Smith-Normalform

4. Juni 2015

1 Algorithmus zur Berechnung der Smith-Normalform einer Matrix $A \in R^{m \times n}$

Im folgenden ist R ein Hauptidealring.

1.1 Elementarmatrizen über Hauptidealringen

Im Prinzip möchten wir Gauß-Elimination anwenden, doch die Elementarmatrizen, die das Element a_{ji} eliminieren haben die Gestalt

$$E_{\alpha}^{ij} = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & \alpha & \ddots & \\ & & & 1 \end{pmatrix}, \tag{1}$$

wobei $\alpha = -a_{ji}/a_{ii}$ ist und in Zeile j und Spalte i steht. Offensichtlich kann dieser Quotient nur gebildet werden, wenn $a_{ii} \mid a_{ji}$ gilt. Falls dies nicht der Fall ist, müssen wir auf andere Matrizen ausweichen.

Seien dazu zunächst $\alpha, \beta \in R$ teilerfremd. Dann gibt es ebenfalls teilerfremde Elemente $\sigma, \tau \in R$ so dass gilt

$$\alpha\sigma + \beta\tau = 1. \tag{2}$$

Für diese Elemente sind die Matrizen

$$\begin{pmatrix} \alpha & \beta \\ -\tau & \sigma \end{pmatrix} \in R^{2\times 2} \quad \text{und} \quad \begin{pmatrix} \sigma & -\beta \\ \tau & \alpha \end{pmatrix} \in R^{2\times 2} \tag{3}$$

invers zueinander. Ebenso gilt dies natürlich für

$$E_{\alpha\beta}^{ij} = \begin{pmatrix} 1 & & & & \\ & \alpha & & \beta & \\ & & 1 & & \\ & -\tau & & \sigma & \\ & & & & 1 \end{pmatrix} \in R^{n\times n}, \tag{4}$$

bei der die Zahlen $\alpha, \beta, \sigma, -\tau$ in den Zeilen und Spalten i und j stehen und die Matrix $E^{ij}_{\sigma,-\beta}$, sofern die Beziehung aus Gleichung (2) gilt.

Aus der Beziehung $B = E^{ij}_{\alpha\beta}A$ folgt, für die Zeilenvektoren b_k von B und a_k von A:

$$\begin{aligned} b_i &= \alpha a_i + \beta a_j, \\ b_j &= -\tau a_i + \sigma a_j. \end{aligned} \tag{5}$$

Insbesondere modifiziert eine Matrix dieses Typs beide Zeilen in Abhängikeit voneinander. Will man die Operationen von Gleichung (5) auf die Spalten- statt der Zeilenvektoren anwenden, so wird dies durch

$$B = (E^{ij}_{\alpha\beta}A^T)^T = A\left(E^{ij}_{\alpha\beta}\right)^T = AE^{ij}_{\alpha,-\tau} \tag{6}$$

erreicht.

1.2 Der Algorithmus

Vorbemerkung: Um die Notation nicht zu verkomplizieren, wird die resultierende Matrix der vorherigen Operation immer wieder mit A bezeichnet.

Sei nun also $A \in R^{m\times n} \neq 0$.

1. Falls $a_{11} = 0$, wende Permutationen an, so dass $a_{11} \neq 0$:
$$A \leftarrow S^{(1)}AT^{(1)}$$
2. In diesem Schritt sorgen wir dafür, dass wir eine Matrix bekommen, in der das Element a_{11} alle Elemente a_{j1} mit $j = 2,\ldots,m$ und a_{1j} mit $j = 1,\ldots,n$ teilt.
   (a) Für $j = 2,\ldots,m$, führe folgende Operationen aus, falls $a_{11} \nmid a_{j1}$: sei $\gamma = ggT(a_{11}, a_{j1})$. Dann sind $\alpha = a_{11}/\gamma$ und $\beta = a_{j1}/gamma$ teilerfremd und es gibt teilerfremde $\sigma, \tau \in R$ mit $\alpha\sigma + \beta\tau = 1$. Daher ist $E^{1j}_{\sigma\tau}$ invertierbar und für die Matrix
   $$B = E^{1j}_{\sigma\tau}A \tag{7}$$
   gilt $b_{11} = \sigma a_{11} + \tau a_{j1} = \gamma$, es wird also a_{11} durch den Teiler γ ersetzt.
   (b) Für $j = 2,\ldots,n$ führt man dasselbe Verfahren mit Multiplikation mit Elementarmatrizen von rechts durch und erreicht dadurch, dass $a_{11} \mid a_{1j}$.
   (c) Im vorigen Schritt wurde möglicherweise die Relation $a_{11} \mid a_{j1}$ zerstört, da die erste Spalte jeweils auch modifiziert wurde. Daher müssen die Schritte (a) und (b) wiederholt werden, bis sich a_{11} in einem kompletten Zyklus nicht mehr ändert. Da a_{11} immer durch einen Teiler von sich selbst ersetzt wird, die Primfaktorzerlegung zu Anfang aber endlich ist, kommt diese Iteration tatsächlich zum Stillstand.

3. Nun gilt $a_{11} \mid a_{j1}$ mit $j = 2, \ldots, m$, daher können wir die Elementarmatrizen E_α^{1j} mit $\alpha = -a_{j1}/a_{11}$ von links anwenden. Diese eliminieren das Element a_{j1} ohne die erste Zeile zu verändern. Ebenso können wir $\left(E_\alpha^{1j}\right)^T$ mit $\alpha = -a_{1j}/a_{11}$ für $j = 1, \ldots, n$ von rechts anwenden um a_{1j} zu eliminieren ohne die erste Spalte zu verändern.

4. Als Ergebnis dieser Schritte erhalten wir die Darstellung

$$A = S \left(\begin{array}{c|ccc} a_{11} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \tilde{A} & \\ 0 & & & \end{array}\right) T \tag{8}$$

wobei die Matrizen $S \in R^{m \times m}$ und $T \in R^{n \times n}$ als Produkte von Elementarmatrizen invertierbar sind.

5. Wiederhole nun den Prozess für die Matrix $\tilde{A} \in R^{m-1 \times n-1}$ und iteriere insgesamt r Schritte, bis $\tilde{A} = 0$, was spätestens nach m oder n Wiederholungen eintritt. Das Ergebnis hat bereits die Gestalt (wir setzen $\alpha_i = a_{ii}$):

$$A = S \left(\begin{array}{ccc|c} \alpha_1 & & & \\ & \ddots & & 0 \\ & & \alpha_r & \\ \hline & 0 & & 0 \end{array}\right) T. \tag{9}$$

Hierbei mögen der untere oder der rechte Block leer sein.

6. In den verbleibenden Schritten wird die Teilbarkeitsbeziehung $\alpha_i \mid \alpha_{i+1}$ sichergestellt. Sei dazu nun A die Diagonalmatrix aus Gleichung (9), und für einen Index i gelte $\alpha_i \nmid \alpha_{i+1}$. Dann sei $\gamma = ggT(\alpha_i, \alpha_{i+1})$ und $\sigma\alpha_i + \tau\alpha_{i+1} = \gamma$ mit $\sigma, \tau \in R$ teilerfremd. Durch Multiplikation mit Elementarmatrizen (transponierte von rechts) erreichen wir

$$\begin{pmatrix} \alpha_i & \\ & \alpha_{i+1} \end{pmatrix} \xrightarrow{\left(E_{\alpha_{i+1}}^{i+1,1}\right)^T} \begin{pmatrix} \alpha_i & \\ \alpha_{i+1} & \alpha_{i+1} \end{pmatrix} \xrightarrow{E_{\sigma\tau}^{i,1+1}} \begin{pmatrix} \gamma & 0 \\ 0 & \frac{\alpha_i \alpha_{i+1}}{\gamma} \end{pmatrix}, \tag{10}$$

wobei wir nur die relevanten Zeilen und Spalten dargestellt haben. Das Produkt $\alpha_i \alpha_{i+1}$ enthält einen Faktor γ^2, so dass wir das Ziel $\alpha_i \mid \alpha_{i+1}$ erreicht haben.

7. Wie schon weiter oben kann es nun passieren, dass durch den vorigen Schritt die erzielte Teilbarkeit z. B. $\alpha_{i-1} \mid \alpha_i$ zerstört wurde. Wir sehen aber, dass die Transformationen in Gleichung (10) die Anzahl der Primfaktoren im Produkt $\alpha_1 \alpha_2 \cdots \alpha_r$ nicht ändern, das ferner Primfaktoren immer nur „nach rechts wandern“. Entsprechend bricht auch diese Iteration nach endlich vielen Schritten ab, spätestens, wenn alle Elemente mit Ausnahme des letzten Einheiten sind.