Linear Diophantine Equation Systems

Martina Tscheckl
Advisor: Roswitha Risser, Dipl.-Ing. Dr.techn.

Outlook

1. Motivation
2. Definitions
3. Existence of Smith Normal Form
4. Uniqueness of Smith Normal Form
5. Solvability of Linear Diophantine Equation Systems
6. (Algorithms)

Motivation

Given: A $u \in \mathbb{C} \setminus \mathbb{Z}$ such that $\exists f_\ell \in \mathbb{Z}$ with $u^n = -\sum_{\ell=0}^{n-1} f_\ell u^\ell$. Assume n to be minimal, then

$$R = \left\{ \sum_{\ell=0}^{n-1} v_\ell u^\ell \,\middle|\, v_0, \ldots, v_{n-1} \in \mathbb{Z} \right\} \tag{1}$$

is a commutative ring. Let further I be an ideal with generated by $a_1, \ldots, a_m \in R$

$$I = \langle a_1, \ldots, a_n \rangle \lhd R. \tag{2}$$

Question: Take some $b \in R$. Is b also an element in I?

Idea

Assume $b \in I$. Then $\exists x_1, \dots, x_m \in R$ such that

$$b = \sum_{j=1}^{m} x_j a_j .$$

Every element in R has a unique representation. Thus $\exists b_\ell, x_{\ell j}, a_{\ell j} \in \mathbb{Z}$ such that

$$\sum_{\ell=0}^{n-1} b_\ell u^\ell = b = \sum_{j=1}^{m} \left(\sum_{\ell=0}^{n-1} x_{\ell j} u^j \right) \left(\sum_{\ell=0}^{n-1} a_{\ell j} u^j \right)$$

Linear Diophantine Equation System

$$u^{n+h} = \sum_{\ell=0}^{n-1} w_{\ell h} u^{\ell}$$

$$w_{\ell h} = \begin{cases} 0 & \text{for } \ell < 0 \\ f_\ell & \text{for } h = 0 \\ w_{(n-1)(h-1)} w_{\ell 0} + w_{(\ell-1)(h-1)} & \text{for } 1 \leq h \leq n-2 \end{cases} .$$

Linear Diophantine Equation System

$$u^{n+h} = \sum_{\ell=0}^{n-1} w_{\ell h} u^{\ell}$$

$$w_{\ell h} = \begin{cases} 0 & \text{for } \ell < 0 \\ f_\ell & \text{for } h = 0 \\ w_{(n-1)(h-1)} w_{\ell 0} + w_{(\ell-1)(h-1)} & \text{for } 1 \leq h \leq n-2 \end{cases} .$$

$$b_\ell = \sum_{j=1}^{m} \left(\sum_{i=0}^{\ell} x_{ij} \cdot a_{(\ell-i)j} + \sum_{i=1}^{n-1} \sum_{h=0}^{i-1} x_{ij} \cdot a_{(h+n-i)j} \cdot w_{\ell h} \right)$$

Matrix Representation

Let $\mathbf{b} = (b_0, \dots, b_{n-1})^t$ and $\mathbf{x} = (x_{01}, \dots, x_{(n-1)1}, x_{02}, \dots, x_{(n-1)m})^t$. Define A as

$$a_{\ell\nu} = \begin{cases} a_{\ell j} & \text{if } \nu = n(j-1) \\ a_{(\ell-i)j} + \sum_{h=0}^{i-1} a_{(h+n-i)j} w_{\ell h} & \text{if } \nu = n(j-1)+i \\ & \text{ for } 1 \leq i \leq \ell \\ \sum_{h=0}^{i-1} a_{(h+n-i)j} w_{\ell h} & \text{if } \nu = n(j-1)+i \\ & \text{ for } \ell < i < n \end{cases}$$

So $b \in I$ if and only if this linear diophantine equation system $A\mathbf{x} = \mathbf{b}$ is solvable.

Definitions I

Definition: Let $I_n \in \mathrm{M}_{n,n}(R)$ be the unit matrix and $E_k^\ell \in \mathrm{M}_{n,n}(R)$ be defined as

$$(e_k^\ell)_{ij} = \begin{cases} 1 & \text{if } i = k \text{ and } j = \ell \\ 0 & \text{otherwise} \end{cases}.$$

Further, we define

$$Q_i^j(\lambda) = I_n + \lambda \cdot E_i^j.$$

with $\lambda \in R$ and $\lambda \neq -1$ in case $i = j$. Matrices $Q_i^j(\lambda)$ are called *elementary matrices*.

Remarks

The inverse of $Q_i^j(\lambda)$ is

$$Q_i^j(\lambda)^{-1} = \begin{cases} Q_i^j\left(-\lambda\right) & \text{if } i \neq j \\ Q_i^j\left(\frac{-\lambda}{1+\lambda}\right) & \text{if } i = j \text{ and } 1+\lambda \in R^{\times} \end{cases}$$

If $1+\lambda \notin R^{\times}$, then there exists no inverse for $Q_i^i(\lambda)$.

Remarks

The inverse of $Q_i^j(\lambda)$ is

$$Q_i^j(\lambda)^{-1} = \begin{cases} Q_i^j\left(-\lambda\right) & \text{if } i \neq j \\ Q_i^j\left(\frac{-\lambda}{1+\lambda}\right) & \text{if } i = j \text{ and } 1+\lambda \in R^\times \end{cases}$$

If $1+\lambda \notin R^\times$, then there exists no inverse for $Q_i^i(\lambda)$.

Interchanging the i-th and j-th columns of a matrix equals a matrix multiplication from right with the following successive column operations

$$Q_j^i(1), Q_i^j(1), Q_j^i(-1), Q_i^j(2), Q_i^i(-2).$$

Definitions II

Definition: Let $M, M' \in \mathsf{M}_{m,n}(R)$. We say M is equivalent to M', written as $M \sim M'$, if and only if there exist two matrices $U \in \mathsf{GL}_m(R)$ and $V \in \mathsf{GL}_n(R)$ such that

$$UMV = M'.$$

We refer to the matrices U and V as *transformation matrices*. Note, that the transformation matrices U and V are not uniquely determined.

Existence of Smith Normal Form

Proposition: Let R be an Euclidean ring and $A \in \mathsf{M}_{m,n}(R)$. Then A is equivalent to a matrix B where $b_{11}|b_{ij}$ and $0 = b_{i1} = b_{1j}$ for all $i, j \geq 2$, and the transformation matrices are a product of elementary matrices.

Existence of Smith Normal Form

Proposition: Let R be an Euclidean ring and $A \in \mathrm{M}_{m,n}(R)$. Then A is equivalent to a matrix B where $b_{11} | b_{ij}$ and $0 = b_{i1} = b_{1j}$ for all $i, j \geq 2$, and the transformation matrices are a product of elementary matrices.

Theorem: Let $A \in \mathrm{M}_{m,n}(R)$ be of rank r. Then there exist matrices $U \in \mathrm{GL}_m(R)$ and $V \in \mathrm{GL}_n(R)$ such that

$$UAV = D = \mathrm{diag}(d_1, d_2, \ldots, d_r, 0, \ldots, 0)$$

where d_i are unique (up to associates) and $d_i | d_{i+1}$ for $i = 1, \ldots, r-1$.

Uniqueness of Smith Normal Form

Definition: A $k \times k$ minor of a matrix A is the determinant of a submatrix of A with k rows and k columns. The greatest common divisor of all $k \times k$ minors is called the k-th determinantal divisor.

Uniqueness of Smith Normal Form

Definition: A $k \times k$ minor of a matrix A is the determinant of a submatrix of A with k rows and k columns. The greatest common divisor of all $k \times k$ minors is called the k-th determinantal divisor.

Proposition: Let $A \sim A'$ and let the transformation matrices be a product of successive elementary row and column operations, then A and A' have the same determinantal divisors.

Uniqueness of Smith Normal Form

Definition: A $k \times k$ minor of a matrix A is the determinant of a submatrix of A with k rows and k columns. The greatest common divisor of all $k \times k$ minors is called the k-th determinantal divisor.

Theorem: Two matrices have the same Smith Normal Form if and only if they have the same determinantal divisors (up to multiplication with associates). In particular, the Smith Normal Form is uniquely determined (up to associates).

Conditions for solvability

Let R be an Euclidean ring and $A \in \mathsf{M}_{m,n}(R)$ be a matrix of rank r. Further, let $U \in \mathsf{GL}_m(R)$ and $V \in \mathsf{GL}_n(R)$ such that $UAV = D = \text{diag}(d_1, \dots, d_r, 0, \dots, 0)$ is the Smith Normal Form of A. For $b \in R^m$ the linear equation system $Ax = b$ is solvable in $x \in R^n$ if and only if, for $c = Ub$, there exist $y_1, \dots, y_r \in R$ such that

$$\begin{aligned} c_i &= d_i \cdot y_i && \text{for } 1 \leq i \leq r \text{ and} \\ c_i &= 0 && \text{for } r < i \leq n \end{aligned}$$

In this case, all solutions to the system are of the form $x = Vy$ with $y_i = \frac{c_i}{d_i}$ for $1 \leq i \leq r$ and $y_{r+1}, \dots, y_n$ arbitrary.

Algorithms

1. Hermite Normal Form
2. Smith Normal Form

Thanks

- Thank you for coming
- Thank you for listening
- Feel free to ask questions