Seminar: Wie genau ist ungefähr

Vortrag 20:
Kurze Vektoren in Gittern

Kerstin Bauer

Sommerakademie Görlitz, 2007

Definition und Problembeschreibung

Definition: **Gitter**

Seien $b_1,\ldots,b_k \in Q^n$. Dann heißt die Menge aller ganzzahligen Linearkombinationen

$$L = \{\lambda_1 b_1 + \ldots + \lambda_k b_k \mid \lambda_i \in IN\}$$

das durch die Vektoren $b_1,\ldots,b_k$ erzeugte **Gitter**.

Die **Länge eines Vektors** ist durch dessen euklidische Norm gegeben.

Problembeschreibung:

Finde einen kürzesten Vektor in einem gegebenen Gitter

Anwendung:

Algebraische Zahlentheorie

Beispiel:

$Q^n = Q$, $b_1 = 8$, $b_2 = 10$, $L = \{8\lambda_1 + 10\lambda_2 \mid \lambda_i \in IN\}$

$\Rightarrow$ $2 = 1*10 - 1*8$ ist auch ein Vektor des Gitters und

damit: $L = \{2\lambda \mid \lambda \in IN\}$

2 und -2 sind die kürzesten Vektoren in L.

Bemerkungen:

- Im Weiteren haben alle Gitter vollen Rang, d.h. sie spannen den kompletten Raum Q^n auf.
- Die Berechnung eines kürzesten Vektoren ist NP-hart, allerdings existieren polynomielle Algorithmen, die einen „relativ kurzen“ Vektor bestimmen, dessen Länge um maximal einen nur von der Dimension, nicht vom Gitter abhängigen Vorfaktor abweicht.

Notation:

- B sei die durch die Zeilenvektoren $b_1,.., b_n$ aufgespannte Matrix
- Vektoren $a_1,.., a_n$ bilden eine Basis eines Gitters L, wenn sie das Gitter L aufspannen
- Quadratische Matrizen mit ganzzahligen Einträgen und Determinante ± 1 heißen **unimodular**

Basen, Determinanten und Orthogonalitätsdefekt

Sei im Weiteren $b_1,.., b_n$ immer eine Basis von L.

Satz:

Gegeben seinen $a_1,.., a_n \in L$. Dann sind äquivalent:

1. $a_1,.., a_n$ bilden eine Basis von L
2. $|\det(B)| = |\det(A)|$
3. Es gibt eine unimodulare n x n Matrix U mit A = UB

Beweis:

$1 \Rightarrow 2$: $b_1,.., b_n$ sind Basis von L

$\Rightarrow a_1, \ldots, a_n$ sind ganzz. Linearkombinationen der b_i

$\Rightarrow A = \Lambda_B B$ mit Λ ganzzahlig

$\Rightarrow \det(A) = k_B * \det B$ mit k_B ganzzahlig

Analog: $\det(B) = k_A * \det A$

$\Rightarrow |\det(B)| = |\det(A)|$

$2 \Rightarrow 3$: Wegen $|\det(B)| = |\det(A)|$ ist $|\det \Lambda_A| = 1$ und damit Λ_A unimodular

$3 \Rightarrow 1$: Da U unimodular ist, ist auch U^{-1} unimodular

$\Rightarrow B = U^{-1} A$ mit U^{-1} unimodular

$\Rightarrow$ Die Vektoren b_i sind ganzzahlige LK der a_i

$\Rightarrow a_1,\ldots, a_n$ bilden eine Basis von L

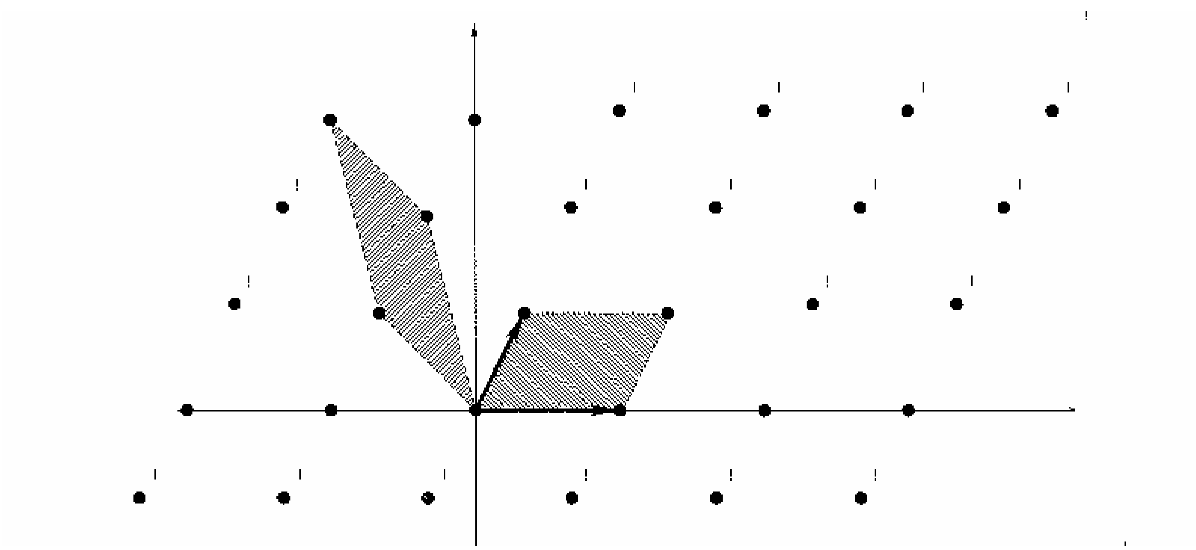
Folgerung:

Die Determinante eines Gitters ist bis auf Vorzeichen eindeutig bestimmt und wird mit det L bezeichnet.

Geometrische Interpretation:

|det L| gibt das Volumen des durch $b_1,\ldots,b_n$ aufgespannten Parallelepipeds an.

Beispiel:



Bemerkungen:

- Orthogonale Basen beinhalten einen kürzesten Vektor
- Hadamards Ungleichung: $|\det B| \leq ||b_1||\ldots||b_n||$

  und Gleichheit, wenn die a_i orthogonal sind

  $\Rightarrow$ $|\det L| \leq ||b_1||\ldots||b_n||$,

  Gleichheit bei orthogonalen Vektoren

  $\frac{||b_1||\ldots||b_n||}{\det L}$ wird **Orthogonalitätsdefekt** der Basis $b_1,\ldots,b_n$ genannt. Je kleiner der Defekt, desto kürzer sind die Vektoren.

Definition: **primitive Vektoren**

Linear unabhängige Vektoren $b_1,\ldots,b_k$ heißen **primitiv**, wenn sie sich zu einer Basis von L ergänzen lassen.

Satz:

Ein Vektor a ist primitiv, wenn er in seiner Richtung am kürzesten ist.

Kürzeste Vektoren in zweidimensionalen Gittern

Idee:

Wie im euklidischen Algorithmus zur Bestimmung des ggT schrittweises Ersetzen der Basis durch eine Basis mit kürzeren Vektoren.

Bezeichnung:

θ sei der Winkel zwischen den Basisvektoren b_1 und b_2.

Satz:

Ist $60° \leq \theta \leq 120°$, dann ist b_1 ein kürzester Vektor von L.

Beweis:

Annahme: Es gibt einen noch kürzeren Vektor b.

b_1 und b_2 sind primitiv

$\Rightarrow$ b ist nicht von b_1 oder b_2 linear abhängig

$\Rightarrow$ Fallunterscheidung:

b bildet entweder mit b_1, b_2, $-b_1$ oder $-b_2$ einen Winkel von maximal $60°$

Sei D die durch b und diesen Vektor gebildete 2×2 Matrix.

$\Rightarrow$ $|\det D| < ||b_1||\ ||b_2|| \sin\theta = \det L$

$\Rightarrow$ Widerspruch zu $|\det D| = k\cdot\det L$ mit $k \in \mathbb{Z}$.

Bezeichnung: $\mu_{21} = \frac{b_2 \cdot b_1}{||b_1||^2}$

(dabei ist μ_{21} b_1 die Komponente von b_2 die in Richtung von b_1 zeigt)

Proposition 1:

Erfüllt eine Basis

- $||b_1|| \leq ||b_2||$
- $|\mu_{21}| \leq ½$

dann ist b_1 ein kürzester Vektor von L.

Beweis:

Es gilt: $\cos\theta = \frac{b_2 \cdot b_1}{||b_2|| \cdot ||b_1||} = \frac{\mu_{21} \cdot ||b_1||}{||b_2||}$

Also ist $\cos\theta \leq ½$ und damit $60° \leq \theta \leq 120°$

Algorithmus 1: kürzester Vektor in Dimension 2

1. Initialisierung: o.B.d.A $\|b_1\| \leq \|b_2\|$
2. **While** (Bed von Prop. 1 nicht erfüllt)

   a) **If** $|\mu_{21}| > ½$ Then

   $b_2 = b_2 - mb_1$ mit $m = \text{round}(\mu_{21})$

   b) **If** $\|b_1\| > \|b_2\|$

   Tausche b_1 und b_2
3. **Return** b_1

- Korrektheit:

  Nach Schritt 2a) ist immer die erste Bedingung von Proposition 1 erfüllt.

  Ist die Bedingung von Schritt 2b) erfüllt, so sind alle Bedingungen von Proposition 1 erfüllt, also ist die Ausgabe korrekt.
- Termination

  $\|b_1\|\cdot\|b_2\|$ wird in jedem Schritt kleiner. Da es nur eine endliche Menge an Gittervektoren innerhalb eines gegebenen Radius gibt, terminiert der Algorithmus.

Kürzeste Vektoren in n-dimensionalen Gittern

Für den Algorithmus wird das Gram-Schmidt-Orthogonalisierungsverfahren benötigt.

<u>Theorem:</u> **Gram–Schmidt–Orthogonalisierung**

Seien $x_1,\dots,x_n \in IR^n$ linear unabhängig. Definiere rekursiv:

- $x_1^* = x_1$
- $x_i^* = x_i - \sum_{j=1}^{i-1} \mu_{ij} x_j^*$ mit $\mu_{ij} := \dfrac{x_i \cdot x_j^*}{x_j^* \cdot x_j^*}$
- $M := (\mu'_{ij})$ mit $\mu'_{ij} = \begin{cases} 1 & j = i \\ 0 & j > i \\ -\mu_{ij} & j < i \end{cases}$

Dann gilt:

a) $x_i^* \neq 0$, $x_i^* x_j^* = 0$ für $i \neq j$, $<x_1,\dots,x_n> = <x_1^*,\dots,x_n^*>$

b) x_i^* ist die Projektion von x_i auf $<x_1,\dots,x_{i-1}>^\perp$

c) $(x_1^*,\dots,x_n^*) = (x_1,\dots,x_n) * M$

Bezeichnungen / Feststellungen:

- Mit $\mu_{ii} = 1$ folgt damit für eine Basis: $b_i = \sum_{j=1}^{i} \mu_{ij} b_j^*$
- Für $j < i$: $b_i(j) := \mu_{ij} b_j^* + \mu_{i,j+1} b_{j+1}^* + \ldots + b_i^*$
- OPT := Länge des kürzesten Vektores eines Gitters L

Lemma:

Sei $b_1,\ldots,b_n$ eine Basis des Gitters L und $b_1^*,\ldots,b_n^*$ die Gram-Schmidt-Orthogonalisierung der Basis. Dann gilt:

$OPT \geq \min\{||b_1^*||, \ldots, ||b_n^*||\}$

Beweis:

Sei $v = \sum_{i=1}^{k} \lambda_i b_i$ ein kürzester Vektor von L, wobei k der größte Index mit $\lambda_k \neq 0$.

Dann ist mit $b_i = \sum_{j=1}^{i} \mu_{ij} b_j^*$ und $\mu_{ii} = 1$:

$$v = \sum_{i=1}^{k} \lambda_i^* b_i^* \quad \text{mit} \quad \lambda_k^* = \lambda_k$$

Da $b_1^*,\ldots,b_n^*$ orthogonal sind und λ_k ganzzahlig, folgt also

$$OPT^2 = ||v||^2 \geq \lambda_k^2\, ||b_k^*||^2 \geq ||b_k^*||^2$$

Damit:

$$OPT \geq \min\{||b_1^*||^2, \ldots, ||b_n^*||^2$$

Definition:

Eine Basis $b_1,\ldots,b_n$ eines Gitters L heißt Gauß-reduziert, wenn gilt:

- $\|b_i(i)\| \leq \frac{2}{\sqrt{3}} \|b_{i+1}(i)\|$
- $|\mu_{i+1,i}| \leq ½$

Algorithmus 2: kürzester Vektor in Dimension n

1. **While** ($b_1,\ldots,b_n$ nicht Gauß-reduziert)

    For i = 1 to n do

    If $|\mu_{i+1,i}| > ½$ Then

    $b_{i+1} = b_{i+1} - mb_i$ mit $m = \mathrm{round}(\mu_{i+1,i})$

    Wähle i beliebig mit $\|b_i\| > \frac{2}{\sqrt{3}} \|b_{i+1}\|$ und

    vertausche b_i und b_{i+1}

2. **Return** b_1

Theorem:

Algorithmus 2 terminiert nach einer polynomialen Anzahl von Iterationen. Die Approximationsgüte beträgt $2^{(n-1)/2}$

Bemerkung:

- Eigentlich müsste gezeigt werden, dass die Zahl der Bit-Operationen polynomial beschränkt ist und nicht nur die Zahl der arithmetischen Operationen.
- Eine einfache Erweiterung von Algorithmus 2, die Lovász-reduzierte Basen benutzt, erfüllt diese Bedingung.

Definition:

Eine Basis $b_1,\ldots, b_n$ des Gitters L ist Lovász-reduziert, wenn gilt:

- $b_1,\ldots, b_n$ ist Gauß-reduziert
- Für $1 \leq j < i \leq n$: $|\mu_{ij}| \leq ½$

Satz:

Der Orthogonalitätsdefekt einer Lovász-reduzierten Basis ist durch $2^{n(n-1)4}$ beschränkt.