

EIN EFFIZIENTES VERFAHREN ZUR BERECHNUNG EINER BASIS VON SUMME UND SCHNITT ZWEIER VEKTORRÄUME

FRANK KLINKER

ZUSAMMENFASSUNG. Wir stellen hier den Zassenhaus-Algorithmus vor. Das ist ein Verfahren, mit dem sich simultan eine Basis des Schnitts und eine Basis der Summe zweier Untervektorräume \mathcal{V} und \mathcal{W} des \mathbb{K}^n berechnen lassen. Dabei seien jeweils ein Erzeugendensystem von \mathcal{V} und \mathcal{W} vorgegeben.

Es seien $\{v_1, \dots, v_r\} \subset \mathbb{K}^n$ und $\{w_1, \dots, w_s\} \subset \mathbb{K}^n$ endliche Teilmengen. Weiter seien \mathcal{V} und \mathcal{W} die von diesen Systemen aufgespannten Vektorräume, d.h. $\mathcal{V} := \text{span}\{v_1, \dots, v_r\}$ und $\mathcal{W} := \text{span}\{w_1, \dots, w_s\}$.

Wir definieren die Matrizen $V \in M_{r,n}(\mathbb{K})$ und $W \in M_{s,n}(\mathbb{K})$ indem wir die Erzeugendensysteme als Zeilen eintragen, also

$$(1) \quad V := \begin{pmatrix} v_1^T \\ \vdots \\ v_r^T \end{pmatrix}, \quad W := \begin{pmatrix} w_1^T \\ \vdots \\ w_s^T \end{pmatrix}.$$

Wir wissen nun aus der Vorlesung, dass wir nach Anwendung des Gaußverfahrens auf $\begin{pmatrix} V \\ W \end{pmatrix} \in M_{r+s,n}(\mathbb{K})$ zu einer Matrix der Form $\begin{pmatrix} B \\ 0 \end{pmatrix} \in M_{r+s,n}(\mathbb{K})$

gelangen, wobei in $B = \begin{pmatrix} b_1^T \\ \vdots \\ b_k^T \end{pmatrix} \in M_{k,n}(\mathbb{K})$ die Zeilen linear unabhängig sind.

Das Gaußverfahren ist nun so geartet, dass die Zeilen von B Linearkombinationen der Zeilen von $\begin{pmatrix} V \\ W \end{pmatrix}$ sind, so dass $\{b_1, \dots, b_k\}$ eine Basis von $\mathcal{V} + \mathcal{W}$ bilden.

Wir können das Gaußverfahren auch mit Hilfe von Matrizen beschreiben. Bei der Durchführung des Gaußverfahrens treten (höchstens) folgenden Manipulationen der Matrix $\begin{pmatrix} V \\ W \end{pmatrix}$ auf:

Email: frank.klinker@math.tu-dortmund.de.

gilt mit $Z := Z_\ell \cdot Z_{\ell-1} \cdot \dots \cdot Z_1$

$$(5) \quad Z \begin{pmatrix} V \\ W \end{pmatrix} = \begin{pmatrix} B \\ 0 \end{pmatrix}.$$

Bemerkung: Die Matrix Z erhalten wir explizit, wenn wir das Gaussverfahren statt nur auf die Matrix $\begin{pmatrix} V \\ W \end{pmatrix}$ auf die um die Einheitsmatrix erweiterte Matrix $\left(\mathbb{1} \mid \begin{pmatrix} V \\ W \end{pmatrix} \right)$ anwenden. Das Ergebnis ist dann gerade $\left(Z \mid \begin{pmatrix} B \\ 0 \end{pmatrix} \right)$.

Wir zerlegen die Matrix $Z \in M_{r+s, r+s}(\mathbb{K})$ nun in kleiner Blöcke $Z_{11} \in M_{k, r}(\mathbb{K})$, $Z_{12} \in M_{k, s}(\mathbb{K})$, $Z_{21} \in M_{r+s-k, r}(\mathbb{K})$, $Z_{22} \in M_{r+s-k, s}(\mathbb{K})$ gemäß

$$(6) \quad Z = \begin{pmatrix} Z_{11} & Z_{12} \\ Z_{21} & Z_{22} \end{pmatrix}.$$

Wenn wir das benutzen, so läßt sich (5) zu

$$(7) \quad Z_{11}V + Z_{12}W = B$$

$$(8) \quad Z_{21}V + Z_{22}W = 0$$

umschreiben. Setzen wir $(Z_{21})_{ij} = -a_{ij}$ für $1 \leq i \leq r+s-k$, $1 \leq j \leq r$ und $(Z_{22})_{ij} = b_{ij}$ für $1 \leq i \leq r+s-k$, $1 \leq j \leq s$ so läßt sich (8) auch in Termen der Erzeugendensysteme von \mathcal{V} und \mathcal{W} schreiben:

$$(9) \quad \sum_{j=1}^s b_{ij}w_j = \sum_{j=1}^r a_{ij}v_j, \quad \text{für } 1 \leq i \leq r+s-k.$$

Alle diese $r+s-k$ Vektoren $z_j := \sum_{j=1}^s b_{ij}w_j$ liegen somit im Schnitt $\mathcal{V} \cap \mathcal{W}$.

Die folgende Überlegung zeigt sogar, dass sie ein Erzeugendensystem für den Schnitt bilden.

Wir betrachten die Vektorräume $\widehat{\mathcal{V}} \subset \mathcal{V} \oplus \{0\} \oplus \mathcal{V}$ und $\widehat{\mathcal{W}} \subset \mathcal{W} \oplus \mathcal{W} \oplus \{0\}$ mit den Erzeugendensystemen $\left\{ \begin{pmatrix} v_1 \\ 0 \\ v_1 \end{pmatrix}, \dots, \begin{pmatrix} v_r \\ 0 \\ v_r \end{pmatrix} \right\}$ und $\left\{ \begin{pmatrix} w_1 \\ w_1 \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} w_s \\ w_s \\ 0 \end{pmatrix} \right\}$.

Es gelten die folgenden Isomorphismen:

$$(10) \quad \widehat{\mathcal{V}} \simeq V, \quad \widehat{\mathcal{W}} \simeq W$$

$$(11) \quad \widehat{\mathcal{V}} + \widehat{\mathcal{W}} \simeq V \oplus W.$$

Die ersten zwei Isomorphismen (10) sieht man sofort, und die letzte (11) ist eine Folgerung aus den ersten beiden und der Dimensionsformel zusammen mit der Tatsache, dass $\widehat{\mathcal{V}} \cap \widehat{\mathcal{W}} = \{0\}$.

Schreiben wir nun die Basen von $\widehat{\mathcal{V}}$ und $\widehat{\mathcal{W}}$ ebenfalls als Matrizen in der Form

$$(12) \quad \begin{pmatrix} V & 0 & V \\ W & W & 0 \end{pmatrix} \in M_{r+s, 3n}(\mathbb{K})$$

so hat diese Matrix wegen (11) den Rang $\dim(\mathcal{V}) + \dim(\mathcal{W})$. Dieser ändert sich nicht, wenn wir die Matrix Z darauf wirken lassen. Diese Wirkung liefert

$$(13) \quad Z \begin{pmatrix} V & 0 & V \\ W & W & 0 \end{pmatrix} = \begin{pmatrix} B & Z_{12}W & Z_{11}V \\ 0 & Z_{22}W & Z_{21}V \end{pmatrix}$$

$$(14) \quad =: \begin{pmatrix} B & Z_{12}W & Z_{11}V \\ 0 & \tilde{C} & -\tilde{C} \end{pmatrix}.$$

Da Z ein Isomorphismus ist, ändert sich der Rang der Matrix nicht. Da nun die ersten k Zeilen linear unabhängig sind (dies gilt schon für B !) sind noch genau $\dim(\mathcal{V}) + \dim(\mathcal{W}) - k$ Zeilen der letzten $r + s - k$ Stück linear unabhängig, was gerade der Dimension von $\mathcal{V} \cap \mathcal{W}$ entspricht. Also bilden die Zeilen von $Z_{21}V = -Z_{22}W = -\tilde{C}$ ein Erzeugendensystem für $\mathcal{V} \cap \mathcal{W}$.

Eine Basis dieses Schnitts erhalten wir nun, indem wir das Gaußverfahren auf die unteren $r + s - k$ Zeilen der Matrix (14) anwenden. Das hat keinen Effekt auf die ersten n Spalten und wir bekommen schließlich

$$(15) \quad \begin{pmatrix} B & Z_{12}W & Z_{11}V \\ 0 & C & -C \\ 0 & 0 & 0 \end{pmatrix}$$

wobei nun die Zeilen von B und auch die Zeilen von C linear unabhängig sind.

Anwendung: Wir wenden das Gaussverfahren entweder auf $\begin{pmatrix} V & V \\ W & 0 \end{pmatrix}$ oder

$\begin{pmatrix} V & 0 \\ W & W \end{pmatrix}$ an. In beiden Fällen erhalten wir $\begin{pmatrix} B & \star \\ 0 & \pm C \\ 0 & 0 \end{pmatrix}$, wobei die Zeilen

von B die Basis von $\mathcal{V} + \mathcal{W}$ und die Zeilen von C eine Basis von $\mathcal{V} \cap \mathcal{W}$ bilden.