Wolfgang K. Seiler
Tel. 2515

B6, B4.08

15. November 2025

11. Übungsblatt Computeralgebra

Aufgabe 1:

a) Zeigen Sie, daß die Vektoren

$$v_1 = \begin{pmatrix} 1\\1\\1\\1 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 1\\1\\-1\\-1 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 1\\-1\\1\\-1 \end{pmatrix} \quad \text{und} \quad v_4 = \begin{pmatrix} -1\\1\\1\\-1 \end{pmatrix}$$

eine Orthogonalbasis des $\mathbb{R}^4$ bilden!

b) Wenden sie den LLL-Algorithmus an auf das Gitter $\Gamma = \mathbb{Z}b_1 + \mathbb{Z}b_2 \oplus \mathbb{Z}b_3 \oplus \mathbb{Z}b_4$ mit $b_1 = 5v_1$, $b_2 = 3v_2$, $b_3 = 2v_3$ und $b_4 = v_4$!

c) Wenden sie den LLL-Algorithmus an auf das Gitter $\Gamma = \mathbb{Z}b_1 + \mathbb{Z}b_2 \oplus \mathbb{Z}b_3 \oplus \mathbb{Z}b_4$ mit $b_1 = 10v_4$, $b_2 = 9v_3$, $b_3 = 8v_2$ und $b_4 = 7v_1$!

d) Allgemein sei Γ ein Gitter mit einer Basis $(b_1, \dots, b_n)$, die eine Orthogonalbasis von $\mathbb{R}^n$ ist. Was macht der LLL-Algorithmus mit einem solchen Gitter?

e) Der LLL-Algorithmus funktioniert auch, wenn man in der Lovász-Bedingung der Faktor $\frac{3}{4}$ durch irgendeine Zahl größer $\frac{1}{4}$ und kleiner 1 ersetzt. Welche Auswirkung hätte das auf die Antwort zur vorigen Frage?

Aufgabe 2:

a) Das Untergitter Γ von $\mathbb{Z}^2$ wird aufgespannt von den Vektoren $\binom{28}{6}$ und $\binom{13}{3}$. Wenden Sie den LLL-Algorithmus darauf an!

b) Zeigen Sie mit Hilfe der Längenabschätzungen für die Vektoren einer LLL-reduzierten Basis, daß der LLL-Algorithmus für jede Ausgangsbasis dieses Gitters als ersten Basisvektor des Ergebnisses einen der beiden Vektoren $\binom{\pm 2}{0}$ liefert.

c) Welche Möglichkeiten gibt es für den zweiten Vektor?

Aufgabe 3:

x sei eine beliebige reelle Zahl und M eine große natürliche Zahl. Die Vektoren $b_i \in \mathbb{R}^{n+2}$ für $i = 0, \dots, n$ haben jeweils die $(i+1)$-te Komponente eins und die $(n+2)$-te Komponente Mx^{i-1}; alle anderen Komponenten sind Null. Der von diesen Vektoren aufgespannte Untervektorraum V wird mit $\mathbb{R}^{n+1}$ identifiziert, und wir betrachten darin das von $b_0, \dots, b_n$ erzeugte Gitter Γ. Welche Bedingung müssen $a_0, \dots, a_n \in \mathbb{Z}$ erfüllen, damit $a_0b_0 + \cdots + a_nb_n$ ein (bezüglich des Standardskalarprodukts von $\mathbb{R}^{n+2}$) „kurzer" Vektor ist, und welche Rolle spielt hierbei die Zahl M ?

Abgabe bis zum Mittwoch, dem 19. November 2025, um 15.30 Uhr