle laminierten Gitter Λ in den Dimensionen 9 bis 17 additiv zerlegbar. Mit Lemma 3.10 lassen sich maximal ganzzahlige Obergitter Λ' von Λ in $\Lambda^\#$ berechnen, die orthogonal zerlegbar sind.

Λ	Λ'	Λ	Λ'
Λ_9	$\bigoplus_{i=1}^8 \mathbb{Z} \perp A_1$	Λ_{13}^{\min}	$E_8 \perp \bigoplus_{i=1}^5 \mathbb{Z}$ $D_{12}^+ \perp \mathbb{Z}$
Λ_{10}	$\bigoplus_{i=1}^8 \mathbb{Z} \perp A_2$ $E_8 \perp A_2$	$\Lambda_{13}^{\text{mid}}$	$E_8 \perp \bigoplus_{i=1}^5 \mathbb{Z}$ $D_{12}^+ \perp \mathbb{Z}$
Λ_{11}^{\min}	$\bigoplus_{i=1}^{11} \mathbb{Z}$ $E_8 \perp \bigoplus_{i=1}^3 \mathbb{Z}$	Λ_{13}^{\max}	$\bigoplus_{i=1}^{13} \mathbb{Z}$ $E_8 \perp \bigoplus_{i=1}^5 \mathbb{Z}$ $D_{12}^+ \perp \mathbb{Z}$
Λ_{11}^{\max}	$\bigoplus_{i=1}^{11} \mathbb{Z}$ $E_8 \perp \bigoplus_{i=1}^3 \mathbb{Z}$	Λ_{14}	$E_8 \perp E_6$
Λ_{12}^{\min}	$E_8 \perp \bigoplus_{i=1}^4 \mathbb{Z}$	Λ_{15}	$E_8 \perp E_7$
$\Lambda_{12}^{\text{mid}}$	$\bigoplus_{i=1}^{12} \mathbb{Z}$ $E_8 \perp \bigoplus_{i=1}^4 \mathbb{Z}$	Λ_{16}	$E_8 \perp E_8$
Λ_{12}^{\max}	$\bigoplus_{i=1}^{12} \mathbb{Z}$ $E_8 \perp \bigoplus_{i=1}^4 \mathbb{Z}$	Λ_{17}	$\mathbb{Z} \perp L^1$

In den Dimensionen 18 bis 24 lässt sich weder Satz 3.8 anwenden, noch existiert ein maximal ganzzahliges, orthogonal zerlegbares Obergitter in $\Lambda^\#$.

3.2 Ergebnisse

Additiv unzerlegbare Gitter können konstruiert werden, indem man aus einem positiv definiten Gitter alle Blockformen bildet und diese auf additive Zerlegbarkeit untersucht. In der Implementierung von Algorithmus 2.5 wurde zusätzlich die Option eingefügt, für ein $A \in \mathbb{Z}^{n \times n}$ symmetrisch und positiv definit alle $A' = A - XX^{\text{tr}}$ für ein $X \in \mathbb{Z}^{n \times k}$ aus zugegeben, so dass A' positiv semidefinit und eine Blockform ist. Die Automorphismengruppe $\text{Aut}(A)$ operiert auf der Menge aller Blockformen die sich so berechnen lassen, zusammen mit der in Kapitel 2, Abschnitt 2 beschriebenen Methode lässt sich

¹ L ist isometrisch zu $U_{(16,1,2)}$ - vgl. Kapitel 4.

also direkt eine Transversale dieser Operation bestimmen. Allerdings können natürlich Blockformen, die nicht in einer Bahn liegen, trotzdem isometrisch sein. Für alle Blockformen werden dann mit Lemma 3.5 ein positiv definites Gitter in der entsprechenden Isometrie Klasse gesucht, welches anschließend auf additive Zerlegbarkeit getestet wird.

3.2.1 Teilgitter von E_6 , E_7 und E_8

Zuerst wurden Teilgitter der Wurzelgitter E_6 , E_7 und E_8 vom Index 2, 3 und 5 betrachtet. Mit Hilfe von Satz 1.12 und Bemerkung 1.14 ist es möglich die Bahnen der Teilgitter von gegebenem Primzahlindex unter der Operation der Automorphismengruppe zu bestimmen, diese Bahnen wurden dann zu Isometrie Klassen zusammen gefasst. Anschließend wurde für jeden Vertreter mit SIB untersucht, ob eine Einbettung in ein $\mathbb{Z}_{\text{orth}}^k$ existiert und welche Blockformen sich bilden lassen, jeweils unter der Operation der Automorphismengruppe. Für jede Blockform wurde dann entschieden, ob diese additiv unzerlegbar ist. Die Determinante ist als Zerlegung in die Elementarteiler angegeben, $|cc|$ gibt an aus wie vielen Spaltenkandidaten sich die möglichen Einbettungen zusammensetzen können. „Einbettungen in (k_1, k_2, \dots) “ bedeutet, dass unter der Operation der Automorphismengruppe jeweils eine Einbettung in $\mathbb{Z}_{\text{orth}}^{k_1}, \mathbb{Z}_{\text{orth}}^{k_2}, \dots$ existiert.

Teilgitter von E_6 :

Index 2: 2 Teilgitter

$\det = 2 \cdot 6$	$\det = 2 \cdot 6$
$ cc = 6$	$ cc = 7$
Einbettung in (8)	Einbettung in (8)
keine Blockformen	keine Blockformen

Index 3: 5 Teilgitter

$\det = 27$	$\det = 3 \cdot 9$	$\det = 27$
$ cc = 2$	$ cc = 14$	$ cc = 8$
keine Einbettungen	Einbettung in (9)	Einbettung in (9)
Blockformen: E_6	Blockformen: E_6	keine Blockformen

$\det = 3 \cdot 9$	$\det = 3^3$
$ cc = 3$	$ cc = 9$
keine Einbettungen	Einbettung in (9)
Blockformen: $2 \times E_6$	keine Blockformen

Index 5: 8 Teilgitter

det = 75
|cc| = 4
keine Einbettungen
Blockformen: $10 \times E_6$

det = 75
|cc| = 15
Einbettungen in (9, 11, 14, 17)
Blockformen: $5 \times E_6$

det = 75
|cc| = 15
Einbettungen in (9, 9, 11, 11)
Blockformen: $3 \times E_6$

det = $5 \cdot 15$
|cc| = 21
Einbettungen in (9, 10, 11, 14)
keine Blockformen

det = 75
|cc| = 16
Einbettungen in (9, 9, 10, 11)
keine Blockformen

det = 75
|cc| = 6
keine Einbettungen
Blockformen: $8 \times E_6$

det = $5 \cdot 15$
|cc| = 24
Einbettung in (9)
Blockformen: $4 \times E_6$

det = 75
|cc| = 16
Einbettungen in (9, 10, 11)
Blockformen: $2 \times E_6$

Teilgitter von E_7 :

Index 2: 3 Teilgitter

det = 8
|cc| = 1
keine Einbettungen
Blockformen: E_7

det = 8
|cc| = 8
Einbettung in (8)
keine Blockformen

det = 2^3
|cc| = 7
Einbettung in (7)
keine Blockformen

Index 3: 5 Teilgitter

det = $3 \cdot 6$
|cc| = 2
keine Einbettungen
Blockformen: $2 \times E_6$

det = 18
|cc| = 8
Einbettung in (8)
keine Blockformen

det = 18
|cc| = 2
keine Einbettungen
Blockformen: $2 \times E_7$

det = $3 \cdot 6$
|cc| = 9
Einbettung in (9)
keine Blockformen

det = 18
|cc| = 3
keine Einbettungen
Blockformen: E_6, E_7

Index 5: 10 Teilgitter

det = 50
|cc| = 4
keine Einbettungen
Blockformen: $8 \times E_7$

det = 50
|cc| = 16
Einbettungen in (9, 11, 14)
keine Blockformen

det = 50
|cc| = 3
keine Einbettungen
Blockformen: $5 \times E_7$

det = 50
|cc| = 10
Einbettungen in (9, 11)
Blockformen: E_7

det = 50
|cc| = 16
Einbettungen in (9, 11)
Blockformen: $2 \times E_7$

det = $5 \cdot 10$
|cc| = 12
Einbettungen in (10, 11)
keine Blockformen

det = 50
|cc| = 6
keine Einbettungen
Blockformen: $3 \times E_6, 2 \times E_7$

det = 50
|cc| = 17
Einbettungen in (9, 9)
Blockformen: $2 \times E_6, E_7$

det = 50
|cc| = 5
keine Einbettungen
Blockformen: $3 \times E_6, 2 \times E_7$

det = 50
|cc| = 13
Einbettungen in (9, 10)
Blockformen: E_7

Teilgitter von E_8 :

Index 2: 2 Teilgitter

det = 2^2	det = 2^2
cc = 8	cc = 1
Einbettung in (8)	keine Einbettungen
keine Blockformen	Blockformen: E_7

Index 3: 4 Teilgitter

det = 9	det = 9	det = 3 ²
cc = 1	cc = 2	cc = 3
keine Einbettungen	keine Einbettungen	keine Einbettungen
Blockformen: E_8	Blockformen: $2 \times E_8$	Blockformen: E_6

det = 9
|cc| = 9
Einbettung in (9)
keine Blockformen

Index 5: 8 Teilgitter

det = 25	det = 25	det = 25
cc = 2	cc = 3	cc = 4
keine Einbettungen	keine Einbettungen	keine Einbettungen
Blockformen: $2 \times E_8$	Blockformen: $5 \times E_8$	Blockformen: $E_7, 2 \times E_8$

det = 25	det = 5 ²	det = 5 ²
cc = 7	cc = 4	cc = 10
keine Einbettungen	keine Einbettungen	Einbettung in (10)
Blockformen: $2 \times E_6, E_8$	Blockformen: $2 \times E_8$	keine Blockformen

det = 25	det = 25
cc = 9	cc = 10
Einbettung in (11)	Einbettung in (9)
keine Blockformen	Blockformen: E_7

3.2.2 Konstruktion von Blockformen

Danach wurden alle Blockformen bestimmt, die sich aus den Gittern der Dimension 12 bis 16 aus [NS] und den Gittern aus [PP85]² und [PP93] ab Dimension 12 bestimmen lassen. Für ein Gitter (L, ϕ) werden bis auf Isometrie alle Gitter (L, ϕ') angegeben, wobei ϕ' eine Blockform ist, die sich mit SIB aus ϕ konstruieren lassen. Im Fall $(L, \phi) = (L, \phi')$ ist ϕ bereits eine Blockform. Falls man mit Satz 3.8 zeigen kann, dass (L, ϕ') additiv unzerlegbar ist, wird es mit $U_{(n,d,s)}$ bezeichnet, wobei n die Dimension und d

²In diesem Paper ist die Matrix Q'_{19} fälschlicherweise nicht symmetrisch, daher konnten nicht alle angegebenen Gitter betrachtet werden.

die Determinante von (L, ϕ') ist und $\min(L^\#, \phi') = \frac{s}{d}$ gilt. Im Fall $n \leq 11$ wurden diese bereits von J. Opgenorth in [Opg92], Kapitel 3 angegeben, für $n \geq 12$ befindet sich eine Beschreibung der Gitter in Kapitel 4. Falls man mit Hilfe von Lemma 3.10 ein orthogonal zerlegbares Obergitter findet wurde dieses angegeben, sonst ist keine Aussage über die additive Zerlegbarkeit einer Blockform möglich. Falls die Determinante des Gitters zu groß ist, kann es passieren, dass die benutzten Algorithmen eine lange Laufzeit haben, dann wurde die Rechnung abgebrochen.

Gitter aus [NS]:

Dimension 12

(L, ϕ)	(L, ϕ')
K12	K12 additiv zerlegbar: $\hookrightarrow E_6 \perp E_6$
A12	–
D12	–
D12+	D12+ = $U_{(12,1,2)}$
O12	$U_{(10,9,12)}$
C6.PSU(4,3).(C2 × C2)	C6.PSU(4,3).(C2 × C2) additiv zerlegbar: $\hookrightarrow E_6 \perp E_6$
$((3+^{1+2}):SL(2,3)) \times SL(2,3).C2$	E_8
$(C2 \times D10 \times A5):C2$	$U_{(10,5,7)}$
$(SL(2,5) \times SL(2,3)).C2$	E_8
A2 × M6,2	Rechnung abgebrochen
$(C2 \times C3.Alt6).(C2 \times C2)$	Rechnung abgebrochen
$(PSL(2,7) \times D8):C2$	–
$(PSL(2,7) \times D8):C2$	Rechnung abgebrochen
A2 × A6	$U_{(10,9,12)}$ $U_{(12,9,12)}$
A2 × A6 ²	Rechnung abgebrochen
A1 ⁶ .sqrt(3)A1 ⁶	D12+ = $U_{(12,1,2)}$
A2 ³ .sqrt(3)A2 ³	E_6
A3 ² .sqrt(3)A3 ²	E_8 $U_{(10,3,4)}$ $U_{(12,9,12)}$

(L, ϕ)	(L, ϕ')
A6.sqrt(3)A6	E_8 $U_{(10,3,4)}$
D6.sqrt(D6)	$D_{12+} = U_{(12,1,2)}$ $U_{(10,3,4)}$ E_8
E6.sqrt(3)E6	E_6 $E_6 \perp E_6$
G2.A5.sqrt(3)A5	E_6 $U_{(10,9,12)}$
$G_2^2.D_4.sqrt(3)D_4$	E_6 E_8
G_2^6	—

Dimension 13

(L, ϕ)	(L, ϕ')
Kappa13	$U_{(13,243,324)}$
D13	—
A13	—
$C_2 \times L(3,3) : C_2$	$U_{(10,3,4)}$
Lambda13_max	-
Lambda13_mid	E_8
Lambda13_min	E_8
$C_2 \times PSL(2,25) : C_2$	Rechnung abgebrochen

Dimension 14

(L, ϕ)	(L, ϕ')
A14	–
D14	–
$E7^{\wedge}2+$	$E7^{\wedge}2+ = U_{(14,1,2)}$
Lambda14	Lambda14 additiv zerlegbar: $\hookrightarrow E_8 \perp E_6$
$C2 \times G(2,3)$	$C2 \times G(2,3)$ keine Aussage möglich
$A2 \times E7$	$U_{(13,243,324)}$
$C2 \times S7$	–
$C2 \times S8$	$C2 \times S8$ keine Aussage möglich
Kappa14	$U_{(13,27,36)}$
$(SU(3,3 \times C4) \cdot C2)$	$U_{(14,576,768)}$
Lambda14.2	E_8
Lambda14.3	E_8
Lambda14.4	$U_{(12,16,24)}$
Kappa14.2	$U_{(13,243,324)}$

Dimension 15

(L, ϕ)	(L, ϕ')
A15	–
A15+	$A15+ = U_{(15,1,2)}$
$C2 \times Sp(6,2)$	$C2 \times Sp(6,2) = U_{(15,192,320)}$
D15	–
Kappa15	Kappa15 keine Aussage möglich
Lambda2A6	–
Lambda2E6	$Lambda2E6 = U_{(15,243,324)}$
Lambda15	Lambda15 additiv zerlegbar: $\hookrightarrow E_8 \perp E_7$
Lambda15.2	$U_{(14,192,256)}$
Lambda15.3	E_8
Lambda15.4	$U_{(14,192,256)}$
Kappa15.2	$U_{(13,27,36)}$

Dimension 16

(L, ϕ)	(L, ϕ')
Lambda16	Lambda16 additiv zerlegbar: $\hookrightarrow E_8 \perp E_8$
Lambda16.2	$U_{(15,128,192)}$
Lambda16.3	$U_{(14,48,64)}$
Lambda16.4	Lambda16.4 keine Aussage möglich
Kappa16	Kappa16 keine Aussage möglich
Kappa16.2	Kappa16.2 additiv zerlegbar: $\hookrightarrow E_8 \perp E_8$
Kappa16.3	Kappa16.3 additiv zerlegbar: $\hookrightarrow E_8 \perp E_8$
BW16odd	$BW16odd = U_{(16,256,384)}$
OBW16	$OBW16 = U_{(16,64,128)}$
A16	-
D16	-
$E_8 \times A_2$	$E_8 \times A_2$ keine Aussage möglich
$A_4 \times F_4$	Rechnung abgebrochen
$(SL(2,9) \times SL(2,9)).(C_2 \times C_2)$	$(SL(2,9) \times SL(2,9)).(C_2 \times C_2)$ keine Aussage möglich
$((Sp(4,3) \times C_3) \times SL(2,3)).C_2$	Rechnung abgebrochen
$((SL(2,5) \times SL(2,5)) : C_2 \times D_{10}) : C_2$	Rechnung abgebrochen
$C_2 \times (S_5 \times S_5) : C_2$	$C_2 \times (S_5 \times S_5) : C_2$ keine Aussage möglich
C2.Alt10	C2.Alt10 keine Aussage möglich
$(SL(2,5) \times (D_8 \times Q_8)).Alt_5.C_2$	Rechnung abgebrochen

Gitter aus [PP85]

(L, ϕ)	(L, ϕ')
Lambda13a	E_8
Lambda13b	E_8
Lambda14a	$U_{(12,4,6)}$
Lambda14b	E_8
Lambda14c	E_8
Lambda14e	$U_{(12,4,6)}$
Lambda15a	$U_{(14,48,64)}$
Lambda15b	$U_{(14,48,64)}$
Lambda15f	$U_{(14,48,64)}$
Lambda16a	$U_{(15,32,48)}_2$
Lambda16b	$U_{(15,32,48)}_2$
Lambda16f	$U_{(15,32,48)}_2$
Lambda17a	$U_{(16,16,32)}$
Lambda17h	$U_{(16,16,32)}$
Lambda18a	$U_{(18,48,64)}$
Lambda18e	$U_{(18,48,64)}$
Lambda18f	$U_{(16,4,8)}$
Lambda19a	$U_{(19,32,48)}$
Lambda19b	$U_{(19,32,48)}$
Lambda19d	$U_{(16,1,2)}$
Lambda20a	$U_{(20,16,32)}$
Lambda20b	$U_{(20,16,32)}$
Lambda20c	$U_{(19,8,12)}$
Lambda21a	$U_{(21,8,16)}$
Lambda21b	$U_{(21,8,16)}$
Lambda22a	$U_{(22,8,3)}$
Lambda22b	$U_{(22,8,3)}$

Gitter aus [PP93]

(L, ϕ)	(L, ϕ')
Kappa13	$U_{(13,243,324)}$
Kappa14.2'	$U_{(13,243,324)}$
Kappa15.2'	$U_{(13,27,36)}$
Kappa14.1'	$U_{(13,27,36)}$
Kappa16.2'	Kappa16.2' additiv zerlegbar: $\hookrightarrow E_8 \perp E_8$
Kappa16.3'	Kappa16.3' additiv zerlegbar: $\hookrightarrow E_8 \perp E_8$
Kappa17.2'	Blockformen
Kappa18'	keine Aussage über additive
Kappa19'	Zerlegbarkeit möglich
Kappa20'	
Kappa21'	
Lambda22	
Kappa15.1	
Kappa16.1	
Kappa17.1	
Kappa18.1	

3.2.3 Obergitter additiv unzerlegbarer Gitter

Die Obergitter von additiv unzerlegbaren Gittern der gleichen Dimension sind wieder additiv unzerlegbar. Mit Hilfe von Lemma 3.10 wurden also von allen untersuchten Gittern (L, ϕ) alle maximal ganzzahligen Obergitter in $(L^\#, \phi)$ gesucht und auf additive Zerlegbarkeit geprüft. Für ein Gitter (L, ϕ) bezeichnet (L, ϕ') ein maximal ganzzahliges und additiv unzerlegbare Obergitter in $(L^\#, \phi)$. In allen Fällen existiert bis auf Isomorphie höchstens ein solches Obergitter. Mit dieser Methode wurden die folgenden additiv unzerlegbaren Gitter gefunden:

(L, ϕ)	(L, ϕ')
$U_{(12,16,24)}$	D12+ = $U_{(12,1,2)}$
$U_{(12,4,6)}$	
$U_{(13,243,324)}$	$U_{(13,3,5)}$
$U_{(14,192,256)}$	$U_{(14,3,4)}_{-1}$
$U_{(14,48,64)}_{-1}$	
$U_{(14,3,4)}_{-1}$	
$U_{(14,576,768)}$	$U_{(14,9,12)}$
Lambda14.2	$U_{(14,3,4)}_{-2}$
$U_{(15,128,192)}$	$U_{(15,2,3)}$
$U_{(15,32,48)}_{-2}$	
$U_{(15,2,3)}$	
$U_{(15,192,320)}$	$U_{(15,3,5)}$
$U_{(15,243,324)}$	$U_{(15,3,4)}$
$U_{(16,256,384)}$	$U_{(16,1,2)}$
$U_{(16,16,32)}$	
$U_{(16,4,8)}$	

3.2.4 Skalierung von Basisvektoren

Ein weiterer Ansatz, aus bekannten, additiv unzerlegbaren Gittern Blockformen zu konstruieren, ist die Skalierung von Basisvektoren. Zuerst wurde das Gitter $U_{(14,3,4)}_{-1}$ betrachtet und der erste Basisvektor skaliert. (L, ϕ') bezeichnet wieder die Blockformen die sich aus dem Gitter berechnen ließen. Damit wurden die folgenden, noch nicht berechneten, additiv unzerlegbaren Gitter gefunden.

Skalierung um	(L, ϕ')
2×	$U_{(12,3,4)}$
3×	$U_{(14,2,3)}$
4×	$U_{(14,8,11)}$
	$U_{(13,3,4)}$
	$U_{(12,3,4)}$
5×	$U_{(13,2,3)}$
	$U_{(13,3,4)}$

Bei einer Skalierung von 6× bis 10× wurden nur schon bekannte Gitter gefunden. Skaliert man bei dem Gitter $U_{(13,3,5)}$ den ersten Basisvektor um 2×, erhält man $U_{(13,2,3)}$ als

Blockform, eine höhere Skalierung (bis $10\times$) führt zu keinem neuem Ergebnis. Betrachtet man allerdings $U_{(13,2,3)}$ mit dem selbem Vorgehen, führt zu mindestens eine niedrigen Skalierungen zu neuen, additiv unzerlegbaren Gittern.

Skalierung um	(L, ϕ')
$3\times$	$U_{(13,7,8)}$
$4\times$	$U_{(13,10,11)}$
$5\times$	$U_{(13,6,8)}$
$6\times$	$U_{(13,6,8)}$
$7\times$	$U_{(13,10,11)}$
$8\times$	$U_{(13,7,8)}$
$9\times$	$U_{(13,8,11)}$
$10\times$	$U_{(13,2,3)}$
$11\times$	$U_{(12,11,12)}$

3.2.5 Konstruktion von Gittern mit gegebener Determinante

Seien $A \in \mathbb{R}_{\text{sym}}^{n \times n}$ und $B \in \mathbb{R}_{\text{sym}}^{m \times m}$ invertierbare, symmetrische Matrizen, $X \in \mathbb{R}^{n \times m}$ und $\lambda \in \mathbb{R}$. Dann gilt

$$\det(A - \lambda X B X^{\text{tr}}) = \det(A) \det(B) \det(B^{-1} - \lambda X^{\text{tr}} A^{-1} X).$$

Diese Gleichung kann genutzt werden um additiv unzerlegbare, positiv definite Matrizen mit gegebener Dimension n und Determinante d zu finden. Sei $A' \in \mathbb{Z}_{\text{sym}, >0}^{n \times n}$ eine solche Matrix. Dann ist $A = A' - X X^{\text{tr}}$ indefinit für jedes $X \in \mathbb{Z}^{n \times 1}$ ungleich dem Nullvektor. Wählt man $A = \text{Diag}(-1, 1, \dots, 1)$, $X = (X_1, \dots, X_n)^{\text{tr}} \in \mathbb{Z}^{n \times 1}$, dann soll $\det(A + X X^{\text{tr}}) = d$ gelten, was nach obiger Formel äquivalent dazu ist, dass $\det(A) \det(1 + X^{\text{tr}} A^{-1} X) = d$ gilt. Dies ist genau dann der Fall, wenn

$$-X_1^2 + \sum_{i=2}^n X_i^2 = -(d + 1)$$

ist. Wählt man X_1 , kann diese Gleichung zum Beispiel mit SIB gelöst werden, indem man alle Lösungen γ_{n-1} der 1×1 -Matrix $(-(d + 1) + X_1^2)$ betrachtet. Für jede solche Lösung erhält man eine Matrix A' , welche dann auf additive Unzerlegbarkeit geprüft werden kann.

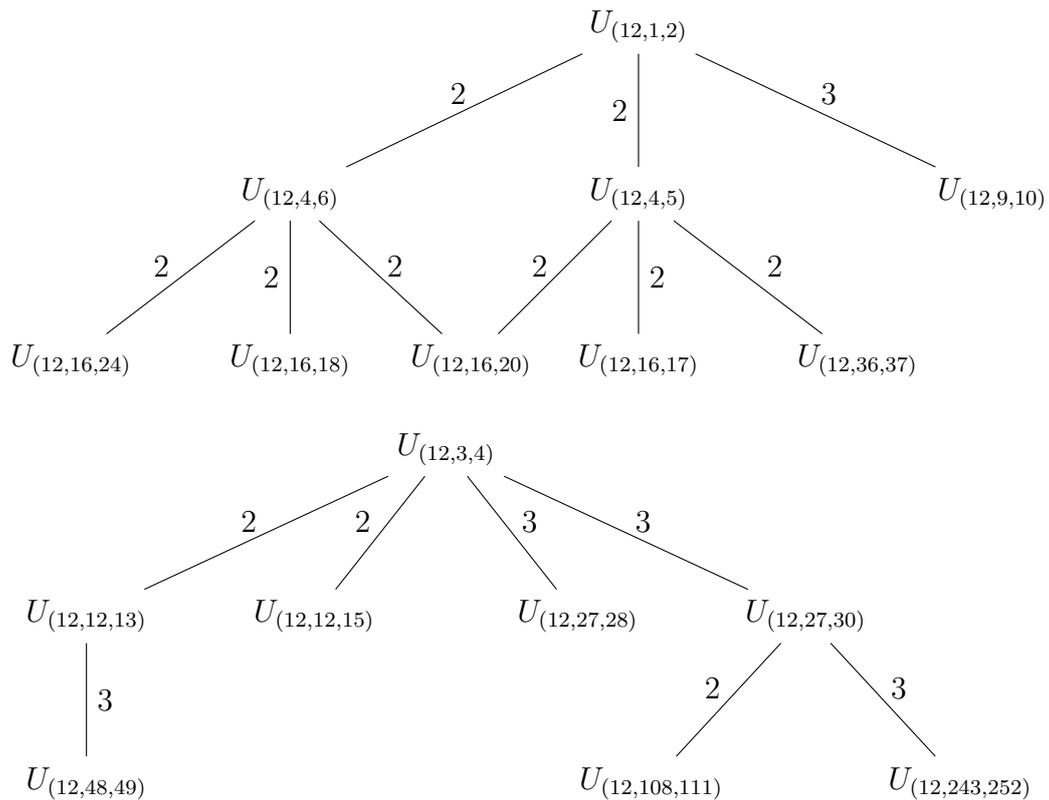
Dies wurde benutzt um ein additiv unzerlegbares Gitter in Dimension 12 mit Determinante 7 zu finden. Wählt man A wie oben und $X = (5, 2, 2, 1, 1, 1, 1, 1, 1, 1, 1, 1)^{\text{tr}} \in \mathbb{Z}^{12 \times 1}$,

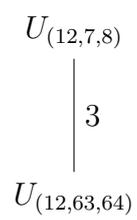
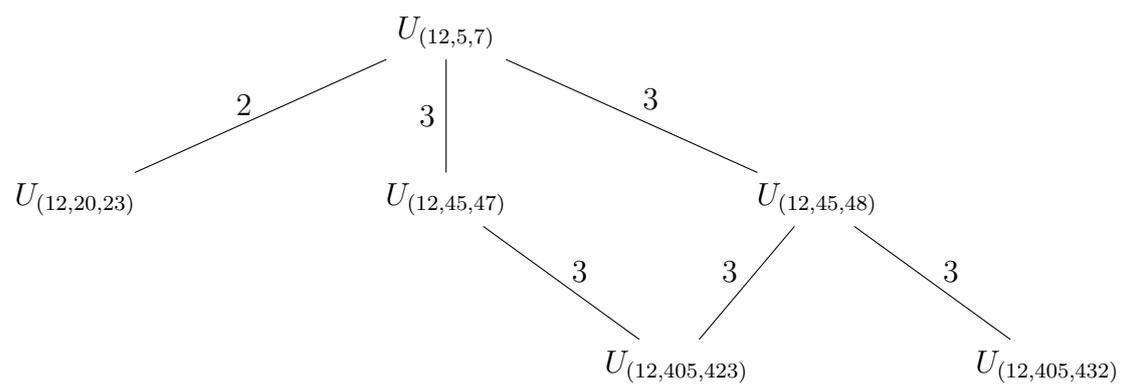
so erhält man das additiv unzerlegbare Gitter $U_{(12,7,8)}$ (eine Gram-Matrix ist in Kapitel 4 angegeben).

Eine weitere Möglichkeit ist die „Nachbarschafts-Methode“, eingeführt von M. Kneser in [Kne57]. Wendet man dies (z.B. mit Magma) auf die Matrix $\text{Diag}((\begin{smallmatrix} 2 & 1 \\ 1 & 3 \end{smallmatrix}), 1, \dots, 1) \in \mathbb{Z}^{12 \times 12}$ an, findet man das additiv unzerlegbare Gitter $U_{(12,5,7)}$ in dem berechnetem Vertretersystem.

3.2.6 Teilgitter additiv unzerlegbarer Gitter

Bisher wurde in Dimension 12 jeweils ein additiv unzerlegbares Gitter mit Determinante 1, 3, 5 und 7 gefunden. Von diesen wurden dann (bis auf Isometrie) alle Teilgitter mit Index 2 und 3 bestimmt, dasselbe wurde dann wiederum mit den gefundenen, additiv unzerlegbaren Teilgittern durchgeführt. Die Ergebnisse sind in den Teilgitter-Verbänden dargestellt.





4 Anhang

In diesem Kapitel sind alle gefundenen, additiv unzerlegbaren Gitter angegeben. $U_{(n,d,s)}$ steht hierbei für ein Gitter (L, ϕ) von Dimension n und Determinante d , so dass $\min(L^\#, \phi) = \frac{s}{d}$ gilt.

$$U_{(12,1,2)} \text{ mit } \phi = \begin{pmatrix} 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}$$

$$U_{(12,3,4)} \text{ mit } \phi = \begin{pmatrix} 2 & 0 & 0 & 1 & -1 & -1 & 0 & 0 & 1 & 1 & -1 & 1 \\ 0 & 2 & 0 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 & -1 & 1 & 0 & -1 & -1 & 0 & 0 \\ 1 & 0 & 0 & 2 & -1 & -1 & 0 & 0 & 1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & 3 & -1 & 1 & 1 & -1 & -2 & 1 & -1 \\ -1 & -1 & -1 & -1 & -1 & 3 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & -1 & 2 & 1 & -1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & -1 & 1 & 2 & 0 & -1 & 0 & 0 \\ 1 & -1 & -1 & 1 & -1 & 0 & -1 & 0 & 3 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -2 & 0 & -1 & -1 & 1 & 3 & 0 & 0 \\ -1 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & -1 & 0 & 2 & -1 \\ 1 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 1 & 0 & -1 & 2 \end{pmatrix}$$

$$U_{(12,4,5)} \text{ mit } \phi = \begin{pmatrix} 2 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 \\ -1 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 2 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 & 1 & 2 & 1 & 1 & -1 & 0 & 0 & -1 \\ -1 & 1 & 1 & 1 & 1 & 1 & 2 & 1 & 0 & 0 & 0 & -1 \\ -1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 0 & 0 & 0 & -1 \\ 1 & 0 & -1 & 0 & -1 & -1 & 0 & 0 & 3 & -2 & -2 & 1 \\ -1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & -2 & 3 & 2 & -1 \\ -1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & -2 & 2 & 3 & -1 \\ 1 & 0 & -1 & 0 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & 3 \end{pmatrix}$$

$$U_{(12,4,6)} \text{ mit } \phi = \begin{pmatrix} 2 & -1 & -1 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 3 & 1 & -1 & 1 & 0 & 1 & 1 & 1 & 1 & -1 \\ 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & -1 & 0 & 2 & 0 & 0 & 0 & -1 & -1 & -1 & 0 \\ -1 & 0 & 1 & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 2 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 2 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & -1 & 0 & 0 & 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 1 & 1 & -1 & 0 & 0 & 0 & 1 & 1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & -1 & 0 & -1 & 0 & 0 & 0 & 2 \end{pmatrix}$$

$$U_{(12,5,7)} \text{ mit } \phi = \begin{pmatrix} 2 & -1 & -1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 2 & 1 \\ -1 & 2 & 1 & 0 & -1 & 0 & 0 & 0 & 0 & -1 & -1 & -1 \\ -1 & 1 & 2 & 0 & -1 & 0 & 0 & -1 & 1 & -1 & -1 & -1 \\ 0 & 0 & 0 & 2 & -1 & 0 & -1 & 0 & 0 & 0 & -1 & -1 \\ 1 & -1 & -1 & -1 & 3 & 1 & 1 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & 1 & 1 & 2 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 2 & -1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 1 & -1 & -1 & 0 & 0 & 0 & 0 & 1 & -1 & 2 & 1 & 1 \\ 2 & -1 & -1 & -1 & 2 & 1 & 1 & 1 & 0 & 1 & 4 & 2 \\ 1 & -1 & -1 & -1 & 1 & 0 & 1 & 0 & 0 & 1 & 2 & 3 \end{pmatrix}$$

$$U_{(12,7,8)} \text{ mit } \phi = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \\ 0 & 1 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \\ 0 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \\ 0 & 1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 1 & 0 \\ -1 & -1 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}$$

$$U_{(12,9,10)} \text{ mit } \phi = \begin{pmatrix} 2 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & -1 & -1 & -1 & 0 \\ 0 & 2 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & -1 & 2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & -1 & 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & -1 & 1 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 & -1 & -1 & 1 & 1 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & 1 & 0 & -1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 2 & -1 & -1 & -1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 3 & 2 & 2 & 0 \\ -1 & 0 & 0 & 0 & 0 & 1 & -1 & -1 & 2 & 3 & 2 & 0 \\ -1 & 0 & 0 & 0 & 0 & 1 & -1 & -1 & 2 & 2 & 3 & 0 \\ 0 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 0 & 0 & 0 & 3 \end{pmatrix}$$

$$U_{(12,20,23)} \text{ mit } \phi = \begin{pmatrix} 2 & -1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 & 1 & 1 & 1 \\ -1 & 2 & 1 & 0 & -1 & 1 & 0 & -1 & 1 & -1 & -1 & 0 \\ -1 & 1 & 2 & 0 & -1 & 1 & 0 & -1 & 1 & -1 & 0 & -1 \\ 0 & 0 & 0 & 2 & -1 & 1 & -1 & 0 & 0 & -1 & 0 & -1 \\ 1 & -1 & -1 & -1 & 3 & -2 & 1 & 1 & -1 & 2 & 0 & 1 \\ -1 & 1 & 1 & 1 & -2 & 3 & 0 & -1 & 1 & -1 & 0 & -1 \\ 0 & 0 & 0 & -1 & 1 & 0 & 2 & 0 & 0 & 1 & 0 & 1 \\ 1 & -1 & -1 & 0 & 1 & -1 & 0 & 2 & -1 & 1 & 1 & 1 \\ -1 & 1 & 1 & 0 & -1 & 1 & 0 & -1 & 2 & -1 & -1 & -1 \\ 1 & -1 & -1 & -1 & 2 & -1 & 1 & 1 & -1 & 3 & 0 & 1 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 3 & 1 \\ 1 & 0 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 3 \end{pmatrix}$$

$$U_{(12,27,28)} \text{ mit } \phi = \begin{pmatrix} 2 & 0 & 0 & 1 & -1 & 0 & 1 & 1 & -1 & 1 & -1 & -1 \\ 0 & 2 & 0 & 0 & 1 & 1 & -1 & -1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 2 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 2 & -1 & 0 & 1 & 1 & -1 & 1 & -1 & 0 \\ -1 & 1 & 1 & -1 & 3 & 1 & -2 & -1 & 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 2 & -1 & -1 & 0 & 0 & 0 & 0 \\ 1 & -1 & -1 & 1 & -2 & -1 & 3 & 1 & -1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 1 & -1 & -1 & 1 & 3 & 0 & 1 & 0 & -1 \\ -1 & 0 & 0 & -1 & 1 & 0 & -1 & 0 & 2 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 & -1 & 0 & 1 & 1 & -1 & 2 & -1 & 0 \\ -1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 1 & -1 & 3 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 2 \end{pmatrix}$$

$$U_{(12,27,30)} \text{ mit } \phi = \begin{pmatrix} 2 & 0 & 0 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 \\ 0 & 2 & 0 & 0 & 1 & -1 & -1 & -1 & -1 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & 1 & -1 & -1 & -1 & -1 & -1 & 0 & 1 \\ 1 & 0 & 0 & 2 & -1 & -1 & 1 & 1 & -1 & 0 & 1 & -1 \\ -1 & 1 & 1 & -1 & 3 & -1 & -1 & -2 & 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 & -1 & 3 & 0 & 0 & 1 & 1 & -1 & 0 \\ 1 & -1 & -1 & 1 & -1 & 0 & 3 & 1 & 0 & 0 & 0 & -1 \\ 1 & -1 & -1 & 1 & -2 & 0 & 1 & 3 & 1 & 0 & 0 & -1 \\ -1 & -1 & -1 & -1 & 0 & 1 & 0 & 1 & 4 & 1 & -2 & 1 \\ -1 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 1 & 3 & -1 & -1 \\ 1 & 1 & 0 & 1 & 0 & -1 & 0 & 0 & -2 & -1 & 3 & -1 \\ -1 & 0 & 1 & -1 & 1 & 0 & -1 & -1 & 1 & -1 & -1 & 3 \end{pmatrix}$$

$$U_{(12,36,37)} \text{ mit } \phi = \begin{pmatrix} 2 & -1 & -1 & -1 & 0 & 0 & 0 & 1 & -1 & -1 & 1 & 1 \\ -1 & 2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 \\ -1 & 1 & 2 & 1 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & -1 \\ -1 & 1 & 1 & 2 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 2 & 1 & 1 & -1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 1 & -1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 2 & 0 & 0 & -1 & 0 & -1 \\ 1 & 0 & -1 & 0 & -1 & -1 & 0 & 3 & -1 & 0 & 0 & 1 \\ -1 & 0 & 1 & 1 & 0 & 0 & 0 & -1 & 3 & 1 & -1 & -1 \\ -1 & 0 & 0 & 0 & -1 & -1 & -1 & 0 & 1 & 3 & -1 & 1 \\ 1 & -1 & 0 & -1 & 0 & 0 & 0 & 0 & -1 & -1 & 3 & 0 \\ 1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 & 1 & 0 & 3 \end{pmatrix}$$

$$U_{(12,48,49)} \text{ mit } \phi = \begin{pmatrix} 2 & 0 & 0 & 1 & -1 & -1 & 0 & 1 & -1 & 1 & 0 & 1 \\ 0 & 2 & 0 & 0 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 \\ 0 & 0 & 2 & 0 & 1 & -1 & 0 & -1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 2 & -1 & -1 & 0 & 1 & 0 & 1 & 0 & 0 \\ -1 & 1 & 1 & -1 & 3 & -1 & 1 & -1 & 0 & -1 & 1 & -1 \\ -1 & -1 & -1 & -1 & -1 & 3 & -1 & 0 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 1 & -1 & 2 & 0 & -1 & -1 & 0 & 0 \\ 1 & -1 & -1 & 1 & -1 & 0 & 0 & 3 & 0 & 1 & -1 & 1 \\ -1 & -1 & 0 & 0 & 0 & 1 & -1 & 0 & 3 & 1 & -1 & -1 \\ 1 & -1 & 0 & 1 & -1 & 0 & -1 & 1 & 1 & 3 & -1 & 0 \\ 0 & 1 & 1 & 0 & 1 & -1 & 0 & -1 & -1 & -1 & 3 & -1 \\ 1 & -1 & 0 & 0 & -1 & 0 & 0 & 1 & -1 & 0 & -1 & 3 \end{pmatrix}$$

$$U_{(12,63,64)} \text{ mit } \phi = \begin{pmatrix} 2 & 1 & 1 & 0 & 0 & 0 & -1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 2 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ 0 & 0 & 0 & 1 & 2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 2 & 1 & -1 & -1 & -1 & -1 & -1 \\ -1 & 0 & -1 & 1 & 1 & 1 & 3 & -1 & -1 & -1 & -1 & -1 \\ 1 & 0 & 0 & -1 & 0 & -1 & -1 & 3 & 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & -1 & 0 & -1 & -1 & 1 & 3 & 2 & 2 & 2 \\ 1 & 1 & 0 & -1 & 0 & -1 & -1 & 2 & 2 & 4 & 2 & 1 \\ 0 & 0 & 0 & -1 & 0 & -1 & -1 & 1 & 2 & 2 & 3 & 2 \\ 0 & 0 & 0 & -1 & 0 & -1 & -1 & 1 & 2 & 1 & 2 & 3 \end{pmatrix}$$

$$U_{(12,108,111)} \text{ mit } \phi = \begin{pmatrix} 2 & 1 & -1 & 1 & -1 & 1 & 1 & 0 & 0 & -1 & 1 & -1 \\ 1 & 2 & -1 & 1 & -1 & 1 & 1 & 0 & 0 & 0 & 1 & -1 \\ -1 & -1 & 3 & -1 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ 1 & 1 & -1 & 3 & 0 & 0 & 0 & -1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 0 & 0 & 3 & -1 & 0 & -1 & 0 & 0 & -1 & 0 \\ 1 & 1 & 0 & 0 & -1 & 3 & 2 & 1 & 0 & -1 & 0 & -1 \\ 1 & 1 & 0 & 0 & 0 & 2 & 3 & 0 & -1 & -1 & 0 & -1 \\ 0 & 0 & 1 & -1 & -1 & 1 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & -1 & 0 & 3 & 0 & -1 & 1 \\ -1 & 0 & 0 & -1 & 0 & -1 & -1 & 0 & 0 & 3 & -1 & 0 \\ 1 & 1 & 0 & 1 & -1 & 0 & 0 & 0 & -1 & -1 & 3 & -1 \\ -1 & -1 & 0 & -1 & 0 & -1 & -1 & 0 & 1 & 0 & -1 & 3 \end{pmatrix}$$

$$U_{(12,243,252)} \text{ mit } \phi = \begin{pmatrix} 2 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 1 & -1 \\ 0 & 4 & 2 & 2 & 0 & -2 & -2 & -2 & -2 & -1 & 1 & -1 \\ 1 & 2 & 4 & 2 & -1 & -2 & -2 & 0 & -2 & 0 & 2 & -1 \\ 0 & 2 & 2 & 3 & 0 & -1 & -2 & -1 & -1 & -1 & 1 & -1 \\ 0 & 0 & -1 & 0 & 2 & 1 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & -2 & -2 & -1 & 1 & 3 & 1 & 1 & 2 & 0 & -1 & 1 \\ 0 & -2 & -2 & -2 & 0 & 1 & 3 & 1 & 1 & 1 & -1 & 1 \\ 1 & -2 & 0 & -1 & 0 & 1 & 1 & 3 & 1 & 0 & 0 & 0 \\ -1 & -2 & -2 & -1 & 1 & 2 & 1 & 1 & 4 & 0 & -2 & 2 \\ 0 & -1 & 0 & -1 & -1 & 0 & 1 & 0 & 0 & 3 & -1 & 0 \\ 1 & 1 & 2 & 1 & 0 & -1 & -1 & 0 & -2 & -1 & 3 & -1 \\ -1 & -1 & -1 & -1 & 0 & 1 & 1 & 0 & 2 & 0 & -1 & 3 \end{pmatrix}$$

$$U_{(12,405,423)} \text{ mit } \phi = \begin{pmatrix} 2 & -1 & 1 & 0 & -1 & 1 & 0 & 1 & -1 & 1 & 0 & -1 \\ -1 & 3 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 3 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & -1 & 0 \\ 0 & -1 & 1 & 3 & -1 & 0 & 1 & 0 & 1 & -1 & 0 & 1 \\ -1 & 1 & 0 & -1 & 3 & -1 & -1 & -1 & 1 & -1 & 0 & 0 \\ 1 & -1 & 1 & 0 & -1 & 3 & 0 & 0 & 0 & 0 & -1 & -1 \\ 0 & -1 & 1 & 1 & -1 & 0 & 3 & 0 & -1 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 & -1 & 0 & 0 & 3 & -1 & 1 & -1 & 0 \\ -1 & 1 & 0 & 1 & 1 & 0 & -1 & -1 & 4 & -1 & -1 & 2 \\ 1 & -1 & 0 & -1 & -1 & 0 & 1 & 1 & -1 & 4 & -1 & 0 \\ 0 & 1 & -1 & 0 & 0 & -1 & 0 & -1 & -1 & -1 & 3 & 0 \\ -1 & 1 & 0 & 1 & 0 & -1 & 0 & 0 & 2 & 0 & 0 & 3 \end{pmatrix}$$

$$U_{(12,405,432)} \text{ mit } \phi = \begin{pmatrix} 4 & -2 & 0 & 2 & -1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 \\ -2 & 3 & -1 & -1 & 1 & 0 & 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & -1 & 3 & -1 & -1 & 0 & -1 & 0 & 1 & 1 & 0 & 1 \\ 2 & -1 & -1 & 3 & 0 & 1 & 0 & 1 & -1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 0 & 3 & 0 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 3 & 1 & 1 & -1 & -1 & 1 & 0 \\ -1 & 1 & -1 & 0 & 1 & 1 & 3 & 1 & 0 & -1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 3 & 0 & -1 & 1 & 0 \\ 0 & -1 & 1 & -1 & -1 & -1 & 0 & 0 & 3 & 0 & -1 & 1 \\ -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & 0 & 3 & -1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 3 & 1 \\ -1 & 0 & 1 & -1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 3 \end{pmatrix}$$

$$U_{(13,2,3)} \text{ mit } \phi = \begin{pmatrix} 2 & 0 & -1 & -1 & -1 & 0 & -1 & -1 & -1 & -1 & 0 & -1 & 0 \\ 0 & 2 & -1 & -1 & 0 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 \\ -1 & -1 & 2 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & -1 \\ -1 & -1 & 1 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & -1 & 1 & 0 \\ -1 & 0 & 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 & 0 & 2 & 0 & 1 & 1 & 1 & 0 & 1 & -1 \\ -1 & 1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 1 \\ -1 & -1 & 1 & 1 & 0 & 1 & 0 & 3 & 2 & 2 & -1 & 2 & -1 \\ -1 & -1 & 1 & 1 & 0 & 1 & 0 & 2 & 3 & 1 & 0 & 2 & -1 \\ -1 & -1 & 1 & 1 & 0 & 1 & 0 & 2 & 1 & 3 & -1 & 2 & -1 \\ 0 & 1 & 0 & -1 & 0 & 0 & 1 & -1 & 0 & -1 & 3 & -1 & 1 \\ -1 & -1 & 1 & 1 & 0 & 1 & 0 & 2 & 2 & 2 & -1 & 3 & -1 \\ 0 & 1 & -1 & 0 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 3 \end{pmatrix}$$

$$U_{(13,3,4)} \text{ mit } \phi = \begin{pmatrix} 3 & 0 & -1 & 1 & -1 & 0 & 0 & -1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & -1 & 0 & 0 & 0 \\ -1 & 0 & 2 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 3 & -1 & -1 & 0 & -1 & -1 & 0 & 1 & -1 & 1 \\ -1 & 0 & 1 & -1 & 3 & -1 & 1 & 1 & 0 & -1 & 0 & 1 & -1 \\ 0 & 0 & -1 & -1 & -1 & 3 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 0 & 0 & 1 & 0 & 1 & -1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & -1 & 1 & -1 & 1 & 2 & -1 & -1 & 0 & 0 & 0 \\ 0 & -1 & -1 & -1 & 0 & 1 & 0 & -1 & 3 & 2 & -1 & 0 & 0 \\ 1 & -1 & -1 & 0 & -1 & 1 & 0 & -1 & 2 & 3 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & -1 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & -1 \\ 0 & 0 & 0 & 1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}$$

$$U_{(22,3,8)} \text{ mit } \phi = \begin{pmatrix} 3 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 0 & 0 & -1 & 0 & 1 & 0 & -1 & -1 & -1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 3 & -1 & 1 & -1 & -1 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & -1 & -1 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 1 & -1 & 3 & -1 & -1 & -1 & -1 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & -1 & 0 & -1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & -1 & 3 & -1 & -1 & -1 & 0 & -1 & -1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 & 3 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ -1 & -1 & -1 & -1 & 1 & 3 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 & 1 & 1 & 3 & -1 & 0 & 0 & 1 & 0 & -1 & 0 & 1 & -1 & 1 & 0 & -1 & 0 & -1 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & -1 & 3 & -1 & -1 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & -1 & 3 & 1 & -1 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & -1 & 1 & 3 & 1 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 1 & 0 & 0 \\ -1 & -1 & -1 & 0 & 1 & 1 & 1 & 0 & -1 & 1 & 3 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & -1 & 1 & 1 & 0 & 3 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 1 & 0 & -1 & 0 & -1 & 0 & -1 & 0 & 0 & 0 & 3 & 0 & 0 & -1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 3 & 0 & 1 & 0 & 0 & 0 & -1 & -1 \\ -1 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 3 & 0 & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 3 & 0 & -1 & -1 & -1 & 0 & 0 \\ 1 & -1 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & -1 & 0 & 3 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 3 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 3 & 0 & 1 \\ 1 & 0 & 1 & 0 & -1 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & -1 & 0 & -1 & 1 & 1 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 1 & 1 & 3 \end{pmatrix}$$

Literaturverzeichnis

- [Cas78] John William Scott Cassels. *Rational Quadratic Forms*. Academic Press, New York, 1978.
- [CS89] John Horton Conway and Neil James Alexander Sloane. Low-Dimensional Lattices V. Integral Coordinates for Integral Lattices. *Proceedings of the Royal Society A*, 426(1871):211 – 232, 1989.
- [CS99] John Horton Conway and Neil James Alexander Sloane. *Sphere Packings, Lattices and Groups*. Springer New York, 1999.
- [Eic52] Martin Eichler. Note zur Theorie der Kristallgitter. *Mathematische Annalen*, 125(1):51–55, 1952.
- [Kne54] Martin Kneser. Zur Theorie der Kristallgitter. *Mathematische Annalen*, 127(1):105–106, 1954.
- [Kne57] Martin Kneser. Klassenzahlen definitiver quadratischer Formen. *Archiv der Mathematik*, 8(4):241–250, 1957.
- [Ko37] Chao Ko. On the representation of a quadratic form as a sum of squares of linear forms. *J. Math. Oxford*, 8:81–98, 1937.
- [Ko39] Chao Ko. On the decomposition of quadratic forms in six variables. *Acta Arith.*, 3:64–78, 1939.
- [Ko42a] Chao Ko. On the decomposition of quadratic forms in eight variables. *Acad. Sinica Sci. Rec.*, pages 33–36, 1942.
- [Ko42b] Chao Ko. On the decomposition of quadratic forms in seven variables. *Acad. Sinica Sci. Rec.*, pages 30–33, 1942.

- [Mor37] Louis Joel Mordell. The Representation of a Definite Quadratic Form as a Sum of Two Others. *Annals of Mathematics*, 38(4):751 – 757, 1937.
- [NS] Gabriele Nebe and Neil James Alexander Sloane. A Catalogue of Lattices.
- [Opg92] Jürgen Opgenorth. Additiv unzerlegbare ganzzahlige quadratische Formen in den Dimensionen 9, 10 und 11. Diplomarbeit, RWTH Aachen, 1992.
- [Ple94] Wilhelm Plesken. Additively Indecomposable Positive Integral Quadratic Forms. *Journal of Number Theory*, 47(3):273 – 283, 1994.
- [Ple95] Wilhelm Plesken. Solving $XX^{\text{tr}} = A$ over the Integers. *Linear Algebra and its Applications*, 226–228(0):331 – 344, 1995.
- [PP85] Wilhelm Plesken and Michael Pohst. Constructing integral lattices with prescribed minimum I. *Math. Comp.*, 45:209–221, 1985.
- [PP93] Wilhelm Plesken and Michael Pohst. Constructing integral lattices with prescribed minimum II. *Math. Comp.*, 60:817–825, 1993.
- [PZ89] Michael Pohst and Hans Zassenhaus. *Algorithmic algebraic number theory*. Cambridge University Press, 1989.
- [Sie56] Carl Ludwig Siegel. *Lectures of quadratic forms*. Tata Institute of Fundamental Research, Bombay, 1955/56.
- [TTT06] Etsuji Tomita, Akira Tanaka, and Haruhisa Takahashi. The worst-case time complexity for generating all maximal cliques and computational experiments. *Theoretical Computer Science*, 363(1):28 – 42, 2006.

Erklärung

Hiermit versichere ich, dass ich diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Aachen, den 29. September 2014

Simon Eisenbarth