

Gitter und Kryptographie

Blatt 1, 18.10.2007, Abgabe 25.10.2007

Aufgabe 1. Sei $A = A^t = (a_{i,j}) \in \mathbb{R}^{n \times n}$ regulär. Zeige, dass es eine eindeutige Zerlegung $A = R^t D R$ gibt, derart, dass $R = (r_{i,j}) \in \mathbb{R}^{n \times n}$ eine obere Dreiecksmatrix ist (also $r_{i,j} = 0$ für $i > j$ und $r_{i,i} > 0$) und D Diagonalmatrix mit Diagonale $(\sigma_1, \dots, \sigma_n) \in \{\pm 1\}^n$.

Induktionsanfang: $a_{1,1} = r_{1,1}^2 \sigma_1$ und somit $\sigma_1 = \text{sign}(a_{1,1})$, $r_{1,1} = (a_{1,1} \sigma_1)^{1/2}$.

Aufgabe 2. Sei $A = A^t \in \mathbb{R}^{n \times n}$ regulär mit Zerlegung $A = R^t D R$ nach Aufgabe 1. Zeige:

1. $f_A(\mathbf{x}) \geq 0$ für alle $\mathbf{x} \in \mathbb{R}^n$ gdw $\sigma_1 = \dots = \sigma_n = 1$
2. $f_A(\mathbf{x}) \leq 0$ für alle $\mathbf{x} \in \mathbb{R}^n$ gdw $\sigma_1 = \dots = \sigma_n = -1$
3. f_A ist indefinit für $\mathbf{x} \in \mathbb{R}^n$ gdw $\exists \sigma_i = 1, \sigma_j = -1$.

Aufgabe 3. Sei $A = A^t = (a_{i,j}) \in \mathbb{R}^{n \times n}$ regulär mit Zerlegung $A = R^t D R$ nach Aufgabe 1. Zeige, dass für die Untermatrizen $A_k := (a_{i,j})_{1 \leq i,j \leq k}$ gilt:

1. $A_k = R_k^t D_k R_k$
2. $\sigma_1 \cdots \sigma_k = \det A_k (\det R_k)^{-2}$
3. $\sigma_k = \text{sign}(\det A_k / \det A_{k-1})$.