3.3 Reduzierte Basen nach Lenstra, Lenstra und Lovász

Alternativ zu klassischen Konzepten wie dem von Minkowski gibt es seit gut 25 Jahren den Reduktionsbegriff von Hendrik W. Lenstra, Arjen Lenstra und Laslo Lovász. Er kommt Hand in Hand mit einem effektiven Algorithmus zur Bestimmung einer reduzierten Basis aus einer gegebenen Basis. Die Struktur der Abschätzungen ist wie bei Minkowski, die Konstanten sind naturgemäß schlechter. Bereits Minimalvektoren werden nur "approximiert", nicht mehr sicher bestimmt. Der LLL-Algorithmus ist von großer praktischer Bedeutung für alle Probleme, die auf ganzzahlige lineare Algebra führen.

In diesem Abschnitt legen wir weiterhin einen n-dimensionalen reellen Vektorraum E mit Skalarprodukt $\langle -, - \rangle$ zugrunde. Wir erinnern an das im wesentlichen aus der Linearen Algebra bekannte Orthogonalisierungsverfahren nach Gram und Schmidt: Die Orthogonalisierung einer Basis $v_1, v_2, ..., v_n$ ist die durch die Formeln

$$\begin{aligned} v_1^* &:= v_1 \\ v_i^* &:= v_i - \sum_{j=1}^{i-1} \mu_{ij} v_j^*, \text{wobei } \mu_{ij} := \frac{\langle v_i, v_j^* \rangle}{\langle v_j^*, v_j^* \rangle} \end{aligned}$$

gegebene Basis $v_1^*, ..., v_n^*$ von E. Alle Basen $w_1, ..., w_n$ mit

$$\begin{aligned} w_1 &= v_1 = v_1^* \\ w_i &= v_i^* + \sum_{j=1}^{i-1} \lambda_{ij} v_j^* \end{aligned}$$

mit beliebigen Koeffizienten $\lambda_{ij} \in \mathbb{R}$, $i > j$, führen auf die gleiche Orthogonalisierung $w_i^* = v_i^*$, $i = 1, ..., n$. Wichtig ist, dass wir lediglich orthogonalisieren; die Betrachtung einer Orthonormalbasis wäre für die Reduktion nicht zielführend. Die Orthonormalisierung nach Gram-Schmidt liefert einen (begrifflich) anderen Zugang zur Dreieckszerlegung erster Art einer positiv definiten quadratischen Form; entsprechend liefert die eben beschriebene Orthogonalisierung die Dreieckszerlegung zweiter Art.

Sei nun $\{b_1, ..., b_n\}$ eine $\mathbb{Z}$-Basis eines Gitters L. Dann besteht zwischen den Längen $\|b_i^*\|$ der Vektoren b_i^* der orthogonalisierten Basis und dem Minimum von L der folgende Zusammenhang.

Lemma 3.3.1 *Es gilt* $\min L \geq \min\{\|b_1^*\|, ..., \|b_n^*\|\}$

Beweis: Sei $b \in L$ ein beliebiger Gittervektor, $b = \sum_{i=1}^n \lambda_i b_i$ mit $\lambda_i \in \mathbb{Z}$ für $1 \leq i \leq n$. Sei k der größte Index mit $\lambda_k \neq 0$. Wir ersetzen in der Darstellung

[5] Mein Dank geht an Herrn Dr. Ralf Gerkmann für wesentliche Beiträge zu diesem Skriptteil im Rahmen einer Vorlesungsvertretung im Sommersemester 2001.

von b die Vektoren b_i, $i = 1, \ldots, k$ durch $\sum_{i=1}^{j} \mu_{ij} b_j^*$. Dadurch erhalten wir eine neue Darstellung $b = \sum_{i=1}^{k} \lambda_i^* b_i^*$ mit $\lambda_k = \lambda_k^* \in \mathbb{Z}$, $\lambda_k \neq 0$. Somit ist

$$\|b\|^2 = \sum_{i=1}^{k} (\lambda_i^*)^2 \|b_i^*\|^2 \geq \lambda_k^2 \|b_k^*\|^2 \geq \|b_k^*\|^2$$

woraus sich die Behauptung ergibt. □

Bemerkung Die Aussage von Lemma 3.3.1 kann als eine Verallgemeinerung der im vorigen Abschnitt nicht im Detail bewiesenen Abschätzung (3.2.10) angesehen werden.

Wir interessieren uns nun für Basen (v_i), die „möglichst" orthogonal sind, d.h. möglichst nahe an ihrer Orthogonalisierung (v_i^*) liegen. Dieses motiviert die erste Bedingung (i) der folgenden Definitionen.

Definition 3.3.2 Es sei c eine fest gewählte Konstante c mit $\frac{3}{4} \leq c < 1$. Eine Basis $b_1, ..., b_n$ von E heißt *LLL-reduziert*, falls folgendes gilt:

(i) $|\mu_{ij}| \leq \frac{1}{2}$ für $1 \leq i < j \leq n$

(ii) $\|b_i^*\|^2 \geq (c - \mu_{i,i-1}^2)\|b_{i-1}^*\|^2$ (*die LLL-Bedingung*)

Dabei ist wie oben $b_1^*, ..., b_n^*$ die Gram-Schmidt-Orthogonalisierung von $b_1, ..., b_n$ und $\mu_{ij} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}$.

Bevor wir uns den Eigenschaften von LLL-reduzierten Basen zuwenden, notieren wir zunächst:

Satz 3.3.3 *Jedes Gitter besitzt eine LLL-reduzierte Basis.*

Man konstruiert eine solche Basis (und beweist somit den Satz) durch den weiter unten angegebenen LLL-Algorithmus. Dabei wird darüber hinaus noch eine Aussage über den Aufwand gemacht, der zur Bestimmung einer solchen Basis im ungünstigsten Fall erforderlich ist. Man beachte noch, dass es nur von der Gram-Matrix $(\langle b_i, b_j \rangle)_{1 \leq i,j \leq n}$ abhängt, ob $b_1, ..., b_n$ LLL-reduziert ist oder nicht. Man kann also auch von einer LLL-reduzierten positiv definiten symmetrischen Matrix bzw. quadratischen Form sprechen. Der Satz besagt dann, dass jede positiv definite quadratische Form (ganzzahlig) äquivalent zu einer LLL-reduzierten quadratischen Form ist.

Der folgende Satz faßt die wesentlichen Eigenschaften einer LLL-reduzierten Basis zusammen[6].

[6]Wir folgen der Darstellung im Buch *Computational Algebraic Number Theory* von Henri Cohen

Satz 3.3.4 *Es sei $b_1, ..., b_n$ eine LLL-reduzierte Basis des Gitters L. Dann gilt folgendes:*

(a) $\prod_{i=1}^{n} \|b_i\|^2 \leq 2^{n(n-1)/2} \det L$

(b) $\|b_1\|^2 \leq 2^{(n-1)/2} (\det L)^{1/n}$

(c) $\|b_1\|^2 \leq 2^{n-1} \cdot \min L$

Bevor wir den Satz beweisen, wollen wir seine verschiedenen Teilaussagen noch etwas erläutern, indem wir den Zusammenhang zu den Aussagen der klassischen Reduktionstheorie herstellen. Für (b) erinnern wir an die bekannten Abschätzungen von Minkowski und Hermite des Minimums durch die n-te Wurzel der Determinante. Dee Konstante $2^{(n-1)/2}$ ist hier noch schlechter als die Konstante $(4/3)^{(n-1)/2}$ von Hermite; der Vorteil ist wie gesagt, dass der Vektor b_1 mit „vertretbarem Aufwand“ gefunden werden kann, was für einen Minimalvektor in der Regel nicht gilt.

Die Aussage (c) gibt an, wie nahe die Länge des vom LLL gelieferten kurzen Vektors an das wirklich Minimum herankommt: immerhin bis auf einen Faktor, der nur von der Dimension abhängt. Für konkrete nicht zu große Dimensionen wie etwa bis 50 ist der Faktor 2^{n-1} in der Praxis viel zu pessimistisch. Der LLL-Algorithmus findet in interessierenden Fällen immer Vektoren, die nahe am wahren Minimum liegen. In höheren Dimensionen kann man solche Vergleichsrechnungen nicht mehr durchführen.

Die Abschätzung für die Größe $\prod_{i=1}^{n} \|b_i\|^2$ unter (a) liefert schließlich einen alternativen Beweis für die Existenz reduzierter Basen im allgemeinen Sinn (siehe 3.1.1), hier mit der relativ schlechten Konstanten $C_n = 2^{n(n-1)/2}$.

Wir weisen an dieser Stelle noch darauf hin, dass die umgekehrte Ungleichung

$$\det L \leq \prod_{i=1}^{n} \|b_i\|^2,$$

für jede Gitterbasis gilt. Der Beweis ergibt sich aus der Gleichheit

$$\det L = \prod_{i=1}^{n} \|b_i^*\|^2$$

Dieses sieht man wie folgt: die Übergangsmatrix zwischen den b_i und den b_i^* hat Determinante 1, d.h. die Determinante der Gram-Matrix ändert sich beim Übergang zu den b_i^* nicht, und die b_i^* liefern eine Diagonalmatrix. Ferner ist offenbar $\|b_i^*\| \leq \|b_i\|$. Wir erhalten einen (nicht wirklich) neuen Beweis der Hadamard-Ungleichung: Für jede positiv definite $n \times n$-Matrix A gilt $\det A \leq \prod_{i=1}^{n} a_{ii}$.

Beweis von Satz 3.3.4

zu (b): Auf Grund der beiden Bedingungen für eine LLL-reduzierte Basis haben wir für $1 \leq j \leq n-1$ die Ungleichungen

$$\|b_{j+1}^*\|^2 \geq (c - \mu_{j+1,j}^2)\|b_j^*\|^2 \geq \frac{1}{2}\|b_j^*\|^2$$

Durch vollständige Induktion über $j-i$, $1 \leq i < j$, folgt daraus $\|b_j^*\|^2 \geq 2^{i-j}\|b_i^*\|^2$, für $i = 1$ insbesondere $\|b_j^*\|^2 \geq 2^{1-j}\|b_1^*\|^2 = 2^{1-j}\|b_1\|^2$. Wir multiplizieren die beiden Seiten dieser Gleichungen für $j = 1, ..., n$ miteinander und erhalten insgesamt

$$\|b_1^*\|^2 \cdot ... \cdot \|b_n^*\|^2 \geq 2^{n-\sum_{j=1}^n j}\|b_1\|^{2n} = 2^{-\frac{1}{2}n(n-1)}\|b_1\|^{2n}$$

Der Wert auf der linken Seite ist gleich $(\det L)^{2n}$. Das Ziehen der n-ten Wurzel auf beiden Seiten liefert somit die Abschätzung (b).

zu (c): Die unter (b) gezeigte Ungleichung $\|b_j^*\|^2 \geq 2^{i-j}\|b_i^*\|$ liefert im Spezialfall $i = 1$ für $2 \leq j \leq n$ die Abschätzung $\|b_j^*\|^2 \geq 2^{1-n}\|b_1\|^2$ und somit $\min \|b_j^*\|^2 \geq 2^{1-n}\|b_1\|^2$. Auf Grund von Lemma 3.3.1 folgt daraus die Behauptung.

zu (a): Durch die Eigenschaft (i) einer LLL-reduzierten Basis und die Definition der Orthogonalvektoren b_i^* erhält man

$$\|b_j\|^2 = \sum_{i=1}^{j} \mu_{ji}^2\|b_i^*\|^2 \leq \|b_j^*\|^2 + \sum_{i=1}^{j-1} \frac{1}{4}\|b_i^*\|^2$$

Mit Hilfe der Ungleichung $\|b_j^*\|^2 \geq 2^{i-j}\|b_i^*\|^2$ ergibt sich daraus

$$\|b_j\|^2 \leq (1 + \sum_{i=1}^{j-1} \frac{1}{4} \cdot 2^{j-i})\|b_j^*\|^2 \leq 2^{j-1}\|b_j^*\|^2$$

Multipliziert man diese Ungleichungen für $j = 1, ..., n$ miteinander, so erhält man nach Ziehen der Quadratwurzel die gewünschte Abschätzung. □

Der LLL-Algorithmus

Bezeichnungen:

$c := \frac{3}{4}$
$B_i := \|b_i^*\|^2$
$\mu_{i,j} := \dfrac{\langle b_i, b_j^* \rangle}{\|b_j^*\|^2} = \dfrac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}$
$B_i \geq (c - \mu_{i,i-1}^2) B_{i-1}$ (LLL-Bedingung)

Algorithm 1 Hilfsfunktionen zum LLL-Algorithmus

procedure $Red(k, l)$
if $|\mu_{k,l}| > \frac{1}{2}$ **then**
  $q \leftarrow \lfloor \mu_{k,l} + \frac{1}{2} \rfloor$
  $b_k \leftarrow b_k - q b_l$
  $H_k \leftarrow H_k - q H_l$
  $\mu_{k,l} \leftarrow \mu_{k,l} - q$
  for $i = 1, ..., l-1$ **do**
    $\mu_{k,i} \leftarrow \mu_{k,i} - q\mu_{l,i}$
  end for
end if
end procedure

procedure $Swap(k)$ **{size of reduction of** b_k**}**
$b_k \leftrightarrow b_{k-1}$
$H_k \leftrightarrow H_{k-1}$
if $k > 2$ **then**
  for $j = 1, ..., k-2$ **do**
    $\mu_{k,j} \leftrightarrow \mu_{k-1,j}$
  end for
end if
$\mu \leftarrow \mu_{k,k-1}$
$B \leftarrow B_k + \mu^2 B_{k-1}$
$\mu_{k,k-1} \leftarrow \mu \frac{B_{k-1}}{B}$
$B_k \leftarrow (B_{k-1} B_k)/B$
$B_{k-1} \leftarrow B$
for $i = k+1, k+2, ..., k_{max}$ **do**
  $t \leftarrow \mu_{i,k}$
  $\mu_{i,k} \leftarrow \mu_{i,k-1} - \mu t$
  $\mu_{i,k-1} \leftarrow t + \mu_{k,k-1}\mu_{i,k}$
end for
end procedure

Algorithm 2 LLL-Algorithmus

$c := \frac{3}{4}$
$B_i := \|b_i^*\|^2$
$B_i \geq (c - \mu_{i,i-1}^2) B_{i-1}$
$\mu_{i,j} := \dfrac{\langle b_i, b_j^* \rangle}{\|b_j^*\|^2} = \dfrac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}$
procedure LLL
$k \leftarrow 2$ $\quad //* \ 1.\ Initialize\ *//$
$k_{max} \leftarrow 1$
$b_1^* = b_1$
$B_1 = \langle b_1, b_1 \rangle$
$H \leftarrow I_n$
$\quad //* \ 2.\ GramSchmidt\ *//$
if $k \leq k_{max}$ **then**
  goto 3
else
  $k_{max} \leftarrow k$
  $b_k^* \leftarrow b_k$
  for $j = 1, ..., k-1$ **do**
    $\mu_{k,j} \leftarrow \dfrac{\langle b_k, b_j^* \rangle}{B_j}$
    $b_k^* \leftarrow b_k^* - \mu_{k,j} b_j^*$
  end for
  $B_k \leftarrow \langle b_k^*, b_k^* \rangle$
  if $B_k = 0$ **then**
    error
  end if
end if
$Red(k, k-1)$ $\quad //* \ 3.\ Test\ LLL\ condition\ *//$
if $B_k < (c - \mu_{k,k-1}^2) B_{k-1}$ **then**
  $Swap(k)$
  $k \leftarrow \max(2, k-1)$
  goto 3
else
  for $l = k-2, k-3, ..., 1$ **do**
    $Red(k, l)$
    $k \leftarrow k+1$
  end for
end if
if $k \leq n$ **then**
  goto 2
else
  output $b_1^*, ..., b_n^*, H$
end if
end procedure