Prof. C. P. Schnorr Sommersemester 2006

Diskrete Mathematik

Blatt 2, 28.04.2006, Abgabe 05.05.2006

Aufgabe 1. **4 P.** Seien $\mathbf{b}_1, \mathbf{b}_2 \in \mathbf{R}^n$ linear unabhängig. Zeige

a) $\langle \mathbf{b}_1 - \mathbf{b}_2 \langle \mathbf{b}_1, \mathbf{b}_2 \rangle / \langle \mathbf{b}_2, \mathbf{b}_2 \rangle \mathbf{b}_2, \mathbf{b}_2 \rangle = 0$,

b) $\mathbf{b}_1 - q\,\mathbf{b}_2$ ist Vektor minimaler Länge in $\mathbf{b}_1 + \mathbf{b}_2\mathbf{Z}$ gdw
$|q - \langle \mathbf{b}_1, \mathbf{b}_2 \rangle / \langle \mathbf{b}_2, \mathbf{b}_2 \rangle|$ minimal ist für $q \in \mathbf{Z}$.

Aufgabe 2. **5 P.** Zeige:

Die Ausgabebasis des Reduktionsalgorithmus ist reduziert.

Aufgabe 3. **5 P.** Zeige: jede reduzierte Basis $\mathbf{b}_1, \mathbf{b}_2$ erfüllt

$$\|\mathbf{b}_1\|^2 \leq \sqrt{\tfrac{4}{3}} \det L(\mathbf{b}_1, \mathbf{b}_2).$$

Hinweis: $\det L(\mathbf{b}_1, \mathbf{b}_2) = \|\mathbf{b}_1\| \; \|\mathbf{b}_2 - \langle \mathbf{b}_1, \mathbf{b}_2 \rangle / \langle \mathbf{b}_1, \mathbf{b}_1 \rangle \mathbf{b}_1\|$.

Aufgabe 4. **8 P.** Sei K ein Körper. Zeige

a) durch vollständige Induktion nach grad g: zu $g, h \in K[x] \setminus \{0\}$ gibt es $r, s \in K[x]$, so dass $g = s \cdot h + r$ und grad $r <$ grad h,

b) die Zerlegung $g = s \cdot h + r$ aus a) ist eindeutig,

c) $K[x]$ ist ein Euklidischer Ring,

d) Bestimme den ggT von $x^4 + x^3 + x^2 + 1$ und $x^3 + x^2 + x + 1$ in $\mathbf{Z}_2[x]$.

Algorithmus zur Reduktion von Gitterbasen der Dim. 2.

`EINGABE` $\mathbf{x}, \mathbf{y} \in \mathbf{Z}^n$ lin. unabh. $\|\mathbf{x}\| \geq \|\mathbf{y}\|$

1. $\mathbf{b}_1 := \mathbf{x},\ \mathbf{b}_2 := \mathbf{y}$ ($\mathbf{b}_1, \mathbf{b}_2$ seien Zeilenvektoren)
2. $\begin{bmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{bmatrix} := \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix} \begin{bmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{bmatrix}$ $\left(\text{d.h. } \begin{array}{lcl} \mathbf{b}_1^{\text{neu}} & := & \mathbf{b}_2 \\ \mathbf{b}_2^{\text{neu}} & := & \mathbf{b}_1 - q\mathbf{b}_2 \end{array}\right)$

   mit $q := \lceil \langle \mathbf{b}_1, \mathbf{b}_2 \rangle / \langle \mathbf{b}_2, \mathbf{b}_2 \rangle \rfloor$

   ($\mathbf{b}_2^{\text{neu}}$ hat minimale Länge unter den Vektoren in $\mathbf{b}_1 + \mathbf{b}_2\mathbf{Z}$.)
3. `IF` $\|\mathbf{b}_1\| > \|\mathbf{b}_2\|$ `THEN GO TO 2`

`AUSGABE` reduzierte Basis $\mathbf{b}_1, \mathbf{b}_2$.

Der Reduktionsalgorithmus ist analog zum zentrierten Eukl. Alg.
Es wird der längere Vektor $\mathbf{b}_1$ reduziert zu $\mathbf{b}_2^{\text{neu}} := \mathbf{b}_1 - q\mathbf{b}_2$. Die Iteration

$$\begin{bmatrix} a_0 \\ a_1 \end{bmatrix} := \begin{bmatrix} 0 & 1 \\ 1 & -\lceil a_0/a_1 \rfloor \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}.$$

des zentrierten Eukl. Alg. dividiert die grössere Zahl a_0 durch die kleinere a_1 und bildet den Rest $a_1^{\text{neu}} := a_0 - \lceil a_0/a_1 \rfloor a_1$.

Der Ausgabevektor $\mathbf{b}_1$ ist minimal in $\mathbf{xZ} + \mathbf{yZ} \setminus 0$.
ggT(m, n) ist minimal in $m\mathbf{Z} + n\mathbf{Z} \setminus 0$.

Definition Die Basis $\mathbf{b}_1, \mathbf{b}_2 \in \mathbf{R}^n$ ist *reduziert*, wenn

1. $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$
2. $|\langle \mathbf{b}_1, \mathbf{b}_2 \rangle / \langle \mathbf{b}_1 \mathbf{b}_1 \rangle| \leq 1/2$.