4.4. Automatisierbarkeit des Polynomkalküls

In Blatt 2 Aufgabe 2b wurde gezeigt, dass es einen Algorithmus gibt, der in Zeit $n^{O(k)}$ entscheidet, ob eine gegebene 3-KNF eine Resolutionswiderlegung der Weite k besitzt.

Ziel dieses Abschnitts ist es, eine analoge Aussage für den Polynomkalkül zu zeigen:

Satz 4.4

Für jedes d gibt es einen Algorithmus A_d, welcher für Polynome $f_1, \dots, f_m, g \in \mathbb{F}[x_1, \dots, x_n]$ vom Grad $\leq d$ entscheidet, ob es eine Ableitung von g aus $\{f_1, \dots, f_m\} \cup \{x_1^2 - x_1, \dots, x_n^2 - x_n\}$ vom Grad $\leq d$ gibt und falls dies der Fall ist, eine solche Ableitung berechnet. Die Laufzeit von A_d ist $O(n^{3d})$.

Technisch gesehen ist der Algorithmus A_d eine "Grad-beschränkte" Variante von Buchbergers Gröbnerbasis-Algorithmus.

Es ist nützlich, die folgende multilineare Version des Polynomkalküls zu betrachten.

Für ein Polynom $f = \sum_j a_j \cdot \prod_{i \in I_j} x_i^{d_i}$ sei

$$ML(f) := \sum_j a_j \cdot \prod_{i \in I_j} x_i \,.$$

Für multilineare Polynome $f_1, \dots, f_m$ (mit $\deg(f_i) \leq d$) besteht eine Grad-d Ableitung im ML-Polynomkalkül aus den Regeln

$$\frac{}{f_i}\,, \quad \frac{f \quad g}{a \cdot f + b \cdot g}\,, \quad \frac{f'}{ML(x \cdot f')} \qquad \text{mit } \deg(f), \deg(g) \leq d,\ \deg(f') \leq d-1.$$

für Polynome $f, f', g \in \mathbb{F}[X_1, \dots, X_n]$, Variablen $x \in \{X_1, \dots, X_n\}$, Konstanten $a, b \in \mathbb{F}$.

Lemma 4.5 Seien $g, f_1, \dots, f_m$ multilineare Polynome.

- g hat aus $\{f_1, \dots, f_m\}$ eine Ableitung im ML-Polynomkalkül vom Grad d.

$\Longleftrightarrow$ g hat aus $\{f_1, \dots, f_m\} \cup \{X_1^2 - X_1, \dots, X_n^2 - X_n\}$ eine Ableitung im Polynomkalkül vom Grad d.

Für den Rest des Abschnitts sei $\mathbb{F}$ ein Körper, $n \geq 1$ und V die Menge aller multilinearen Polynome aus $\mathbb{F}[x_1, \ldots, x_n]$.

Beobachtung: V ist ein Vektorraum.

▷ Sei $V_d(f_1, \ldots, f_m) := \{ g \mid g$ hat eine Grad-d Ableitung aus $\{f_1, \ldots, f_m\}$ im ML-Polynomkalkül $\}$.

Lemma 4.6

$V_d(f_1, \ldots, f_m)$ ist der kleinste Vektorraum $V' \subseteq V$ mit:

- $f_i \in V'$ für $1 \leq i \leq m$
- $f \in V' \Rightarrow M(x f) \in V'$ für alle f mit $\deg(f) \leq d-1$.

Beweis: Übung.

Der Algorithmus A_d (aus Satz 4.4) berechnet nun zunächst eine Basis für den Vektorraum $V_d(f_1, \ldots, f_m)$.

Sei $\prec$ eine Ordnung auf der Menge $\{ I \mid I \subseteq [n] \}$ mit $|I_1| < |I_2| \Rightarrow I_1 \prec I_2$.

Der Leitterm $LT(f)$ eines Polynoms $f = \sum_I a_I \cdot \prod_{i \in I} x_i \in V$ ist das Monom $\prod_{i \in I'} x_i$ für das größte (bzgl. $\prec$) I' mit $a_{I'} \neq 0$.

Analog ist der <u>Leitkoeffizient</u> $LK(f)$ der Koeffizient a_I vor dem Leitterm $\prod_{i \in I} x_i$.

Im Folgenden sei $f \in V$ ein Polynom und $B \subseteq V$ eine Menge von Polynomen mit $g, g' \in B,\ g \neq g' \Rightarrow LT(g) \neq LT(g')$.
(Daraus folgt, dass B linear unabhängig ist.)

REDUZIERE(f, B)

Falls es kein $g \in B$ mit $LT(g) = LT(f)$ gibt:

return f

Sonst sei $g \in B$ eindeutiges Polynom mit $LT(g) = LT(f)$

$$f' := f - \frac{LK(f)}{LK(g)} \cdot g$$

Falls $f' = 0$:

return 0

Sonst:

return REDUZIERE(f', B)

Nun gilt:

- REDUZIERE$(f, B) = 0 \iff f \in \text{span}(B)$
- REDUZIERE$(f, B) = f' \neq 0 \Rightarrow B \cup \{f'\}$ ist linear unabhängig und $\text{span}(B \cup \{f\}) = \text{span}(B \cup \{f'\})$.

Satz 4.7.

Der folgende Algorithmus berechnet eine Basis B für den Vektorraum $V_d(f_1, \dots, f_m)$ mit der Eigenschaft $g \neq g' \in B \Rightarrow LT(g) \neq LT(g')$ in Zeit $O(n^{3d})$.

```
BASIS_d(f_1, ..., f_m)
    B := ∅
    S := {f_1, ..., f_m}
    Solange S ≠ ∅:
        Wähle f ∈ S
        S := S \ {f}
        f' := REDUZIERE(f, B)
        Falls f' ≠ 0:
            B := B ∪ {f'}
            Falls deg(f') < d:
                Für j = 1, ..., n:
                    S := S ∪ {ML(x_j · f')}
    return B
```

Laufzeit:

- $REDUZIERE(f, B) \in O(n^{2d})$
- Wenn n Polynome in S eingefügt werden, wurde ein Polynom f' mit neuem Leitterm vom Grad $\leq d-1$ in B hinzugefügt.
  $\Rightarrow$ Die Solange-Schleife wird $O(n \cdot n^{d-1})$ mal durchlaufen.

$\Rightarrow BASIS_d(f_1, \dots, f_m) \in O(n^{3d})$.

Korrektheit:

Seien B_i, S_i die Mengen nach i Durchläufen der Solange-Schleife und $B_\infty := B_\ell$, $S_\infty := S_\ell$ für das kleinste ℓ mit $S_\ell = \emptyset$ ($\ell \leq \mathcal{O}(nd)$).

Wir zeigen induktiv für alle i:

a) $\text{span}(B_i \cup S_i) \subseteq V_d(f_1, \dots, f_m)$

b) $\text{span}(B_i \cup S_i) \subseteq \text{span}(B_{i+1} \cup S_{i+1})$

c) $g \in \text{span}(B_i) \Rightarrow x_j \cdot g \in \text{span}(B_i \cup S_i)$ für alle $1 \leq j \leq n$ und g mit $\deg(g) \leq d-1$.

Aus b) folgt • $\{f_1, \dots, f_m\} = S_0 \subseteq \text{span}(B_0 \cup S_0) \subseteq \text{span}(B_\infty \cup S_\infty) = \text{span}(B_\infty)$.

Aus c) folgt • $g \in \text{span}(B_\infty) \Rightarrow x_j \cdot g \in \text{span}(B_\infty)$.

$\Rightarrow$ (Lemma 4.6) $V_d(f_1, \dots, f_m) \subseteq \text{span}(B_\infty)$.

$\Rightarrow$ (wegen a)) $V_d(f_1, \dots, f_m) = \text{span}(B_\infty)$ w.z.b.w.

zu a) leicht zu sehen

zu b) Sei $f \in S_i$ mit $S_{i+1} \supseteq S_i \setminus \{f\}$, $f' := \text{REDUZIERE}(f, B_i)$.

• $f' = 0 \Rightarrow f \in \text{span}(B_i) \Rightarrow \text{span}(B_i \cup S_i) = \text{span}(B_{i+1} \cup S_{i+1})$.

• $f' \neq 0 \Rightarrow \text{span}(B_i \cup S_i) = \text{span}((B_i \cup \{f\}) \cup (S_i \setminus \{f\}))$

$= \text{span}((B_i \cup \{f'\}) \cup (S_i \setminus \{f\}))$

$\subseteq \text{span}(\underbrace{B_{i+1}}_{=} \cup \underbrace{S_{i+1}}_{=})$

zu c) Sei $g = \sum_{t \in T} a_t g_t$ und $g_t \in B_i$ wurde zum Zeitpunkt $t \leq i$ zu B_t hinzugefügt.

$\Rightarrow x_j g_t \in S_t$

$\Rightarrow x_j g_t \in span(B_t \cup S_t) \overset{b)}{\subseteq} span(B_i \cup S_i)$

$\Rightarrow x_j g = \sum_{t \in T} a_t x_j g_t \in span(B_i \cup S_i)$. □

Beweis von Satz 4.4.

Es ist leicht zu sehen, dass der Algorithmus aus Satz 4.7 eine Grad-d Ableitung im ML-Polynomkalkül für alle $g \in B$ generiert. Aus dieser kann nach Lemma 4.5 eine Ableitung aus $\underbrace{\{f_1, \dots, f_m\} \cup \{x_1^2 - x_1, \dots, x_n^2 - x_n\}}$ gewonnen werden.

Nun gilt, dass g aus B ableitbar ist $\Leftrightarrow$ REDUZIERE$(g, B) = 0$ und dies kann in $O(n^{2d})$ getestet werden.

Deswegen kann aus dem Lauf von REDUZIERE(g, B) eine Ableitung aus B gewonnen werden. □