RWTH Aachen – Sommersemester 2007

Zusammenfassung

# Gitter und Codes*

Ulrich Loup
*Ulrich.Loup@rwth-aachen.de*

13. Januar 2008

*Anmerkungen:*

- Ich garantiere weder Vollständigkeit noch Korrektheit meiner Angaben.
- Dieses Dokument ist primär als persönliches Nachschlagewerk erstellt worden.
- Verbesserungsvorschläge oder sonstige Bemerkungen nehme ich gerne entgegen.

*Gehalten von Prof. Dr. Gabriele Nebe.

# Inhaltsverzeichnis



# Literatur

[Ebeling] *Lattices and Codes*, Wolfgang Ebeling, Vieweg, 1994.

[Nebe] *Gitter und Codes*, Gabriele Nebe, Vorlesungsskript, RWTH Aachen 2007.

[LoupOB] *Zusammenfassung Optimierung B*, Ulrich Loup, private Zusammenfassung, 2008.

## Motivation

Gitter sind algebraische Strukturen, die in der Zahlentheorie verwendet werden (aus [Ebeling]) und zunächst keine direkte Verbindung zur Kodierungstheorie haben. Die Kodierungstheorie behandelt die Gestaltung effizienter und sicherer Nachrichtenübertragungs-Systeme mittels Fehlerkorrektur-Codes. Viele Probleme, die bei Codes auftreten, können auf Gitter übertragen werden, so dass die Kodierungstheorie algebraische Methoden verwenden kann. Die Gittertheorie ist auch beim Bestimmen dichter Kugelpackungen hilfreich, wie sie in vielen Bereichen wie etwa der Chemie gebraucht werden.

## Übersicht

**Gitter:** Zunächst werden Gitter und einige der wichtigsten Begriffe im Umfeld derer in Abschnitt 2.1 und insbesondere den Unterabschnitten 2.1.1, 2.1.2, 2.1.3 definiert und durch Bemerkungen motiviert, bis in Abschnitt 2.1.4 eine erste Anwendung bei der Findung von dichten Kugelpackungen angedeutet wird. Die wichtigsten Konzepte sind (auch aus Abschnitt 3)

- *Isometrie und Isometrieklassen*

  Isometrische Gitter sind die unter orthogonalen Transformationen invarianten Gitter. Die so induzierten Isometrieklassen haben jeweils einen konstanten Wert der HERMITE-Funktion, weswegen sie auch das gleiche Minimum und gleich dichte gitterförmige Kugelpackungen besitzen.

- *Irreduzibilität von Gittern und die Zerlegung von Gittern in irreduzible Teilgitter*

  Irreduzible Gitter sind die nicht mehr durch echte, orthogonale Teilgitter (in einer orthogonalen Summe) darstellbaren Gitter. Jedes Gitter ist durch eine orthogonale Summe dieser Teilgitter darstellbar.

- *Kürzeste Vektoren*

  Die Bestimmung der kürzesten Vektoren unterstützt durch den LLL-Algorithmus ist wichtig zur Berechnung des Minimums eines Gitters, welches beispielsweise für das Minimalgewicht eines Codes (bezüglich des zugehörigen Codegitters) oder die Dichte einer Kugelpackung gebraucht werden kann.

- *Extreme Gitter und deren Charakterisierung als perfekt und eutaktisch*

  Die extremen Gitter bilden die Maxima der HERMITE-Funktion. Extreme Gitter sind nach VORONOI genau die perfekten und eutaktischen Gitter, welche jeweils über die gleichnamigen Begriffe ihrer Grammatrizen definiert sind. Der VORONOI-Algorithmus kann perfekte Gitter bestimmen.

**Codes:** Das Ziel der in Abschnitt 2.2 behandelten Begriffe ist das Verständnis darüber, wie Codes als Teilmenge eines Vektorraums $\mathbb{F}_q^r$ zur Fehlerkorrektur eingesetzt werden kön-

nen. Dazu wird zunächst das allgemeine Prinzip des Kodierens und Dekodierens erklärt und später die Vorteile linearer Codes diskutiert beziehungsweise charakterisiert, in welchen Fällen die Zuordnung eines eventuell fehlerhaft übertragenen Informationsworts zu einem Codewort eindeutig ist. Als Beispiel werden der binäre Wiederholungscode und in Abschnitt 2.2.1 der HAMMING-Code betrachtet.

**Codegitter:** In Abschnitt 3.1 liegt die Kernaussage der hier behandelten Korrespondenz zwischen Gittern und Codes in Form eines Codegitters. Dort wird erklärt, inwiefern die Begriffe der beiden Konstrukte in Einklang gebracht werden können.

# 1 Grundlagen

*Erinnerung:* Für einen Körper $K$ ist ein **$K$-Vektorraum** $(V, +, \cdot)$ eine abelsche Gruppe $(V, +)$ mit Operatorbereich $K$ und den folgenden zusätzlichen Gesetzen: Seien $a, b \in K$ und $v, w \in V$.

1. *Distributivgesetze:* $a(v + w) = av + aw, \qquad (a + b)v = av + bv,$
2. *Neutralität der skalaren Eins:* $1_K v = v$.

$V$ ist also eine spezielle $K$-Gruppe, genauer ein $K$-Linksmodul. Es ist aber weder jede abelsche $K$-Gruppe ein $K$-Vektorraum [1] noch jeder $R$-Linksmodul ein Vektorraum [2].

## 1.1 Bilinearform und Grammatrix

Sei $V$ ein Vektorraum (Abkürzung für $(V, +, \cdot)$) über dem Körper $K$.

**Definition 1.**

- *Eine Abbildung* $\Phi : V \times V \to K$ *heißt* ***Bilinearform****, falls für alle* $v_1, v_2, w_1, w_2 \in V$ *und* $a \in K$ *gilt:*
  - $\Phi(v_1 + v_2, w_1) = \Phi(v_1, w_1) + \Phi(v_2, w_1)$, $\Phi(v_1, w_1 + w_2) = \Phi(v_1, w_1) + \Phi(v_1, w_2)$ *und*
  - $a\Phi(v_1, w_1) = \Phi(av_1, w_1) = \Phi(v_1, aw_1)$.
- $\Phi$ *heißt* ***symmetrisch****, falls* $\Phi(v, w) = \Phi(w, v)$ *für alle* $v, w \in V$ *ist.*
- *Ist* $\Phi$ *symmetrisch, so bezeichnet* $\mathrm{Kern}(\Phi) := \{v \in V \mid \Phi(v, w) = \Phi(w, v) = 0 \ \forall w \in V\}$ *den* ***Kern von*** $\Phi$. *Ist* $\mathrm{Kern}(\Phi) = \{0\}$, *so heißt* $\Phi$ ***nicht ausgeartet****, das heißt, falls aus* $\Phi(v, w) = 0$ *für alle* $w \in V$ $v = 0$ *folgt.*[3]
- *Zwei Vektoren* $v, w \in V$ *heißen* ***orthogonal zueinander bezüglich*** $\Phi$*, falls* $\Phi(v, w) = 0$.

[1] wegen der fehlenden Gesetze

[2] da $R$ nicht notwendig ein Körper sein muss

[3] Also steht in dem Fall nur der der Nullvektor auf allen anderen senkrecht.

Eine Bilinearform ist also eine Abbildung, die in jeder Komponenten linear ist. Bilinearformen sind Verallgemeinerungen des Skalarprodukts beziehungsweise Ausgangspunkt für den Begriff „orthogonal“. Die Bilinearform $\Phi : V \times V \to K$ heißt **Skalarprodukt**, falls $\Phi$ **positiv definit** ist, das heißt, falls $\Phi(v, w) \geq 0$ für alle $v, w \in V$ mit Gleichheit genau dann, wenn $v = w$.
Bilinearformen lassen sich auch allgemeiner auf zwei unterschiedlichen Vektorräumen $V, W$ definieren und ebenso kann der Kern für nicht symmetrische Bilinearformen separat als Rechts- beziehungsweise Linkskern definiert werden. Diese Begrife werden im Folgenden aber nich benötigt.
Eine Bilinearform kann bei gegebener Basis wie eine lineare Abbildung durch eine Matrix spezifiziert werden.

**Definition 2.** *Sei $\Phi : V \times V \to K$ eine Bilinearform und $B = (v_1, \ldots, v_n)$ eine Basis von $V$. Die Matrix*

$$\mathcal{G}(B) := (\Phi(v_i, v_j))_{1 \leq i,j \leq n} \in K^{n \times n}$$

*heißt **Grammatrix von $B$ bzgl.** $\Phi$.*

Die Bilinearform kann bereits in der Definition des Vektorraums gegeben sein wie zum Beispiel das Skalarprodukt $(,)$ beim **Euklidischen Vektorraum**[4] $\mathbb{E} := (\mathbb{R}^n, (,))$, so dass dann $\mathcal{G}(B) := ((v_i, v_j))_{1 \leq i,j \leq n}$.

**Bemerkung 1.**
*Ist $B$ eine orthogonale Basis von $\mathbb{E}$, so ist die zugehörige Grammatrix $\mathcal{G}(B)$ eine Diagonalmatrix.*

*Beweis:* $\mathcal{G}(B) = ((b_i, b_j))_{1 \leq i,j \leq n}$ hat nur für $i = j$ Skalarprodukte $\neq 0$. □

Bilinearformen können auch als lineare Abbildungen über dem Tensorprodukt der zu Grunde liegenden Vektorräumen aufgefasst werden.

**Definition und Bemerkung 3.** *Seien $V, W$ Vektorräume mit Basen $B_V = (v_1, \ldots, v_n)$ und $B_W = (w_1, \ldots, w_m)$.*

1. *Der Vektorraum $V \otimes W$ heißt das **Tensorprodukt von $V$ und $W$**, wobei $(v_i \otimes w_j)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ die Basis von $V \otimes W$ ist mit $v_i \otimes v_j = (v_i, v_j) \in B_V \times B_W$.*[5]

   *Somit:* $\dim V \otimes W = \dim V \dim W = nm$.

2. *Ein Element $x \in V \otimes W$ heißt **Tensor** und hat die Form $x = \sum_{(i,j)=(1,1)}^{(n,m)} a_i (v_i \otimes w_j)$.*

   *Zu gegebenen $v \in V, w \in W$ kann über deren Summendarstellung auch eine Darstellung von $v \otimes w$ hergeleitet werden:*

$$v \otimes w := \sum_{(i,j)=(1,1)}^{(n,m)} a_i b_j (v_i \otimes w_j), \text{ falls } v = \sum_{i=1}^{n} a_i v_i \text{ und } w = \sum_{j=1}^{m} b_j w_j.$$

[4] Euklidischer Vektorraum: $\mathbb{E} = (\mathbb{R}^n, (,))$ mit $(,)$ Skalarprodukt.
[5] Tensorprodukte können noch allgemeiner über Moduln definiert werden.

*3. Zu jeder Bilinearform $\Phi : V \times V \to K$ gibt es eine lineare Abbildung $\phi : V \otimes V \to K$.*

*Beweis:* Sei $\Phi : V \times V \to K$ eine Bilinearform. Definiere $\phi : V \otimes V \to K : v \otimes w \mapsto \Phi(v, w)$. □

Im Gegensatz zu Temsorprodukten dient bei ringdirekten Summen oder direkten Produkten von Gruppen stets das kartesische Produkt der Summanden beziehungsweise Faktoren als Trägermenge, weswegen sich dort die Dimensionen aufaddieren.

## 1.2 Dualbasen, Dualräume und Orthogonalräume

Sei $B = (b_1, \ldots, b_n)$ Basis eines Vektorraums.

**Definition und Bemerkung 4.** *Die Basis $B^* = (b_1^*, \ldots, b_n^*)$ heißt die **zu** $B$ **duale Basis**, falls $(b_i^*, b_j) = \delta_{i,j} = \begin{cases} 1, & i=j \\ 0, & i \neq j \end{cases}$.*

Zur Konstruktion von Dualbasen kann Algorithmus 2 angewandt werden.

**Bemerkung 2.**
*Ist $A = ((b_i, b_j))_{1 \leq i,j \leq n} = \mathcal{G}(B)$, so können Dualbasen wie folgt berechnet werden:*

$$b_i^* = \sum_{j=1}^{n} a_{ij}^* b_j, \text{ wobei } (a_{ij}^*) = A^{-1}.$$

**Bemerkung 3.**
*Es ist $\mathcal{G}(B^*) = \mathcal{G}(B)^{-1}$.*

*Beweis:* Es gilt $\mathcal{G}(B)\mathcal{G}(B)^{-1} = I$. Zeige: $\mathcal{G}(B)\mathcal{G}(B^*) = I$ (genau dann ist $\mathcal{G}(B^*) = \mathcal{G}(B)^{-1}$).

$i \neq j$**:**

$$\begin{aligned}(\mathcal{G}(B)\mathcal{G}(B^*))_{ij} &= \sum_{k=1}^{n}(b_i, b_k)(b_k^*, b_j^*) = \sum_{k=1}^{n}\left(\sum_{r=1}^{n}(b_i)_r(b_k)_r \sum_{s=1}^{n}(b_k^*)_s(b_j^*)_s\right) \\ &= \sum_{k=1}^{n}\left(\sum_{r=1}^{n}\sum_{s=1}^{n}(b_i)_r(b_k)_r(b_k^*)_s(b_j^*)_s\right)\end{aligned}$$

$i = j$**:** $(\mathcal{G}(B)\mathcal{G}(B^*))_{ij} = \sum_{k=1}^{n}(b_i, b_k)(b_k^*, b_j^*) \overset{\text{s.o.}}{=} \sum_{k=1}^{n} b_i^T b_j^* = n.$

□

Dualbasen sind also Basen, deren Elemente othonormal zu den entsprechenden Elementen der ursprünglichen Basis sind.

**Definition und Bemerkung 5.** *Sei $(V, \Phi)$ ein Vektorraum über einer symmetrischen, nicht ausgearteten Bilinearform $\Phi : V \times V \to$ und $U \leq V$ ein Teilraum. $U^\perp := \{v \in V \mid \Phi(v, u) = 0 \ \forall u \in U\}$ ist ein Teilraum von $V$ und heißt **Orthogonalraum zu** $U$. Es gilt* $\dim U^\perp = \dim V - \dim U$ .

*Beweis:*

- Zeige: $U^\perp \leq V$.

  Seien $u, w \in U^\perp$. Es genügt zu beweisen, dass $au + w \in U^\perp$ für $a \in K$. Sei nun $v \in V$ beliebig. Es gilt $\Phi(v, au + w) = a\underbrace{\Phi(v,u)}_{=0} + \underbrace{\Phi(v,w)}_{=0} = 0$.

- Zeige: $\dim U^\perp = \dim V - \dim U$.

  Sei $B$ Basis von $V$ und $B_U \subseteq B$ Basis von $U$. Es ist $B_{U^\perp} = \{\}$

□

# 2 Begriffe und Notationen

Hier werden Begriffe eingeführt und durch kleinere Bemerkungen und Beweise motiviert und vertieft. Der Übersichtlichlkeit halber werden Gitter und Codes in getrennten Abschnitten behandelt.

## 2.1 Gitter

Am Anfang steht das Gitter als Teilmenge eines Vektorraums $(V, (,))$ (identifiziert mit $V$).

**Definition 6.**

- *$L \subset V$ heißt **Gitter**, falls eine **Gitterbasis** $B = (b_1, \ldots, b_m)$ existiert mit*

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

  *$m = \dim L$ heißt die **Dimension von** $L$ und $\mathcal{L}_m$ die Menge aller $m$-dimensionalen Gitter.*

- *$L$ heißt **volles Gitter in** $V$, falls $m =: \dim L = \dim V$.*

  *Sei $V = (\mathbb{R}^n, (,))$. $L$ ist volles Gitter, falls $\mathbb{R}L := \langle B \rangle_{\mathbb{R}} = V$ ist.*

- $\det(L) := \det(\mathcal{G}(B))$ *heißt die **Determinante von** $L$.*

- $\mathcal{G}(L)$ *heißt **Grammatrix von** $L$, falls $\mathcal{G}(L) = \mathcal{G}(B')$ für eine Basis $B'$ von $L$.*

Ein Gitter ist also ein endlich erzeugter $\mathbb{Z}$-Modul und insbesondere eine abelsche $\Omega$-Gruppe.

**Erinnerung 1.** *Sei $G$ eine Gruppe*

1. *Sei $G$ abelsch. Jede Untergruppe $U \leq G$ ist ein Normalteiler in $G$.*
2. *Sei $U \leq G$. Es gilt $U \trianglelefteq N_G(U)$.*

3. *Ist $U \trianglelefteq G$, so bildet $G/U$ eine Gruppe vermöge dem* Komplexprodukt $G/U \times G/U \to G/U : (gU, hU) \mapsto gUhU =: \{gu_1hu_2 \mid u_1, u_2 \in U\}$, *die* ***Faktorgruppe von $G$ nach $U$***.

*Beweis:*

1. Seien $u \in U$ und $g \in G$. Da $G$ abelsch, ist ${}^g u = gug^{-1} = gg^{-1}u = u$.
2. Klar mit $N_G(U) = \{g \in G \mid {}^g U = U\}$.
3. Zeige: $G/U \times G/U \to G/U : (gU, hU) \mapsto gUhU$ ist wohldefiniert.

   Seien $gU, hU \in G/U$. Da $U$ Normalteiler und somit $hU = Uh$ ist, gilt

   $$gUhU = gUUh = gUh = ghU.$$

   Daraus folgen die Assoziativität, die Eigenschaften der Eins und der Inversen auf Vertreterebene.

□

**Definition und Bemerkung 7.**

- *Eine Gruppe $G$ heißt* ***topologische Gruppe****, falls die Verknüpfung und die Inversionsabbildung stetig sind.*
- *Ein Gitter $L$ in $V$ ist eine* ***diskrete Untergruppe von*** *$V$, das bedeutet, eine topologische Gruppe mit der* diskreten Topologie.

Sei von nun an $L \subset V$ mit Gitterbasis $B = (b_1, \ldots, b_m)$ und Dimension $m$ . In [Ebeling] wird $L$ als volles Gitter über dem EUKLIDISCHEN Vektorraum $\mathbb{E} := (\mathbb{R}^{n\times 1} =: \mathbb{R}^n,\ (,))$ vorausgesetzt, was im Folgenden weiter verfolgt wird (auch angelehnt an das zu Grunde liegende Skript).
$L$ ist keineswegs ein Teilraum von $\mathbb{E}$. Allerdings kann ein Gitter einen Teilraum erzeugen: $\mathbb{R}L := \langle B \rangle_{\mathbb{R}}$ (dann ist $L$ volles Gitter in $\mathbb{R}L$). Ein anschauliches Beispiel für ein volles Gitter in $\mathbb{E}$ ist $\mathbb{Z}^n \subset \mathbb{R}^n$.

**Definition und Bemerkung 8.** *1. Die Menge*

$$P(B) := \{\sum_{i=1}^{m} a_i b_i \mid 0 \leq a_i \leq 1\} = \{v \in \mathbb{R}L \mid (v, v) \leq 1\}$$

*heißt* ***Parallelepiped*** *oder* ***Pralellotop****. Enthält $B$ nur Standardbasisvektoren, so ist $P(B)$ $m$-dimensionaler Einheitswürfel. Ein dreidimensionales Parallelepiped heißt* ***Spat****, ein zweisimensionales* ***Pralellogramm****.*

2. *Das Volumen* $\mathrm{vol}(P(B))$ *des Parallelepipeds hängt direkt mit der Grammatrix von* $L$ *zusammen:*

$$\mathrm{vol}(P(B)) = \sqrt{\det(\mathcal{G}(L))}.$$

*Diese Tatsache ist allgemein mit der Transformationsformel für* Lebesque*-Integrale beweisbar, für die Standardbasis aber beispielsweise direkt einsehbar, da die Grammatrix die Einheitsmatrix ist.*[6]

3. *Sei* $L$ *ein volles Gitter. Die Menge* $F \subseteq \mathbb{R}^n$ *heißt* ***Fundamentalbereich der Operation von*** $L$ ***auf*** $\mathbb{E}$*, falls*

   *(i)* $P(B)$ *abgeschlossen ist,*

   *(ii) es für alle* $v \in \mathbb{R}^n$ *ein* $l \in L$ *gibt mit* $l + v \in F$ *und*

   *(iii) sind* $v \neq w \in F$*, so dass* $v - w \in L$*, so gilt* $v, w \in \partial F$*.*

4. *Ist* $L$ *ein volles Gitter, so ist* $P(B)$ *ein Fundamentalbereich der Operation von* $L$ *auf* $\mathcal{E}$*.*

*Beweis:* Zu *4.* (Übung 1, Aufgabe 1):

(i) Zeige: $C := \complement_{\mathbb{R}^n} P(B)$ ist offen bezüglich der natürlichen Topologie auf $\mathbb{R}^n$.

(ii) Sei $v \in \mathbb{R}^n$ mit $v = \sum_{i=1}^n r_i b_i$, $r_i \in \mathbb{R}$. Wähle $l = \sum_{i=1}^n -\lfloor r_i \rfloor b_i$. Dann folgt

$$v + l = \sum_{i=1}^n (r_i - \lfloor r_i \rfloor) b_i = \sum_{i=1}^n a_i b_i \in P(B), \text{da } a_i \in [0,1].$$

(iii) Seien $v \neq w \in P(B)$, $v = \sum_{i=1}^n v_i b_i$ und $w = \sum_{i=1}^n w_i b_i$ mit $v - w \in L$. Es gilt

$$v - w = \sum_{i=1}^n (v_i - w_i) b_i \in L \quad \Longrightarrow \quad (v_i - w_i) \in \mathbb{Z} \cap [0,1],$$

wobei $(v_j - w_j) = 1$ für mindestens ein $1 \leq j \leq n$, da sonst $v = w$. Also $v - w \in \partial P(B) = \{\sum_{i=1}^n a_i b_i \mid 0 \leq a_i \leq 1, a_j = 1 \text{ für mindestens ein } 1 \leq j \leq n\}$.

□

### 2.1.1 Duale Gitter

Das duale Gitter sind alle Vektoren, die einen ganzzahligen Abstand zu den Gittervektoren haben.

**Definition 9.** *Sei* $L$ *ein volles Gitter in* $\mathbb{E}$*.*

[6] Im Allgemeinen ist die Determinante der von einer Menge von Vektoren aufgespannten Matrix gleich dem Volumen des von den Vektoren aufgespannten Parallelepipeds.

- *Das Gitter* $L^{\#} := \{v \in V \mid (v,l) \in \mathbb{Z} \text{ für alle } l \in L\}$ *heißt das* ***zu*** $L$ ***duale Gitter***.
- *Ist* $L \subseteq L^{\#}$, *so heißt* $L$ ***ganz***.
- *Ist* $L = L^{\#}$, *so heißt* $L$ ***unimodular***.

**Bemerkung 4.**
*Sei* $L$ *ein volles Gitter in* $\mathbb{E}$.

1. *Ist* $B$ *Basis von* $L$, *so bildet die Dualbasis* $B^*$ *eine Basis von* $L^{\#}$.
2. $\det(L)\det(L^{\#}) = 1$.
3. *Ist* $L$ *ganz, so ist die Faktorgruppe* $L^{\#}/L$ *eine endliche abelsche Gruppe mit* $|L^{\#}/L| = \det(L)$.

*Beweis:*

1.
2. $\mathcal{G}(L)\mathcal{G}(L^{\#}) = I$ nach Bemerkung 3 und $\det(\mathcal{G}(L)\mathcal{G}(L^{\#})) = \det(\mathcal{G}(L))\det(\mathcal{G}(L^{\#}))$ mit Induktion.
3. Es ist $L^{\#}/L = \{v + L \mid v \in L^{\#}\}$, wobei $v + L = \{v + l \mid l \in L\}$

□

Interessant ist auch, dass unimodulare Gitter unimodulare Grammatrizen haben (siehe auch [LoupOB]).

### 2.1.2 Wurzelgitter und Irreduzibilität

Sei $L$ ein Gitter in $\mathbb{E}$ mit Basis $B$.

**Definition 10.**
1. *Ist* $(l,l) \in 2\mathbb{Z}$ *für jedes* $l \in L$, *so heißt* $L$ ***gerade***.
2. *Die* $l \in L$ *mit* $(l,l) = 2$ *werden als* ***Wurzeln von*** $L$ *bezeichnet,* $L_{=2} = R(L) := \{l \in L \mid (l,l) = 2\}$.
3. *Ist* $L$ *ganz*[7] *und* $L = \langle R(L)\rangle_{\mathbb{Z}}$, *so heißt* $L$ ***Wurzelgitter***.

**Bemerkung 5.**
1. $L$ *Wurzelgitter* $\Longrightarrow$ $L$ *gerade.*
2. $L$ *gerade* $\Longrightarrow$ $L$ *ganz.*
3. *Sei* $L$ *ganz.* $L$ *gerade* $\Longleftrightarrow$ $(b_i, b_i) \in 2\mathbb{Z}$ *für jedes* $b_i \in B$.

[7] Also dim $L$ = dim $\mathbb{E}$ , da $L$ insbesondere volles Gitter ist.

*Beweis:*

1. Jeder Vektor $v \in L$ kann als $\mathbb{Z}$-Vielfaches $v = zl$ eines $l \in R(L)$ dargestellt werden, so dass $(v,v) = (zl,zl) = z^2(l,l) = 2z^2$ gilt und somit $L$ auch gerade ist.
2. $l \in L$, $L$ gerade $\Longrightarrow (l,l) \in 2\mathbb{Z} \subset \mathbb{Z} \Longrightarrow l \in L^{\#}$, also $L \subset L^{\#}$ ganz.
3. „$\Longrightarrow$“: Klar, da $B \subset L$.

   „$\Longleftarrow$“ Sei $\sum_i z_i b_i = l \in L$ mit $z_i \in \mathbb{Z}$. $\Longrightarrow$

$$(l,l) = (\sum_i z_i b_i, l) = \sum_i z_i (b_i, l) = \sum_i z_i (b_i, \sum_i z_i b_i) = \sum_i z_i \left( \sum_i z_i \underbrace{(b_i, b_i)}_{\in 2\mathbb{Z}} \right) \in 2\mathbb{Z}.$$

□

**Definition und Bemerkung 11.**

- *Ist $L$ ein Wurzelgitter, so heißt $W(L) := \langle \sigma_l \mid l \in R(L), \sigma_l$ Spiegelung entlang $l \rangle$ die* ***Weyl-Gruppe*** *von $L$.*
- *$W(L) \trianglelefteq \mathrm{Aut}(L)$ ist ein Normalteiler.*
- Erinnerung: *Eine Gruppe $G$ operiert transitiv auf einer Menge $M$, falls ein $m \in M$ existiert, so dass $Gm = M$.*

Die irreduziblen Gitter sind die kleinsten Bestandteile aller Gitter. Diese Aussage ist das Ziel des hiesigen Abschnitts.

**Definition und Bemerkung 12.**

- *Ein Gitter $L$ heißt* ***irreduzibel****, falls es nicht als orthogonale Summe*[8] *echter Teilgitter geschrieben werden kann.*
- *Ist $L$ ein irreduzibles Gitter, so operiert $W(L)$ transitiv auf $R(L)$.*
- Satz von Kneser: *Jedes Gitter lässt sich eindeutig als orthogonale Summer irreduzibler Teilgitter schreiben.*

### 2.1.3 Dynkin-Diagramme

Sei $L$ ein Gitter in $\mathbb{E}$ mit Basis $B = \{b_1, \ldots, b_k\}$. Neben der Determinante $\det(L)$ gibt es auch eine graphentheoretische Darstellung der Grammatrix von $L$.

**Definition und Bemerkung 13.** *Sei $G = (V,E)$ ein Graph mit*

- $V = B$,
- $E = \{(i,j) \mid (b_i, b_j) = -1\}$[9].

[8] direkte Summe orthogonal zueinander stehnder Teilräume

[9] Beachte: $(i,j)$ ist ein Tupel und $(b_i, b_j)$ Skalarprodukt.

*$G$ heißt* **Dynkin-*Diagramm zu* $L$.**
*$\mathcal{G}(B)$ ist bis auf Einträge $\neq -1$ die Adjazenzmatrix von $G$.*

Diese Diagramme veranschaulichen beispielsweise die Wurzelgitter, die nach Theorem 1.1 in [Ebeling] eine Basis $\{r_1, \ldots, r_k\}$ haben, so dass $(r_i, r_i) = 2$ und $(r_i, r_j) \in \{0, -1\}$ für $1 \leq i \neq j \leq k$.

### 2.1.4 Kugelpackungen

Sei $L$ ein Gitter in $\mathbb{E}$. Die Gitterpunkte können als Mittelpunkte von Kugeln aufgefasst werden, welche nicht überlappen und jeweils die Kugeln benachbarter Gitterpunkte berühren. Dazu werden noch einige Begriffe bezüglich der Gittervektoren benötigt.

**Definition und Bemerkung 14.**

- *Die Menge $L_{\leq S} = \{l \in L \mid (l,l) \leq S\}$ ist die Menge der Vektoren mit Länge $\leq S$ für ein $S \in \mathbb{R}$.*
- $\min(L) := \min\{(l,l) \mid l \in L \setminus \{0\}\}$ *heißt das* ***Minimum von*** $L$.
- $S(L) := \{l \in L \mid (l,l) = \min(L)\}$ *heißt* ***Menge der kürzesten Vektoren von*** $L$. $|S(L)|$ *heißt die* ***Kusszahl von*** $L$.

Das Minimum von $L$ ist also der kleinste Abstand zwischen zwei Gitterpunkten. Dieser Wert kann zur Definition der zu $L$ gehörigen Kugelpackung in $\mathbb{E}$ benutzt werden. Die Kugelpackung ist fest innerhalb des Gitters, deren Dichte kann aber durch Variation des Gitters verändert werden.

**Definition und Bemerkung 15.**

- *Für $x = (x_1, \ldots, x_m) \in L$ sind $N(x) := \{(x_1 + 1, x_2, \ldots, x_n), \ldots, (x_1, \ldots, x_{n-1}, x_n + 1)\}$ die* ***Nachbarn von $x$ in $L$.***

  $N(x) \stackrel{?}{=} \{l \in L \mid (x,l) = \min(L)\}$.

- *Eine* ***Kugelpackung***[10] *ist eine Anordnung von unendlich vielen, gleich großen, nicht überlappenden, $n$-dimensionalen Kugeln in $\mathbb{E}$.*

  *Auf $L$ kann eine Kugelpackung definiert werden, bei der die Mittelpunkte Gitterpunkte sind mit Radien $\frac{1}{2}\sqrt{\min(l)}$, die zu $L$ gehörige* ***gitterförmige Kugelpackung****.*

- *Die* ***Dichte einer Kugelpackung*** *ist das Verhältnis des Volumens der Kugelpackung zum Gesamtvolumen des Raums. Gitterförmige Kugelpackungen haben die Dichte*

$$\Delta(L) = \frac{1}{2^n}\sqrt{\gamma(L)}^n V_n,$$

  *wobei*

[10] Englisch: sphere packing

- $\gamma : \mathcal{L}_n \to \mathbb{R}_{\geq 0} : \gamma(L) = \frac{\min(L)}{\sqrt[n]{\det(L)}}$ *die* ***Hermite-Funktion*** *und*
- $V_n$ *das Volumen der n-dimensionalen Einheitskugel ist.*

- *Sei L ein Gitter. Die Kugeln der gitterförmigen Kugelpackung in L haben jeweils immer genau $|S(L)|$ direkte Nachbarkugeln.*

*Beweis:*

- 
- Der Radius ergibt sich als Folge des Satzes von PYTHAGORAS.
- 

□

Offenbar ist die Bestimmung der dichtesten Kugelpackung in $\mathbb{R}^n$, das heißt die Kugelpackung mit maximaler Dichte, gleichzusetzen mit der Maximierung der Hermite-Funktion.

**Extreme Gitter** Das Ziel des Abschnitts ist es, die Gitter mit maximalem HERMITE-Funktionswert, die *extremen Gitter*, zu charakterisieren.

**Definition und Bemerkung 16.**

- *Ist $L \cong L'$, so ist $\gamma(L) = \gamma(L')$. Das heißt, $\gamma : \mathcal{L}_n / \cong \to \mathbb{R}_{\geq 0}$.*
- *Ein Gitter L heißt* ***extrem****, falls $[L] \in \mathcal{L}_n / \cong$ ein lokales Maximum der* HERMITE-*Funktion ist.*

Im folgenden werden die Begriffe „perfekt“ und „eutaktisch“ zuerst für Matrizen und dann für Gitter definiert.

**Definition und Bemerkung 17.**

- *Eine symmetrische*[11]*, positiv definite Matrix $A \in \mathbb{R}^{n \times n}$ heißt* perfekt*, falls der Spaltenraum von A den Raum der symmetrischen $n \times n$-Matrizen erzeugt: $\langle x^T x \mid x \text{ Spalte von } A \rangle = \mathrm{Sym}_n(\mathbb{R})$.*

  *L heißt* ***perfekt****, falls $\mathcal{G}(L)$ perfekt ist.*

- *Eine symmetrische, positiv definite Matrix $A \in \mathbb{R}^{n \times n}$ heißt* eutaktisch*, falls $A^{-1} = \sum \rho_x x^T x$, x Spalte von A für gewisse $\rho_x \in \mathbb{R}_{>0}$.*

  *L heißt* ***eutaktisch****, falls $\mathcal{G}(L)$ eutaktisch ist.*

**Satz 1.**
*Ein Gitter ist genau dann extrem, wenn es perfekt und eutaktisch ist.*

[11] Das heißt, $A = A^T$.

Der VORONOI-Algorithmus ist eine Methode, perfekte Gitter zu finden.
Nicht bewiesen aber wichtig für die Termination der Suche nach perfekten beziehungsweise extremen Gittern ist folgende Folgerung.

**Folgerung 1.** *Da es nur endlich viele perfekte Gitter gibt, gibt es auch nur endlich viele extreme Gitter $L \in \mathcal{L}_n$.*[12]

## 2.2 Codes

Ganz allgemein sind Codes Mengen von Wörtern über einem Alphabet, die Bild einer Kodierungsabbildung sind. Als Alphabete werden hier endliche Körper $\mathbb{F}_q$ verwendet, die Codeworte sind also Folgen beziehungsweise Vektoren aus $\mathbb{F}_q^n$.
Bedingungen an den Code liefern brauchbare Eigenschaften für die Kodierungsabbildung. Dazu wird auf $\mathbb{F}_q^n$ das **Standardskalarprodukt** $\cdot : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q^n : x \cdot y \mapsto \sum_{i=1}^n x_i y_i$ definiert.

**Definition 18.** *1. Eine echte, nicht-leere Teilmenge $C \subset \mathbb{F}_q^n$ heißt **Code über** $\mathbb{F}_q$. $n$ ist die **Länge des Codes** $C$.*

*2. Ist $C \leq \mathbb{F}_q^n$ ein linearer Teilraum von $\mathbb{F}_q^n$ (aufgefasst als Vektorraum), so heißt $C$ **linearer Code über** $\mathbb{F}_q^n$ (im Folgenden als Code bezeichnet).*

*3. Für einen Code $C$ heißt der Orthogonalraum $C^\perp$ der **zu** $C$ **duale Code**.*

*4. Ist $C$ ein Code und $C \subseteq C^\perp$, so heißt $C$ **selbstorthogonal**. Ist sogar $C = C^\perp$, so heißt $C$ **selbstdual**.*

**Ziel:** Werden die Worte $v \in \mathbb{F}_q^k$ ($k$ nicht notwendig gleich $n$) als Informationsworte aufgefasst (für $q = 2$ beispielsweise Binärstrings), die durch einen fehleranfälligen Kanal übertragen werden, kann ein Code $C \leq \mathbb{F}_q^n$ zur Fehlerkorrektur dienen. Das Prinzip dabei ist es, $v$ mittels der Codeworte $c \in C$ auszudrücken, diese zu übertragen und zu dem empfangenen Wort $\tilde{c} \in \mathbb{F}_q^n$ das nächste Codewort $c' \in C$ bezüglich eines gegebenen Abstandsmaßes $d$ (hier der HAMMING-Abstand) zu bestimmen. Dabei ist natürlich $c = c'$ erwünscht.

Der Vorteil von *linearen* Codes ist die besonders einfache Struktur der Kodierungs- beziehungsweise Dekodierungsabbildung.

**Definition und Bemerkung 19.** *1. Das **Kodieren** eines Codes $C$ kann durch die Abbildung $\mathrm{cod} : \mathbb{F}_q^k \to \mathbb{F}_q^n : x \mapsto xG$ bewerkstelligt werden, wobei $G \in \mathbb{F}_q^{k \times n}$ die **Erzeugermatrix von** $C$ ist, das heißt, die Zeilen von $G$ sind die Basisvektoren von $C$.*

*2. Das **Dekodieren** eines Codes $C$ kann durch die Abbildung $\mathrm{decod} : \mathbb{F}_q^n \to \mathbb{F}_q^{n-k} : x \mapsto xP$ bewerkstelligt werden, wobei $P \in \mathbb{F}_q^{n \times (n-k)}$ die **Prüfmatrix von** $C$ ist, das heißt, die Spalten von $P$ sind die Basisvektoren von $C^\perp$.*

[12] Endlich viele bis auf Isometrie.

3. *Es gilt* $\text{Bild}(\text{cod}) = C = \text{Kern}(\text{decod})$.

4. *Das Bild* $vP$ *eines* $v \in \mathbb{F}_q^n$ *unter* decod *heißt auch das* ***Syndrom von*** $v$ ***unter der Basis von*** $C^\perp$. $v \in C$ *genau dann, wenn das Syndrom* $vP = 0$ *ist.*

*Beweis:* Sei $C \leq \mathbb{F}_q^n$ ein Code mit Basis $B$.

$$\begin{aligned} \text{Bild}(\text{cod}) &= \{v \in \mathbb{F}_q^n \mid \exists w \in \mathbb{F}_q^k : \text{cod}(w) = wG = v\} \\ &= \{v \in \mathbb{F}_q^n \mid \text{decod}(v) = vP = 0\} = \text{Kern}(\text{decod}) = C. \end{aligned}$$

Also ist $v \in C$ genau dann, wenn $v \in \text{Kern}(\text{decod})$ genau dann, wenn das Syndrom von $v$ gleich 0 ist. □

**Definition und Bemerkung 20.** 1. *Für* $x, y \in \mathbb{F}_q^n$ *bezeichnet*

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

*den* **Hamming-*Abstand***. *Der* Hamming-*Abstand ist eine Metrik.*

2. *Mit* $w(x) := |\{i \in [1, n] \mid x_i \neq y_i\}|$ *wird das* ***Gewicht*** *eines* $x \in \mathbb{F}_q^n$ *bezeichnet. Es gilt* $w(x) = d(x, 0)$.

3. *Für einen Code* $C \leq \mathbb{F}_q^n$ *heißt* $d(C) := \min\{w(x) \mid x \in C\}$ *das* ***Minimalgewicht von*** $C$.

**Bemerkung 6.**
*Sei* $C \subseteq \mathbb{F}_q^n$ *ein linearer Code.*

1. *Es gilt* $d(C) = \min\{d(x, y) \mid x, y \in C\}$.

2. *Die (über den fehleranfälligen Kanal) empfangenen Codeworte* $\tilde{c} \in \mathbb{F}_q^n$ *können höchstens den Abstand* $d(C)$ *von einem* $c' \in C$ *haben, das bedeutet, sie können sich von* $c'$ *um höchstens* $d(C)$ *Komponenten unterscheiden.*

Eine Möglichkeit des Dekodierens ist also das Wählen des am nächsten liegenden Codeworts.

**Definition 21.** *Für einen Code* $C \leq \mathbb{F}_q^n$ *heißt die Abbildung* $f : \mathbb{F}_q^n \to C$ ***minimal distance decoder (MDD)****, falls* $d(f(v), v) = \min\{d(c, v) \mid c \in C\}$ *ist.*

Ein MDD $f : \mathbb{F}_q^n \to C$ weist jedem empfangenen Informationswort $v \in \mathbb{F}_q^n$ ein Codewort $f(v) \in C$ zu. Es gibt nun zwei Fälle:

1. $d(v, f(v)) \geq \frac{d(C)}{2}$: Das erkannte Codewort ist nicht notwendig eindeutig bestimmt und somit nicht notwendig das vor der Übertragung gewählte.

2. $d(v, f(v)) < \frac{d(C)}{2}$: Der MDD kann eindeutig entscheiden, welches von je zwei Codeworten am nächsten zu $v$ liegt. Gäbe es nämlich ein weiteres $c' \neq c := f(v)$ mit $c' < \frac{d(C)}{2}$, so gälte nach der $\triangle$-Ungleichung beziehungsweise Symmetrie von $d$

$$d(c, c') \leq d(c, v) + d(v, c') < \frac{d(C)}{2} + \frac{d(C)}{2} = d(C),$$

was ein Widerspruch zur Minimalität von $d(C)$ ist.

**Beispiel 1.** *Der Code $C = \{(0, \ldots, 0), (1, \ldots, 1)\} \subset \mathbb{F}_2^n$ heißt **binärer Wiederholungscode der Länge** $n$. Es ist $d(C) = n$.*

- *Ist $n$ ungerade, so kann stets entschieden werden, welchem der Codeworte das vorliegende fehlerhafte Informationswort zuzuweisen ist.*
- *Ist $n$ jedoch gerade, kann zu einem Informationswort mit genau $\frac{n}{2}$ Einsen nicht eindeutig eines der Codeworte bestimmt werden.*

Die Codes, bei denen einen eindeutige Zuweisung möglich ist, werden allgemein auf folgende Art charakterisiert.

**Definition 22.** *Ein Code $C \subset \mathbb{F}_q^n$ heißt **perfekt**, falls es eine Zahl $e$ gibt, so dass zu jedem $v \in \mathbb{F}_q^n$ genau ein $c \in C$ existiert mit $d(v, c) \leq e$.*

Aus der obigen Analyse des MDD ergibt sich die obere Schranke $e < \frac{d(C)}{2}$ für einen Code $C$. Die Zahl $e$ ist also die Anzahl der von dem zu $C$ gehörigen MDD korrigierten Übertragungsfehler.

**Beispiel 2.**
- *Der Binäre Wiederholungscode ist für ungerade $n$ und $e = \frac{d(C)-1}{2} = \frac{n-1}{2}$ perfekt, für gerade $n$ jedoch nicht.*
- ***Triviale Codes** $C = \{c\} \subseteq \mathbb{F}_q^n$ [13] sind perfekt mit $e = \max\{d(c, v) \mid v \in \mathbb{F}_q^n\}$.*
- *Der Code $\mathbb{F}_q^n$ ist mit $e = 0$ ebenfalls perfekt, da $d(v, v) = 0$ für alle $v \in \mathbb{F}_q^n$.*

Die folgende Charakterisierung *binärer* perfekter Codes erlaubt eine strukturelle Betrachtung derselben[14].
Betrachte die Abbildung

$$f : \mathcal{P}\mathrm{ot}([1, n]) \to \mathbb{F}_2^n : M \mapsto (\sum_{m \in M} \delta_{m,1}, \ldots, \sum_{m \in M} \delta_{m,n})$$

und die Äquivalenzrelationen

$$\begin{aligned} \sim &:= \{(m, n) \mid w(m) = w(n)\} \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^n, \\ \approx &:= \{(M, N) \mid |N| = |M|\} \subseteq \mathcal{P}\mathrm{ot}([1, n]) \times \mathcal{P}\mathrm{ot}([1, n]). \end{aligned}$$

[13] das heißt, Codes mit Länge 1
[14] siehe Seite 61 in [Ebeling]

Offenbar ist somit

$$\mathcal{P}\mathrm{ot}([1,n])\,/\!\approx \;\cong \mathbb{F}_2^n\,/\!\sim$$

vermöge der auf die Faktorstrukturen fortgesetzten Abbildungsvorschrift von $f$ und unter der Vereinigung $\cup$ auf $\mathcal{P}\mathrm{ot}([1,n])$ und der Addition auf $\mathbb{F}_2^n$. Die gehen also mit den gleichmächtigen Teilmengen $P \subseteq \mathcal{P}\mathrm{ot}([1,n])$ gehen also mit den Klassen $f(P) \subseteq \mathbb{F}_2^n$ von Informationsworten gleichen Gewichts bezüglich des HAMMING-Abstandes einher.

**Bemerkung 7.**
*$C \subset \mathbb{F}_2^n$ ist perfekt genau dann, wenn $|C|(\sum_{i=0}^{e}\binom{n}{i}) = 2^n$.*

*Beweis:* □

**Beispiel 3.** *Prüfen von Bemerkung 7.*

- *Binärer Wiederholungscode für $n = 5$: $2 \cdot (1 + 5 + 10) = 2 + 10 + 20 = 32 = 2^5$.*

### 2.2.1 HAMMING-Codes

Dieser Unterabschnitt behandelt die Klasse der HAMMING-Codes als ein weiteres Beispiel.

**Definition und Bemerkung 23.** *Seien $\mathbb{F}_q$ ein endlicher Körper, $r \in \mathbb{N}$ und $n := \frac{q^r-1}{q-1}$.*

- *$n$ ist die Anzahl der 1-dimensionalen Teilräume $\langle x_i\rangle$ $(1 \le i \le n)$ von $\mathbb{F}_q^r$.*[15]
- *Die Matrix $P \in \mathbb{F}_q^{n\times r}$, die die $x_i \in \mathbb{F}_q^r$ als Zeilen hat, hat Rang $r$ und paarweise linear unabhängige Zeilen.*

*Der Code mit Prüfmatrix $P$ heißt* **HAMMING-*Code der Länge* $n$** *und wird mit $H(\mathbb{F}_q, r)$ bezeichnet.*

**Bemerkung 8.**

- *$H(\mathbb{F}_q, r) \le \mathbb{F}_q^r$ ist linear.*
- *$H(\mathbb{F}_q, r)$ ist perfekt mit $e = 1$.*
- *$d(H(\mathbb{F}_q, r)) = 3$.*

*Beweis:*

- Die Spalten der Prüfmatrix $P \in \mathbb{F}_q^r$ von $H(\mathbb{F}_q, r)$ sind die Erzeuger des HAMMING-Codes, oder genauer:
$$H(\mathbb{F}_q, r) = \mathrm{Kern}(\mathrm{decod} : \mathbb{F}_q^n \to \mathbb{F}_q^r)$$
- Sei $a \in \mathbb{F}_q^n$. Es ist Zeige: $aP \in H(\mathbb{F}_q, r)$ ist eindeutig mit $d(a, aP) \le 1$.
$$d(a, aP) = |\{i \in [1,n] \mid a_i \neq a_i(P)_i\}|$$

□

[15] Zähle die linear unabhängigen Vektoren aus $\mathbb{F}_q^r$.

# 3 Ergebnisse und deren Verwendung

## 3.1 Codegitter

Die Hauptanwendung der Gittertheorie auf Codes ist in folgender Definition verankert, die **Konstruktion A** genannt wird.

**Definition 24.** *Seien $p$ Primzahl, $C \leq \mathbb{F}_p^n$ ein Code über $\mathbb{F}_p$ der Länge $n$, $\{e_1, \ldots, e_n\}$ eine Orthogonalbasis von $\mathbb{E}$ mit $(e_i, e_i) = \frac{1}{p}$ sowie $M = \langle e_1, \ldots, e_n \rangle_{\mathbb{Z}}$ ein Gitter. Ferner sei*

$$\pi : M \to \mathbb{F}_p^n : e_i \mapsto \bar{e}_i$$

*der natürliche Epimorphismus vermöge der Identifikation $^-$ von $\mathbb{F}_p$ in $\mathbb{R}$ als Restklassenkörper $\mathbb{Z}_p = Z / \langle p \rangle$. Es gilt:*

1. *$\pi$ Epimorphismus, da $^-$ Epimorphismus ist.*
2. *$\mathrm{Kern}(\pi) = \{m \in M \mid \pi(m) = \bar{0}\} = pM$.*
3. *$\pi^{-1}(C) = \{m \in M \mid m = \sum_{i=1}^n a_i e_i, \bar{a}_i, \bar{e}_i \in C\} = \langle e_{i_1}, \ldots, e_{i_m} \mid \pi(e_{i_j}) = \bar{e}_{i_j} \in C \rangle_{\mathbb{Z}} \leq M$ ist ein Gitter in $\mathbb{E}$.*

*$L_C := \pi^{-1}(C)$ heißt das **Codegitter zu $C$ in $\mathbb{E}$**.*

Mit dieser Definition fallen einige Begriffe über Gittern mit Begriffen über Codes zusammen. Sei nun $C \leq \mathbb{F}_p^n$ ein Code über $\mathbb{F}_p$ der Länge $n$ und $L_C$ das Codegitter zu $C$ in $\mathbb{E}$.

**Bemerkung 9.**

- $L_C^{\#} = L_{C^\perp}$.
- *$L_C$ ist genau dann ganz (beziehungsweise unimodular), wenn $C$ selbstorthogonal (beziehungsweise selbstdual) ist.*

*Beweis:*

- Verwende $(e_i, e_i) = \frac{1}{p}$.
- Folgt direkt aus dem ersten Punkt.

□

**Definition und Bemerkung 25.**

- *Ein Code $C \leq \mathbb{F}_p^n$ heißt **doppelt-gerade**, falls $w(c) \in 4\mathbb{Z}$ für alle $c \in C$.*
- *$L_C$ ist genau dann gerade, wenn $C$ ein binärer, doppelt-gerader Code ist.*

Das Minimalgewicht $d(C)$ von $C$ und das Minimum $\min(L_C)$ von $L_C$ hängen in folgender Weise zusammen.

**Bemerkung 10.**

- $\min(L_C) \geq \min\{p, \frac{1}{p}d(C)\}$.
- *Ist* $p \in \{2, 3\}$*, so gilt sogar* $\min(L_C) = \min\{p, \frac{1}{p}d(C)\}$.

*Beweis:*

□

Offenbar sind viele Eigenschaften der Gitter und Codes durch die Konstruktion A vereinbar. *Frage:* Lassen sich so auch perfekte Codes charakterisieren?

## 3.2 Orthogonalisierung

Ein Gitter mit einer orthogonalen Basis hat einige folgende brauchbare Eigenschaften.

**Bemerkung 11.**
*Sei $L$ ein Gitter mit einer orthogonalen Basis $(b_1, \ldots, b_n)$.*

- $\mathcal{G}(L) = \mathrm{diag}((b_i, b_i) \mid 1 \leq i \leq n)$.
- $\det(L) = \prod_{i=1}^{n}(b_i, b_i)$.
- *$L$ ist isometrisch zu $\mathbb{Z}^n$.*
- *Sei $p$ eine Primzahl. $L$ ist ein Codegitter, falls $(b_i, b_i) = \frac{1}{p}$ für $i \in \{1, \ldots, n\}$ und $L = L_C = \pi^{-1}(C)$ für eine Einbettung $\pi : L \to \mathbb{F}_p^n : e_i \mapsto \bar{e}_i$.*

**Algorithmus 1 (Gram-Schmidt Orthogonalisierungsverfahren).**

| | |
|---|---|
| ***Eingabe:*** | *Basis $(b_1, \ldots, b_n)$ von $\mathbb{E}$* |
| ***Verfahren:*** | *Für $i = 1, \ldots, n$: $b'_i := b_i - \sum_{j=1}^{i-1} \underbrace{\frac{(b_i, b'_j)}{(b'_j, b'_j)}}_{:=\mu_{ij}} b'_j$.* |
| ***Ausgabe:*** | *Orthogonalbasis $(b'_1, \ldots, b'_n)$ von $\mathbb{E}$, so dass $\langle b_1, \ldots, b_i\rangle_{\mathbb{R}} = \langle b'_1, \ldots, b'_i\rangle_{\mathbb{R}}$ für jedes $1 \leq i \leq n$.* |

Die Vektoren $b'_i$ der Orthogonalbasis werden sukzessive aus den bereits berechneten Basisvektoren $b'_j$ für $1 \leq j \leq i-1$ und $b_i$ berechnet.

**Bemerkung 12 (Korrektheit des Orthogonalisierungsverfahren).**
*$B'$ aus Algorithmus 1 ist eine Orthogonalbasis von $\mathbb{E}$.*

*Beweis:* Zu zeigen ist, dass im $i$-ten Schritt $b'_i \perp \langle b'_1, \ldots, b'_{i-1}\rangle$.
Anstatt die gewünschten Eigenschaften nachzurechnen wird hier eine Herleitung gewählt.

Es muss gelten

$$(b'_i, b'_k) = 0 \quad \text{für alle} k \in \{1, \ldots, i-1\}. \tag{1}$$

Ansatz: Kombiniere $b'_i$ aus den bereits gebildeten $b'_k$ und $b_i$.
Bilde dazu den Differenzvektor

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

und bestimme $\mu_{ij}$ durch Einsetzen in (1). Sei nun dazu $k \in \{1, \ldots, i-1\}$. Einsetzen ergibt

$$0 = (b'_i, b'_k) = (b_i - \sum_{j=1}^{i-1} \mu_{ij} b'_j, b'_k) = (b_i, b'_k) - \sum_{j=1}^{i-1} \mu_{ij} (b'_j, b'_k).$$

für zu gewisse $\mu_{ij}$. Betrachte folgende Umformungen zur Bestimmung von $\mu_{ik}$.

$$\begin{aligned} 0 &= (b_i, b'_k) - \sum_{j=1}^{i-1} \mu_{ij} (b'_j, b'_k) \\ &= (b_i, b'_k) - \sum_{j=1}^{i-1} \mu_{ij} (b'_j, b'_k) \overset{(b'_j, b'_k)=0 \text{ für } j \neq k}{=} (b_i, b'_k) - \mu_{ik} (b'_k, b'_k) \quad \Longleftrightarrow \\ \mu_{ik} &= \frac{(b_i, b'_k)}{(b'_k, b'_k)}. \end{aligned}$$

□

Sei nun $\langle B \rangle_{\mathbb{Z}} \subset \mathbb{E}$ ein volles Gitter mit Basis $B$ und $B'$ die zu $B$ orthogonale Basis.

**Bemerkung 13.**
$\det(\langle B \rangle_{\mathbb{Z}}) = \det(\langle B' \rangle_{\mathbb{Z}}) = \prod_{i=1}^{n} (b'_i, b'_i)$.

*Beweis:* $\mathcal{G}(B')$ ist eine Diagonalmatrix. Der Rest folgt durch Nachrechnen und Induktion. □

Dies läßt die folgende Abschätzung zu.

**Lemma 1 (Hadamard Ungleichung).** *Sei $L$ ein Gitter mit Basis $B$. Es ist* $\det(L) \leq \prod_{i=1}^{n} (b_i, b_i)$.

*Beweis:*

□

Für die bisher betrachteten Begriffe bedeutet dies Folgendes.

**Folgerung 2.** *Sei $L$ ein Gitter mit Basis $(b_1, \ldots, b_n)$.*

$$\text{vol}(P(B)) \overset{\text{Def. u. Bem. 8}}{=} \sqrt{\det(L)} = \sqrt{\det(\mathcal{G}(L))} \overset{\text{Lemma 1}}{\leq} \prod_{i=1}^{n} (b_i, b_i).$$

Das obige Verfahren kann ebenfalls zur Bestimmung einer dualen Basis verwendet werden.

**Algorithmus 2 (Orthonormierungsverfahren).**

| | |
|---|---|
| ***Eingabe:*** | *Basis* $(b_1, \ldots, b_n)$ *von* $\mathbb{E}$ |
| ***Verfahren:*** | *(1) Berechne über das* Gram-Schmidt *Orthogonalisierungsverfahren eine orthogonale Basis* $B'$. |
| | *(2) Setze* $B^* := \{b^* \mid b^* = \frac{b'}{(b',b')}, b' \in B'\}$. |
| ***Ausgabe:*** | *Orthonormalbasis* $(b_1^*, \ldots, b_n^*)$ *von* $\mathbb{E}$ |

**Bemerkung 14 (Korrektheit des Orthonormierungsverfahren).**
*$B^*$ aus Algorithmus 2 ist eine Dualbasis.*

*Beweis:* Durch Nachrechnen. Sei $b_i^* \in B^*$. Dann gilt

$$(b_i^*, b_i^*) = (\frac{b_i'}{(b_i', b_i')}, b_i') = \frac{(b_i', b_i')}{(b_i', b_i')} = 1.$$

□

Die Orthognalsisierung ist auch durch andere Verfahren erreichbar, etwa durch eine $QR$-Zerlegung der Matrix $A$, die aus den Gitterbasisvektoren besteht. Dann gilt $A = QR$, wobei $Q$ orthogonal ist und $R$ eine rechte obere Dreiecksmatrix.

### 3.3 Endlichkeit

Sei $L$ ein Gitter. Die Ganzzahligkeit der Koeffizienten der Gittervektoren $l \in L$ liefert die Endlichkeit verschiedener Mengen im Umfeld von $L$.

**Satz 2.**

1. *Die Menge der kurzen Vektoren* $L_{\leq S} = \{l \in L \mid (l, l) \leq S\}$ *ist endlich.*
2. *Die Automorphismengruppe* $\mathrm{Aut}(L)$ *von* $L$ *ist endlich.*

*Beweis:*

1.

□

### 3.4 Äquivalenzen bei Gittern und Codes

Sowohl für Gitter als auch für Codes ist die Vergleichbarkeit definierbar. Im folgenden werden die wichtigsten Notationen aufgeführt.

**Erinnerung 2.**
- *Eine Matrix* $A \in \mathbb{R}^{n \times n}$ *ist* ***orthogonal****, wenn eine der folgenden äquivalenten Bedingungen gilt:*

1. $A^T A = I$.
2. *Die Spalten oder Zeilen von $A$ zueinander orthonormal sind.*
3. $(v, w) = (Av, Aw)$ *für alle* $v, w \in \mathbb{R}^n$.

**Definition 26.** 1. *Seien $L, L'$ Gitter in $\mathbb{E}$.*

- *$L$ und $L'$ heißen* ***isometrisch****, falls es einen orthogonalen Automorphismus $g : \mathbb{E} \to \mathbb{E}$[16] gibt, so dass $Lg = L'$.*
- $\mathrm{Aut}(L) := \{g \in \mathrm{O}(\mathbb{E}) \mid Lg = L\}$ *heißt die* ***Automorphismengruppe von*** *$L$.*

2. *Seien $C, C' \leq \mathbb{F}_q^n$ zwei Codes.*

- *$C$ und $C'$ heißen* ***permutationsäquivalent****, falls es ein $g \in S_n$ gibt mit $gC = \{(c_{g(1)}, \ldots, c_{g(n)}) \mid (c_1, \ldots, c_n) \in C\} = C'$.*
- $\mathrm{Aut}(C) := \{g \in S_n \mid gC = C\}$ *heißt die* ***Automorphismengruppe von*** *$C$.*

**Bemerkung 15.**

1. *Isometrische Gitter haben die gleiche Grammatrix.*
2. *Ist $L$ ein volles Gitter mit Orthogonalbasis $B' = (b'_1, \ldots, b'_n)$. Dann ist $L$ isometrisch zu $\mathbb{Z}^n$.*

*Beweis:* Die Normierung der Basisvektoren ist eine orthogonale Transformation $g = \mathrm{diag}(\frac{1}{(b'_i, b'_i)} \mid 1 \leq i \leq n)$. Dann gilt für alle $b'_i \in B'$

$$gb'_i = \sum_{j=1}^{n} g_{ij} b'_i = \frac{b'_i}{(b'_i, b'_i)}.$$

Dann liegt bis auf Drehung, welche wieder eine orthogonale Transformation ist, die Standardbasis von $\mathbb{Z}^n$ vor. □

**Bemerkung 16.**

1. *Ist $C \leq \mathbb{F}_q^n$ ein Code und $g \in S_n$, so ist $gC^\perp = (gC)^\perp$.*[17]
2. *Permutationsinvarianz eines Codes $C \leq \mathbb{F}_q^n$ induziert Isometrie des zugehörigen Codegitters $L_C$.*

*Beweis:*

1.
2. Permutation der nichtnegativen Basisvektorkomponenten ist eine orthogonale Transformation.

□

[16] das heißt, eine orthogonale Matrix $g \in \mathrm{O}(\mathbb{E}) \subset \mathbb{R}^{n \times n}$.

[17] Also zum einen ist $g$ *invariant* unter der Orthogonalisierung, zum anderen erhält $g$ die Orthogonalität.

## 3.5 Bestimmung kurzer Vektoren

Das Bestimmen der kürzesten Vektoren eines Gitter $L$ ist für die Berechnung des Minimums $\min(L)$ wichtig, das sowohl beim Finden dichter Kugelpackungen (siehe Definition und Bemerkung 15) als auch bei der Abschätzung des Minimalgewichts eines Codes hilfreich sein kann. Der LLL-Algorithmus leistet dies und wird im Folgenden auf intuitiver Ebene erklärt. LLL steht für die drei Anfangsbuchstaben der Erfinder: Lenstra, Lenstra und Lovasz.
Die durch den Algorithmus berechneten Basisvektoren sind nicht notwendig die kürzesten Vektoren, sie liegen aber sehr nahe daran. Die Ausgabe-Basis des Algorithmus wird im folgenden definiert.

**Definition 27.** *Seien $L$ ein Gitter mit Basis $B = \{b_1, \ldots, b_n\} \subseteq \mathbb{R}^n$ und $\mu_{ij} = \frac{(b_i, b'_j)}{(b'_j, b'_j)}$ die Koeffizienten aus der* Gram-Schmidt*-Orthogonalisierung sowie $B' = \{b'_1, \ldots, b'_n\}$ die so berechnete Orthogonalbasis.*
*$B$ heißt **LLL-reduziert**, falls*

*(1)* $|\mu_{ij}| \leq \frac{1}{2}$ *und*

*(2)* $(b'_i, b'_i) + \mu^2_{i,i-1}(b'_{i-1}, b'_{i-1}) \geq \frac{3}{4}(b'_{i-1}, b'_{i-1})$ *für alle* $2 \leq i \leq n$.

Die Elemente LLL-reduzierter Basen erfüllen also bestimmte Bedingungen an deren Längendifferenz (2) und deren Orthogonalität (1) bezüglich der Gram-Schmidt-Orthogonalisierung. Der LLL-Algorithmus[18] kann für jedes beliebige Gitter eine LLL-reduzierte Basis bestimmen. Dazu werden (1) und (2) für jeden Basisvektor geprüft, bei Nichterfülltsein werden die entsprechenden Vektoren in der Länge reduziert. Die Änderungen werden stets in der Transformationsmatrix $T$ festgehalten.
Zum besseren Verständnis noch einige Bemerkungen:

Zu (1): Es gilt

$$0 = \mu_{ij} = \frac{(b_i, b'_j)}{(b'_j, b'_j)} \quad \Longleftrightarrow \quad (b_i, b'_j) = 0 \quad \Longleftrightarrow \quad b_i \perp b'_j$$

und ferner

$$1 = \mu_{ij} = \frac{(b_i, b'_j)}{(b'_j, b'_j)} \quad \Longleftrightarrow \quad (b_i, b'_j) = (b'_j, b'_j) \quad \Longleftrightarrow \quad b_i = b'_j.$$

Mit einer Abweichung von $\mu_{ij}$ nimmt also die Orthogonalität von $b_i$ und $b'_j$ ab. Der Algorithmus versucht im ersten Teil des Schleifenrumpfes

Zu (2): Der Parameter $\frac{3}{4}$ beschreibt die Abweichung der Längen zwischen $b_i$ und $b_{i-1}$. Ist die Ungleichung erfüllt, so wird durch Subtraktion der $\mu_{i,j}$ von $b_j$ für alle $j \leq i-2$ und anschließender entsprechender Aktualisierung der übrigen $\mu_{kl}$ für $l \leq j-1$ die Bedingung erfüllt.

[18] Algorithmus 3.10 in [Nebe]

**Algorithmus 3 (LLL-Algorithmus).**

| | |
|---|---|
| ***Eingabe:*** | *Basis* $B = (b_1, \ldots, b_n)$ *des Gitters* $L$ *in* $\mathbb{E}$ |
| ***Verfahren:*** | *Bestime Orthogonalbasis* $B' := \{b'_i := b_i - \sum_{j=1}^{i-1} \mu_{ij} b'_j \mid b_i, b_j \in B\}$. |
| | *Setze* $k := 2$, $\tilde{B} := B$, $T := I$. |
| | *Solange* $k \leq n$: |
| *Teste (1):* | *Falls* $\lvert\mu_{k,k-1}\rvert < \frac{1}{2}$: |
| | *Reduziere* $\tilde{b}_k$ *vermöge* $\mu_{k,k-1}$. |
| | *Aktualisiere* $\mu_{kj}$ *für* $1 \leq j \leq k-2$. |
| | *Setze* $b'_k := \tilde{b}_k - \sum_{j=1}^{k-1} \mu_{kj} b'_j$. |
| *Teste (2):* | *Falls* $(b'_k, b'_k) + \mu^2_{k,k-1}(b'_{k-1}, b'_{k-1}) \geq \frac{3}{4}(b'_{k-1}, b'_{k-1})$: |
| | *Für* $j = k-2, \ldots, 1$: |
| | *Reduziere* $\tilde{b}_k$ *vermöge* $\mu_{k,j}$. |
| | *Setze* $k := k+1$. |
| | *Sonst:* |
| | *Tausche* $b_k$ *und* $b_{k-1}$, $k$*-te und* $(k-1)$*-te Spalte von* $T$. |
| | *Setze* $k := k-1$. |
| ***Ausgabe:*** | *Transformationsmatrix* $(t_{ij}) = T \in \mathrm{Gl}_n(\mathbb{Z})$ *mit* $\tilde{b}_i = \sum_{j=1}^{n} t_{ij} b_j$, |
| | *so dass* $\tilde{B} = (\tilde{b}_1, \ldots, \tilde{b}_n)$ *LLL-reduziert und* $L = \langle B \rangle_{\mathbb{Z}} = \langle \tilde{B} \rangle_{\mathbb{Z}}$. |

Die LLL-reduzierten Basisvektoren sind nicht notwendig kürzeste Vektoren von $L$. Diese können aber mittels der LLL-reduzierten Basis schneller berechnet werden. Ein Verfahren dazu ist, die Menge $L_{\leq S}$ für verschiedene $S$ über einer LLL-reduzierten Basis von $L$ zu bestimmen und etwa mittels binärer Suche die Schranke $S$ bis auf $\min(L)$ einzugrenzen (vergleiche Satz 2).
In der LLL-reduzierten Basis $\tilde{B} = (\tilde{b}_1, \ldots, \tilde{b}_n)$ ist $\tilde{b}_1$ der dem kürzesten Vektor in $L$ am nächsten liegende Vektor, $\tilde{b}_2$ der nächst kürzeste zu $\tilde{b}_1$ linear unabhängige Vektor und so weiter.

### 3.5.1 Anwendungen

**Ganzzahlige lineare Optimierung**

# 4 Beispiele von Gittern

In diesem Abschnitt sollen alle Begriffe über Gittern veranschaulicht werden.

## 4.1 Standardgitter

Eins der einfachsten Beispiele für Gitter ist $L := \mathbb{Z}^m$ in $\mathbb{E}$ für $m \leq n$.

- Basis besteht aus den Standardbasisvektoren $e_i$ des $\mathbb{R}^n$.

- $L$ ist voll, falls $m = n$.
- $\det(L) = \det(E_m) = 1$.
- $P(B) = \{v \in \mathbb{R}^m = \mathbb{R}L \mid (l, l) \leq 1\}$, $\text{vol}(P(B)) = \sqrt{\det(L)} = 1$.
- $L^{\#} = L$, weswegen $L$ ganz und unimodular ist und die Faktorgruppe $L^{\#}/L \cong \{0\}$.
- Wegen $(e_1, e_2) = 1$ ist $L$ nicht gerade.
- $\min(L) = 1$ und $S(L) = \{\pm e_1, \pm e_2\}$, womit 4 die Kusszahl von $L$ ist.

## 4.2 Hexagonales Gitter

Das hexagonale Gitter $\mathbb{A}_n$ ist extrem.

# Index