Technische Universität München
Zentrum Mathematik
Prof. Dr. P. Gritzmann, Dipl.-Inf. Dipl.-Math. S. Borgwardt, Dr. M. Ritter

Optimierung 2, WS 2008/09

Übungsblatt 13

Aufgabe 13.1
Betrachten Sie das folgende Problem:

Problem (Gitterbasis-Transformation)
Gegeben: $v_1, ..., v_n \in \mathbb{Z}^m$

Auftrag: *Bestimme eine Basis* $b_1, ..., b_k$ *von* $L := \{\sum_{j=1}^{n} \lambda_j v_j : \lambda_1, ..., \lambda_n \in \mathbb{Z}\}$ *mit* $u_i^T b_j = 0$ *für alle* $i \in \{1, ..., m\}, j \in \{1, ..., k\}$ *mit* $i < j$.

a) Erklären Sie detailliert, wie Sie eine Instanz von Gitterbasis-Transformation lösen können.

b) Zeigen Sie: Gitterbasis-Transformation kann in polynomieller Zeit gelöst werden.

c) Seien $v_1 = (1, 0, 1, 2)^T$,$v_2 = (2, 2, 3, -1)^T$,$v_3 = (3, 2, 4, 1)^T$,$v_4 = (2, -1, 4, 0)^T$. Lösen Sie Gitterbasis-Transformation für den Input v_1, v_2, v_3, v_4.

d) Zeigen Sie:

Seien L ein Gitter des $\mathbb{R}^n$, sowie $v_1, ..., v_n$ und $w_1, ..., w_n$ zwei Basen von L. Dann ist

$$|det(v_1, ..., v_n)| = |det(w_1, ..., w_n)|$$

Die von der Wahl der Basis demnach unabhängige Größe $|det(v_1, ..., v_n)|$ heißt *Determinante* von L (oder wenn der Bezug zu L klar ist, *Gitterdeterminante*).

e) Seien $v_1, ..., v_n$ bzw. $w_1, ..., w_n$ Basen für Gitter L_v bzw. L_w mit $|det(v_1, ..., v_n)| = |det(w_1, ..., w_n)|$. Gilt dann $L_v = L_w$? Begründen Sie Ihre Antwort.

Lösung zu Aufgabe 13.1

a) Wir gehen analog zum Beweis von Korollar 7.1.24 vor, um $b_1, ..., b_k$ zu bestimmen.

Zunächst bestimmen wir den Rang k der Matrix $A' = (v_1, ..., v_n)$ und permutieren die Spalten von A' so, dass die ersten k Spalten bereits Rang k haben. Es ergibt sich eine Matrix $A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}$ mit $A_1 \in \mathbb{Z}^{k \times k}$, $A_2 \in \mathbb{Z}^{k \times (n-k)}$, $A_3 \in \mathbb{Z}^{(m-k) \times k}$, $A_4 \in \mathbb{Z}^{(m-k) \times (n-k)}$ und $rg(A_1) = k$.

Nun bestimmen wir eine unimodulare Matrix C, so dass $(A_1 A_2)C = B_1$ Hermite Normalform hat. Dann bekommen wir unsere neue Basis als die Nicht-0-Spalten von $AC = \begin{pmatrix} B_1 & 0 \\ B_3 & 0 \end{pmatrix}$. (Vgl. Korollar 7.1.24.)

Der Hauptteil der Arbeit besteht dabei in der Berechnung von C. Wir überführen $(A_1 A_2)$ zeilenweise in Hermite Normalform durch elementare Spaltenoperationen. Diese lassen sich als unimodulare Matrizen schreiben, deren Hintereinanderausführung (Matrixprodukt) am Ende C ergibt.

Um die i-te Zeile in die richtige Form zu bringen (in der Matrix, in der die ersten $i-1$ Zeilen bereits Hermite Normalform haben), führen wir eine ggT-Berechnung der Elemente mit Indizes i bis n dieser Zeile durch (vgl. Korollar 7.1.18, Satz 7.1.20), nachdem durch etwaige Multiplikation von Spalten mit -1 diese Elemente alle positiv gemacht wurden. Dann vertauschen wir die Spalte mit dem ggT mit der i-ten Spalte, wodurch das Diagonalelement $\beta_{i,i}$ der aktuellen Matrix dem ggT entspricht. Die Elemente mit Index $j < i$ der Zeile werden jetzt noch durch geeignetes Addieren der i-ten Spalte auf die j-te Spalte ins Intervall $[0, \beta_{i,i}[$ gebracht. (Vgl. Satz 7.1.20a).)

Man beachte, dass einige der durchgeführten Operationen für die Lösung von GITTERBASIS-TRANSFORMATION redundant sind, wie z.B. das Multiplizieren von Spalten mit -1 zum Erhalten positiver Einträge und das "Korrigieren" der Einträge vor den Diagonalelementen.

b) Das in a) beschriebene Vorgehen lässt sich nach Satz 7.1.34 in polynomieller Zeit durchführen:

Die Bestimung des Rangs k einer Matrix und dazugehöriger k Spalten ist mit Gauß-Elimination in polynomieller Zeit möglich.

Die Berechnung der Hermiten Normalform von $(A_1 A_2)$ und der zugehörigen unimodularen Matrix ist ebenso in polynomieller Zeit möglich. (Vgl. 7.1.31, 7.1.33.)

Alle weiteren Operationen sind trivialerweise in polynomieller Zeit möglich.

c) Wir lösen das Problem analog zur Beschreibung in Teilaufgabe a). Die Matrix der v_i ist

$$A' = \begin{pmatrix} 1 & 2 & 3 & 2 \\ 0 & 2 & 2 & -1 \\ 1 & 3 & 4 & 4 \\ 2 & -1 & 1 & 0 \end{pmatrix}$$

$rg(A') = 3$, da $v_3 = v_1 + v_2$ und v_1, v_2, v_4 linear unabhängig sind. Wir vertauschen die 4. Spalte mit der 3. Spalte und erhalten eine Matrix A mit

$$(A_1 A_2) = \begin{pmatrix} 1 & 2 & 2 & 3 \\ 0 & 2 & -1 & 2 \\ 1 & 3 & 4 & 4 \end{pmatrix}$$

Diese Matrix überführen wir nun zeilenweise in Hermite Normalform. (j) bezeichne im Folgenden die jeweils aktuelle j-te Spalte.

Zeile 1: Als Operationen benutzen wir (2) := (2) − 2(1), (3) := (3) − 2(1), (4) := (4) − 3(1). Das ergibt die unimodulare Matrix

$$C_1 = \begin{pmatrix} 1 & -2 & -2 & -3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

und

$$(A_1A_2)_1 = (A_1A_2)C_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & -1 & 2 \\ 1 & 1 & 2 & 1 \end{pmatrix}$$

Zeile 2: Als Operationen benutzen wir (in dieser Reihenfolge) (3) := $-1 \cdot (3)$, (2) := (2) − 2(3), (4) := (4) − 2(3) und das Vertauschen von (2) und (3). Das ergibt die unimodulare Matrix

$$C_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 2 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

und

$$(A_1A_2)_2 = (A_1A_2)_1C_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & -2 & 5 & 5 \end{pmatrix}$$

Die Zeile erfüllt die Eigenschaften der Hermiten Normalform.

Zeile 3: Als Operationen benutzen wir (in dieser Reihenfolge) (4) := (4) − (3), und danach, damit das Element mit Index $(3, 2)$ zwischen 0 und dem ggT der Restzeile liegt, (2) := (2) + (3). Das ergibt die unimodulare Matrix

$$C_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

und

$$(A_1A_2)_3 = (A_1A_2)_2C_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 3 & 5 & 0 \end{pmatrix}$$

$(A_1A_2)_3$ ist nun in Hermiter Normalform.

Wir erhalten $(A_1A_2)C = (A_1A_2)_3$ für

$$C = C_1 \cdot C_2 \cdot C_3 = \begin{pmatrix} 1 & -4 & -6 & -1 \\ 0 & 1 & 1 & -1 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Insgesamt gilt nun

$$AC = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 3 & 5 & 0 \\ 2 & -9 & -13 & 0 \end{pmatrix}$$

und wir bekommen unsere neue Basis als $b_1 = (1, 0, 1, 2)^T$, $b_2 = (0, 1, 3, -9)^T$ und $b_3 = (0, 1, 5, -13)^T$.

d) Nach 7.1.12 bilden die unimodulare Transformationen einen Gruppenautomorphismus von $(\mathbb{Z}^n, +)$. Damit gilt die Behauptung für das Standardgitter, denn es gibt eine unimodulare Matrix, die die eine Basis in die andere überführt, und (als unimodulare Matrix) natürlich den Betrag der Determinante der Basisvektoren gleich lässt. Nach Bemerkung 7.1.3 gilt die Behauptung auch für allgemeine Gitter.

e) Die Aussage ist falsch, wir geben ein einfaches Gegenbeispiel an:

$v_1 = (1, 2)^T$, $v_2 = (2, 1)^T$, damit ist $det(v_1, v_2) = -3$. $w_1 = (-3, 0)^T$, $w_2 = (0, 1)^T$, damit ist auch $det(w_1, w_2) = -3$.

Durch diese Basen entstehen unterschiedliche Gitter: Vgl. Bsp. 7.1.2 für das Gitter von v_1 und v_2. Dieses enthält den Punkt $(-3, 1)^T$ nicht, da $-3+1 = -2$ nicht durch 3 teilbar ist. Trivialerweise liegt dieser Punkt aber im Gitter von w_1 und w_2.

Aufgabe 13.2 *Hausaufgabe*
Betrachten Sie das diophantische Gleichungssystem

$$Ax = b, \qquad A = \begin{pmatrix} 4 & 2 & 2 & 2 \\ 1 & 3 & 4 & 5 \end{pmatrix}, b = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}, b_1, b_2 \in \mathbb{Z}, x \in \mathbb{Z}^4$$

Bestimmen Sie - analog zur Vorlesung - alle Vektoren b, für die das Gleichungssystem eine ganzzahlige Lösung x hat. Berechnen Sie für beliebiges (zulässiges), aber festes b die Menge $\{x \in \mathbb{Z}^4 : Ax = b\}$.

Lösung zu Aufgabe 13.2
Trivialerweise existiert ein $b \in \mathbb{Z}^2$, so dass das Gleichungssystem lösbar ist. Um herauszufinden, wie ein solches b aussehen muss, bestimmen wir zunächst die Hermite Normalform von A und die zugehörige unimodulare Transformationsmatrix C. (j) bezeichne im Folgenden die jeweils aktuelle j-te Spalte.

Zeile 1: Als Operationen benutzen wir (in dieser Reihenfolge) $(1) := (1) - 2(2)$, $(3) := (3) - 1(2)$, $(4) := (4) - 1(2)$ und das Vertauschen von Spalte (1) und (2). Das ergibt die unimodulare Matrix

$$C_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & -2 & -1 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Wir erhalten

$$A' = AC_1 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 3 & -5 & 1 & 2 \end{pmatrix}$$

Zeile 2: Als Operationen benutzen wir (in dieser Reihenfolge) $(2) := -1 \cdot (2)$, $(2) := (2) - 5(3)$, $(4) := (4) - 2(3)$, das Vertauschen von Spalte (2) und (3) und $(1) := (1) - 3(2)$. Das ergibt die unimodulare Matrix

$$C_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -5 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ -3 & 1 & -5 & -2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Wir erhalten die Hermite Normalform als

$$A'' = A'C_2 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

und bekommen unsere Transformationsmatrix C als

$$C = C_1 \cdot C_2 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 4 & -1 & 7 & 1 \\ -3 & 1 & -5 & -2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Das Gleichungssystem ist genau dann ganzzahlig lösbar, wenn

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-1} b = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix} b = \begin{pmatrix} \frac{1}{2}b_1 \\ b_2 \end{pmatrix} \in \mathbb{Z}^2$$

Das ist genau der Fall für gerade b_1 und beliebige b_2.

Seien nun b_1,b_2 beliebig, aber fest, mit b_1 gerade. Sei $y = \begin{pmatrix} \frac{1}{2}b_1 \\ b_2 \\ 0 \\ 0 \end{pmatrix}$. Dann ist

$$Cy = \begin{pmatrix} 0 \\ 2b_1 - b_2 \\ -\frac{3}{2}b_1 + b_2 \\ 0 \end{pmatrix}$$

und

$$Cu_3 = \begin{pmatrix} -1 \\ 7 \\ -5 \\ 0 \end{pmatrix}, \quad Cu_4 = \begin{pmatrix} 0 \\ 1 \\ -2 \\ 1 \end{pmatrix}$$

Aus dem (konstruktiven) Beweis von 7.1.34 wissen wir, dass dann

$$\{x \in \mathbb{Z}^4 : Ax = b\} = \begin{pmatrix} 0 \\ 2b_1 - b_2 \\ -\frac{3}{2}b_1 + b_2 \\ 0 \end{pmatrix} + \lambda_3 \begin{pmatrix} -1 \\ 7 \\ -5 \\ 0 \end{pmatrix} + \lambda_4 \begin{pmatrix} 0 \\ 1 \\ -2 \\ 1 \end{pmatrix}$$

für $\lambda_3, \lambda_4 \in \mathbb{Z}$.