Discrete Optimization (MA 3502)

Prof. Dr. P. Gritzmann | Dipl.-Math. Viviana Ghiglione | Dr. M. Ritter

Exercise Sheet 3

Exercise 3.1 [6 credits]

Determine the complete set of integral solutions of the following diophantine equation system:

$$\begin{pmatrix} 6 & -6 & 9 \\ 3 & 2 & 2 \end{pmatrix} x = \begin{pmatrix} -3 \\ 6 \end{pmatrix}$$

Answer to Exercise 3.1

we start by computing the Hermite Normal Form of the given matrix A together with a unimodular transformation by performing elementary column operations:

$$\begin{pmatrix} 6 & -6 & 9 \\ 3 & 2 & 2 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{S_2+S_1, S_3-S_1} \begin{pmatrix} 6 & 0 & 3 \\ 3 & 5 & -1 \\ \hline 1 & 1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{S_1-2S_3, S_1 \leftrightarrow S_3} \begin{pmatrix} 3 & 0 & 0 \\ -1 & 5 & 5 \\ \hline -1 & 1 & 3 \\ 0 & 1 & 0 \\ 1 & 0 & -2 \end{pmatrix} \xrightarrow{S_1+S_2, S_3-S_2} \begin{pmatrix} 3 & 0 & 0 \\ 4 & 5 & 0 \\ \hline 0 & 1 & 2 \\ 1 & 1 & -1 \\ 1 & 0 & -2 \end{pmatrix}$$

With this we get $AC = H$ with

$$C := \begin{pmatrix} 0 & 1 & 2 \\ 1 & 1 & -1 \\ 1 & 0 & -2 \end{pmatrix}, \quad H := \begin{pmatrix} 3 & 0 & 0 \\ 4 & 5 & 0 \end{pmatrix}.$$

To solve the equation system $Ax = b$, we first consider the system $ACy = b$ which is equal to $Hy = b$. This gives us the solutions $y_1 = -1$, $y_2 = 2$, $y_3 \in \mathbb{Z}$. Hence with $x = Cy$ we get

$$x = Cy = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 1 & -1 \\ 1 & 0 & -2 \end{pmatrix} \begin{pmatrix} -1 \\ 2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ -1 \end{pmatrix} + y_3 \begin{pmatrix} 2 \\ -1 \\ -2 \end{pmatrix}, y_3 \in \mathbb{Z}$$

and the desired set of integral solutions is

$$\begin{pmatrix} 2 \\ 1 \\ -1 \end{pmatrix} + \mathbb{Z} \begin{pmatrix} 2 \\ -1 \\ -2 \end{pmatrix}.$$

Exercise 3.2 [5 credits]

Consider the lattice $L(A) := \{Ax : x \in \mathbb{Z}^3\}$ generated by the columns of

$$A = \begin{pmatrix} 4 & 2 & 2 \\ 1 & 3 & 5 \end{pmatrix}.$$

a) Sketch (parts of) the lattice $L(A)$.

b) Prove or disprove the following statement: There are two linearly independent columns of A that already generate the lattice $L(A)$.

Answer to Exercise 3.2

a) The lattice can be seen in Figure 1.

b) The statement is false in this case (and in many similar cases). Consider any two columns of the matrix A. If the lattice generated by these two columns was identical to $L(A)$, then we would have to be able to express the "missing column" as a linear combination of the two selected columns using only integer coefficients. For example, let us select the first two columns $(4,1)^T$ and $(2,3)^T$. Then we would have to find integers $x_1, x_2 \in \mathbb{Z}$ such that

$$\begin{pmatrix} 4 & 2 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 2 \\ 5 \end{pmatrix}.$$

As the left hand side matrix is regular, this equation has at most one solution, and an easy computation shows that $(x_1, x_2) = (-2/5, 9/5)$ is the unique solution. It is not integral, thus there is no suitable integral combination. The same argument can be used for any other choice of two columns from A.

Exercise 3.3 [7 credits]

Let $A \in \mathbb{Z}^{m \times n}$ be a matrix of full row rank $b \in \mathbb{Z}^m$. Show that the system $Ax = b$ has an integral solution if and only if $y^T b \in \mathbb{Z}$ for each $y \in \mathbb{R}^m$ with $y^T A \in \mathbb{Z}^n$. (This is an integer version of Farkas' lemma.)

Answer to Exercise 3.3

"⇒": Let $x \in \mathbb{Z}^n$ be a solution to $Ax = b$ and let $y \in \mathbb{R}^m$ such that $y^T A \in \mathbb{Z}^n$. Then

$$y^T b = y^T (Ax) = \underbrace{(y^T A)}_{\in \mathbb{Z}^n} \underbrace{x}_{\in \mathbb{Z}^n} \in \mathbb{Z},$$

thus $y^T b \in \mathbb{Z}$.

"⇐": Suppose that for every $y \in \mathbb{R}^m$ with $y^T A \in \mathbb{Z}^n$ we also have $y^T b \in \mathbb{Z}$. The linear equation system $Ax = b$ has at least some fractional solution x, as A has full row rank. The equation $Ax = b$ is invariant with respect to elementary column operation (i. e., multiplication with some unimodular matrix), thus we may assume that there is some unimodular transformation $C \in \mathbb{Z}^{n \times n}$ such that $AC = (B, 0)$ is in Hermite Normal Form. As $B^{-1}A = B^{-1}(B,0)C^{-1} = (I_m, 0)C^{-1} \in \mathbb{Z}^{m \times n}$ we get that $b_i^T A \in \mathbb{Z}^n$ for each row b_i^T of B^{-1} and by our assumption that means $b_i^T b \in \mathbb{Z}$, so $B^{-1} b \in \mathbb{Z}^m$. Thus the vector

$$x' := \begin{pmatrix} B^{-1} b \\ 0 \end{pmatrix} \in \mathbb{Z}^n$$

is integral and it solves the linear equation system $ACx' = b$. Finally, $x := Cx'$ is an integral solution to $Ax = b$.

Exercise 3.4 [6 credits]

Let $A \in \mathbb{Z}^{m\times n}$ be a matrix of full row rank and $L(A) := \{Ax : x \in \mathbb{Z}^n\}$ the lattice generated by its columns. We define the *dual lattice* $L(A)^\perp$ by

$$L(A)^\perp := \left\{ y \in \mathbb{R}^m : y^T z \in \mathbb{Z} \text{ for all } z \in L(A) \right\}.$$

a) Show for a square, nonsingular matrix $A \in \mathbb{Z}^{n\times n}$ that $L(A)^\perp = L((A^{-1})^T)$. In other words, $L(A)^\perp$ is generated by the rows of A^{-1}.

b) Show for square, nonsingular matrix $A \in \mathbb{Z}^{n\times n}$ that $L(A)^{\perp\perp} = L(A)$.

Answer to Exercise 3.4

a) We denote the ith row of A^{-1} by $\tilde{a}_i$ and the ith column of A by a^i.

"$\subset$": Let $y \in L(A)^\perp$. Then, we have $y^T a^i \in \mathbb{Z}$ for each column vector a^i of A (set $z = a^i$ in the definition). This means that $y^T A$ is an integral vector, and therefore $y^T = (y^T A)A^{-1}$ is an integral linear combination of the rows of A^{-1} and thus y is an element of the lattice generated by the rows of A^{-1} (i. e., $y = \sum_i \mu_i \tilde{a}_i{}^T$ with integral μ_i since by convention we view lattice vectors as column vectors).

"$\supset$": Conversely, let y denote an element of the lattice generated by the rows of A^{-1}, thus

$$y = \sum_i \mu_i \tilde{a}_i{}^T,$$

with integral μ_i. Any $z \in L(A)$ is of the form $z = \sum_i \nu_i a^i$ with integral ν_i. Since $A^{-1}A = I$ we thus have $y^T z = \sum_i \mu_i \nu_i \in \mathbb{Z}$, i. e., $y \in L(A)^\perp$.

b) We use the facts that for non-singular A, we have $(A^{-1})^{-1} = A$ and $(A^{-1})^T = (A^T)^{-1}$. The statements in a) can be restated: "If $L(A)$ is generated by the columns of the nonsingular matrix A, then $L(A)^\perp$ is the lattice generated by the colums of $(A^{-1})^T$." In other words, we obtain:

$$\begin{aligned}
&L(A)^{\perp\perp} && \text{is the dual of the lattice generated by the columns of } (A^{-1})^T \\
\Leftrightarrow\, &L(A)^{\perp\perp} && \text{is the lattice generated by the columns of } (((A^{-1})^T)^{-1})^T \\
\Leftrightarrow\, &L(A)^{\perp\perp} && \text{is the lattice generated by the columns of } (((A^T)^{-1})^{-1})^T \\
\Leftrightarrow\, &L(A)^{\perp\perp} && \text{is the lattice generated by the columns of } (A^T)^T = A \\
\Leftrightarrow\, &L(A)^{\perp\perp} = L(A)
\end{aligned}$$

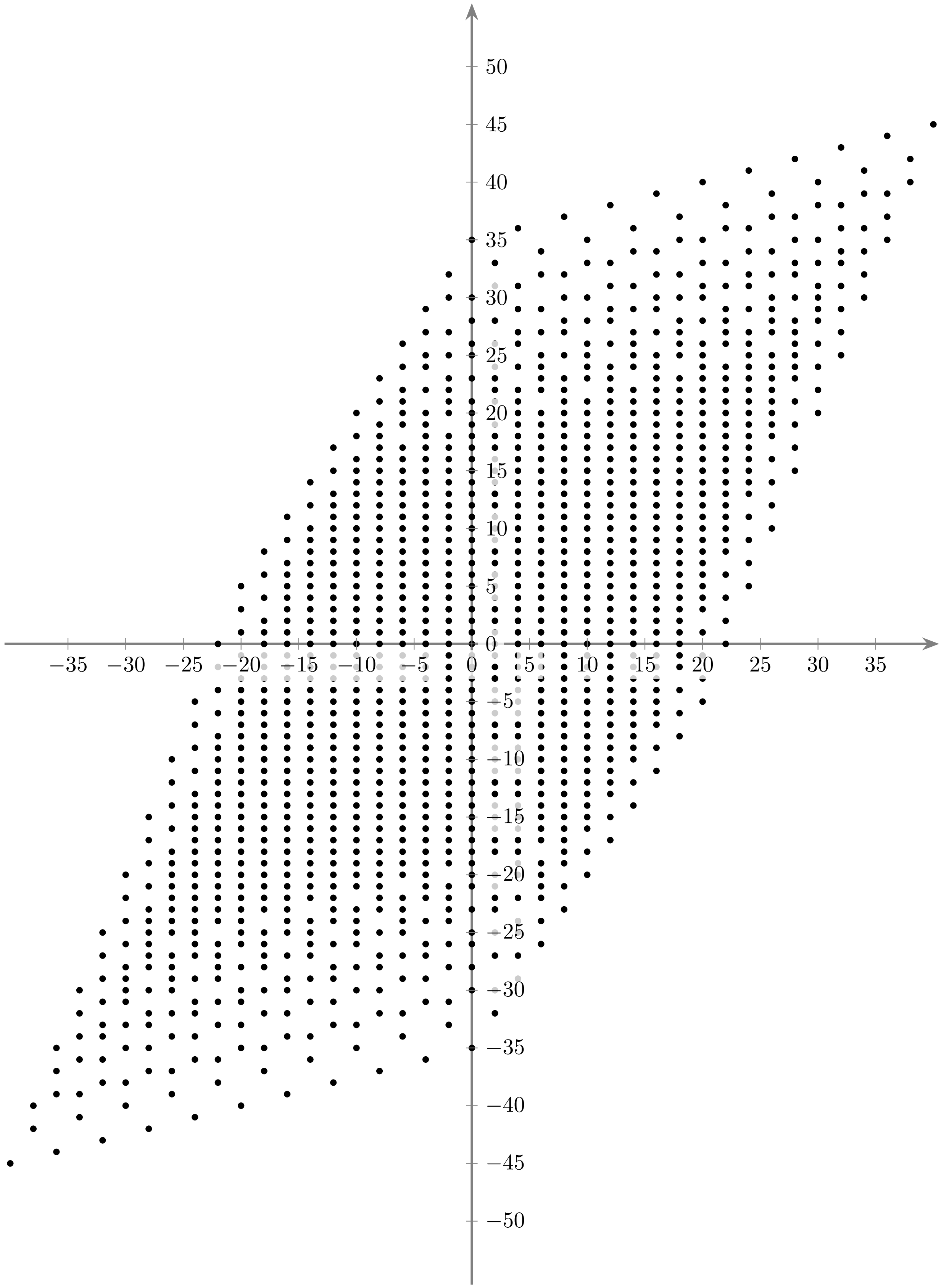

Figure 1: The lattice $L(A)$.