Algorithmische Methoden 1

Wolfgang Windsteiger

RISC Institut

Das Thema der heutigen Vorlesung

Univariate Polynome

Univariate Polynome und Polynomarithmetik

Definition (Polynom, Koeffizientenbereich, Koeffizient)

Wir nennen p ein univariates Polynom über K genau dann, wenn p eine Folge in K ist, die ab einem bestimmten Index nur 0 enthält. Wir nennen K den Koeffizientenbereich des Polynoms und die Folgenelemente von p die Koeffizienten von p.

Beispiel

Die Folge $\left(2, \frac{1}{5}, 0, \ldots\right)$ ist ein Polynom (über $\mathbb{R}$ oder $\mathbb{Q}$) mit den Koeffizienten $2, \frac{1}{5}, 0, \ldots$ und $(3, 5, -1, 0, 2, 0, \ldots)$ ist ein Polynom (über $\mathbb{R}$ oder $\mathbb{Q}$) mit Koeffizienten $3, 5, -1, 0, 2, 0, \ldots$.

Grad, Führender Koeffizient, Normiertheit

- Indizierung beginnt bei 0, d.h. der erste Koeffizient von p ist p_0, der zweite ist p_1 etc.
- Alle Koeffizienten können gleich 0 sein $\rightsquigarrow$ Nullpolynom, wir schreiben dafür $\mathtt{0}$.

Definition (Grad, Führender Koeffizient, Normiertheit)

Sei p ein Polynom über K und sei $d \in \mathbb{N}_0$ der minimale Index, mit dem $p_i = 0$ für alle $i \geq d$ gilt. Dann definieren wir

$$\deg(p) := d - 1,$$

und wir nennen $\deg(p)$ den Grad des Polynoms p. Für $p \neq \mathtt{0}$ nennen wir $p_{\deg(p)} \neq 0$ den führenden Koeffizienten von p und schreiben $\mathrm{fk}(p)$. Ist $\mathrm{fk}(p) = 1$, so nennen wir p normiert. Wir vereinbaren $\mathrm{fk}(\mathtt{0}) := 0$.

Notation

Bezeichnung

$$K[\mathtt{x}] := \left\{ p \;\middle|\; p \textit{ ist ein univariates Polynom über } K \right\}$$
$$K[\mathtt{x}]^n := \left\{ p \in K[\mathtt{x}] \;\middle|\; \deg(p) \leq n \right\}.$$

Koeffizientenvergleich

Definition (Gleichheit von Polynomen)

Zwei univariate Polynome über K sind genau dann gleich, wenn alle Koeffizienten übereinstimmen, d.h.

$$p = q \iff \big(\deg(p) = \deg(q) \quad \textit{und} \quad p_i = q_i \textit{ für } i = 0, \ldots, \deg(p)\big).$$

Diese Eigenschaft nutzen wir beim sogenannten Koeffizientenvergleich, wenn wir die Gleichheit zweier Polynome p und q auf ein System von Gleichheiten aller Koeffizienten reduzieren.

Arithmetik

Definition (Polynomarithmetik in $K[\mathtt{x}]$)

Seien $p, q \in K[\mathtt{x}]$.

$$p + q := (s_0, s_1, \ldots) \quad \textit{mit } s_i := p_i + q_i \textit{ für } i \in \mathbb{N}_0$$

$$p \cdot q := (r_0, r_1, \ldots) \quad \textit{mit } r_i := \sum_{j=0}^{i} p_j q_{i-j} \textit{ für } i \in \mathbb{N}_0.$$

- $K[\mathtt{x}]$ ist ein kommutativen Ring mit Einselement.
- $\mathtt{0}$ ist das neutrale Element bzgl. der Addition.
- Zu $p = (p_0, \ldots, p_n, 0, \ldots)$ ist $-p = (-p_0, \ldots, -p_n, 0, \ldots)$ das Inverse bzgl. der Addition.
- $p - q := p + (-q)$.
- $\mathtt{1} := (1, 0, \ldots)$ ist das neutrale Element bzgl. der Multiplikation.

Schreibweisen

Bezeichnung

Bezeichnet $K[\mathtt{x}]$ die Menge der univariaten Polynome über K, so ist

$$p_0 + p_1\mathtt{x} + \cdots + p_n\mathtt{x}^n = \sum_{i=0}^{n} p_i\mathtt{x}^i$$

die meist verwendete Schreibweise für ein Polynom p von Grad n. Bei $\mathtt{x}$ handelt es sich dabei lediglich um eine Bezeichnung für ein ganz bestimmtes Polynom, nämlich

$$\mathtt{x} = (0, 1, 0, \ldots)\,.$$

Polynomauswertung

Definition (Polynomauswertung)

Sei $p \in K[\mathrm{x}]$ und $w \in K$. Dann ist die Operation der Polynomauswertung (oder Polynomevaluation) definiert durch

$$\mathrm{eval}(p, w) := \sum_{i=0}^{\deg(p)} p_i w^i,$$

und wir nennen $\mathrm{eval}(p, w) \in K$ den Wert von p an der Stelle w.

Satz (Evaluations-Homomorphismus)

Für jedes $w \in K$ ist die Evaluation an der Stelle w ein Homomorphismus von $K[\mathrm{x}]$ nach K, d.h.

$$\mathrm{eval}(p + q, w) = \mathrm{eval}(p, w) + \mathrm{eval}(q, w)$$
$$\mathrm{eval}(p \cdot q, w) = \mathrm{eval}(p, w) \cdot \mathrm{eval}(q, w).$$

Polynomfunktion

Zu jedem Polynom $p \in K[\mathtt{x}]$ kann man eine Funktion von K nach K definieren, deren Funktionswerte sich durch Auswerten von p ergeben.

Definition (Polynomfunktion)

Sei $p \in K[\mathtt{x}]$. *Wir nennen*

$$\begin{aligned} \mathrm{pf}_p : K &\to K \\ x &\mapsto \mathrm{eval}(p, x) \end{aligned}$$

die zu p *gehörige Polynomfunktion (über* K*). Wir vereinbaren*

$$\Pi_K := \left\{ \mathrm{pf}_p \,\middle|\, p \in K[\mathtt{x}] \right\} \quad \textit{und} \quad \Pi_K^n := \left\{ \mathrm{pf}_p \,\middle|\, p \in K[\mathtt{x}], \deg(p) \leq n \right\}$$

für Mengen von Polynomfunktionen über K.

Datenstruktur für Polynome über K

Computerrepräsentation (Datenstruktur $\mathcal{P}_K$ für Polynome über K)

Ein univariates Polynom $p = (p_0, \ldots, p_n, 0, \ldots) \in K[\mathtt{x}]$ *von Grad* n *ist durch das Tupel* $t \in K^{n+1}$ *mit*

$$t_i = p_{i-1} \qquad \text{für } i = 1, \ldots, n+1 \tag{33}$$

charakterisiert. Wir führen daher für Polynome über K *eine Datenstruktur* $\mathcal{P}_K$ *ein, in der wir für* p *das in* (33) *definierte Tupel* t *abspeichern. Für* $p \in \mathcal{P}_K$ *sprechen wir das Koeffiziententupel* t *mit* $\mathrm{koef}(p)$ *an. Der führende Koeffizient steht an der letzten Position im Koeffiziententupel, das Nullpolynom* 0 *enthält ein leeres Koeffiziententupel, und* $|p|$ *bezeichnet die Länge des in* p *gespeicherten Tupels* t*. Zum Anschreiben eines Polynoms* $p \in \mathcal{P}_K$ *verwenden wir einfach das Tupel* t*.*

Grundoperationen

Für $p \in \mathcal{P}_K$ und $t = \text{koef}(p)$ können die Grundoperationen deg und fk durch

$$\deg(p) := |t| - 1$$

$$\text{fk}(p) := \begin{cases} 0 & \text{falls } p = 0 \\ t_{|t|} & \text{falls } p \neq 0 \end{cases}$$

realisiert werden. Die einzelnen Koeffizienten wollen wir auch für $p \in \mathcal{P}_K$ einfach mit p_i für $i \in \mathbb{N}_0$ ansprechen. Dies erreichen wir durch

$$p_i := \begin{cases} t_{i+1} & \text{falls } i \in \{0, \ldots, \deg(p)\} \\ 0 & \text{falls } i > \deg(p). \end{cases}$$

Weiters vereinbaren wir in Anlehnung an die Schreibweise $K[\mathtt{x}]^n$

$$\mathcal{P}_K^n := \{p \in \mathcal{P}_K \mid \deg(p) \leq n\}.$$

Arithmetik

Computerrepräsentation (Polynomarithmetik in $\mathcal{P}_K$)

Wir müssen bei der Definition der Rechenoperationen für Polynome sicherstellen, dass das resultierende Polynom wieder die in der Datenstruktur verlangte kanonische Form hat. Dazu verwenden wir eine Funktion namens kanonisch$_{\mathcal{P}_K}$, die allenfalls am Ende eines Tupels auftretende Nullen eliminiert.

$$p \pm q := s \in \mathcal{P}_K \text{ mit } \operatorname{koef}(s) = \text{kanonisch}_{\mathcal{P}_K}\left((p_i \pm q_i)_{i=0,\ldots,\max(\deg(p),\deg(q))}\right)$$

$$p * q := \begin{cases} 0 & \text{falls } p = 0 \vee q = 0 \\ s \in \mathcal{P}_K \text{ mit } \operatorname{koef}(s) = \left(\sum_{j=0}^{i} p_j q_{i-j}\right)_{i=0,\ldots,\deg(p)+\deg(q)} & \text{sonst,} \end{cases}$$

$$\lambda \cdot p := \begin{cases} 0 & \text{falls } \lambda = 0 \\ s \in \mathcal{P}_K \text{ mit } \operatorname{koef}(s) = (\lambda p_i)_{i=0,\ldots,\deg(p)} & \text{falls } \lambda \neq 0, \end{cases}$$

$$p/\mu := s \in \mathcal{P}_K \text{ mit } \operatorname{koef}(s) = (p_i/\mu)_{i=0,\ldots,\deg(p)}.$$

Spezifikation

Problemstellung (Polynomdivision mit Rest).

$$\begin{aligned} \text{Gegeben:} \quad & a, b \in K[\mathtt{x}] \\ \text{mit:} \quad & b \neq \mathtt{0}. \\ \text{Gesucht:} \quad & q, r \in K[\mathtt{x}] \\ \text{mit:} \quad & a = b \cdot q + r \text{ und } \deg(r) < \deg(b). \end{aligned}$$

Satz (Polynomdivision mit Rest)

Seien $a, b \in K[\mathtt{x}]$ *und* $b \neq \mathtt{0}$. *Dann existieren eindeutig bestimmte* $q, r \in K[\mathtt{x}]$ *mit* $a = b \cdot q + r$ *und* $\deg(r) < \deg(b)$.

Beweis mit Induktion über den Grad von a.

Divisionsalgorithmus

Induktionsbeweis ist konstruktiv $\rightsquigarrow$ rekursiver Algorithmus!

Algorithmus *QuotRestPolyRek*: Division mit Rest in $K[\mathtt{x}]$ rekursiv

if $\deg(a) < \deg(b)$
  $q \leftarrow 0,\ r \leftarrow a$
else
  $m \leftarrow \frac{\mathrm{fk}(a)}{\mathrm{fk}(b)} \cdot \mathtt{x}^{\deg(a)-\deg(b)}$
  $a' \leftarrow a - b * m$
  $(q', r') \leftarrow \mathit{QuotRestPolyRek}(a', b)$
  $q \leftarrow q' + m,\ r \leftarrow r'$
return (q, r)

Aufruf: $\mathit{QuotRestPolyRek}(a, b)$
Eingabe: $a, b \in K[\mathtt{x}]$
mit: $b \neq 0$.
Ausgabe: $q, r \in K[\mathtt{x}]$
mit: $a = b \cdot q + r$ und
$\deg(r) < \deg(b)$.

Analyse des rekursiven Algorithmus $\rightsquigarrow$ effiziente Realisierung als Schleife beruhend auf Datenstruktur $\mathcal{P}_K$.

Polynomdivision als Schleife

Algorithmus *QuotRestPoly*: Division mit Rest in $K[\mathrm{x}]$

$r \leftarrow a$
if $\deg(r) < \deg(b)$
  $q \leftarrow 0$
else
  $\mathrm{koef}(q) \leftarrow (0 \mid i = 0, \ldots, \deg(a) - \deg(b))$
  while $\deg(r) \geq \deg(b)$
    $d \leftarrow \deg(r) - \deg(b)$
    $q_d \leftarrow \frac{\mathrm{fk}(r)}{\mathrm{fk}(b)}$
    $r \leftarrow r - \mathit{Verschiebe}_{\mathcal{P}_K}(q_d \cdot b, d)$
return (q, r)

Aufruf: $\mathit{QuotRestPoly}(a,$
Eingabe: $a, b \in \mathcal{P}_K$
mit: $b \neq 0.$
Ausgabe: $q, r \in \mathcal{P}_K$
mit: $a = b \cdot q + r$ un
$\deg(r) < \deg(b).$