4. Algebraische Beweissysteme

4.1. Einführung

→ Wir wollen zeigen, dass ein System von multivariaten Polynomen (über einem Körper $\mathbb{F}$) keine gemeinsame Nullstelle hat. D.h., dass $\left\{ \begin{array}{l} f_1(x_1, \dots, x_n) = 0 \\ \vdots \\ f_N(x_1, \dots, x_n) = 0 \end{array} \right\}$ unerfüllbar ist.

→ Diesen Ansatz können wir verwenden, um zu zeigen, dass eine k-KNF unerfüllbar ist.

→ Für eine Klausel $C = x_1 \vee \dots \vee x_k \vee \overline{y}_1 \vee \dots \vee \overline{y}_\ell$ sei $f_C = \prod_{i=1}^{k} (1 - x_i) \cdot \prod_{j=1}^{\ell} y_j$, $f_\emptyset := 1$

⇒ Für Belegung α gilt: $\alpha \models C \iff f_C(\alpha) = 0$.

→ Um 0/1 Lösungen im Körper $\mathbb{F}$ zu erzwingen, haben wir zusätzlich Polynome $x^2 - x = 0$ für alle Variable x.

⇒ Für alle k-KNF F und Körper $\mathbb{F}$ gilt:

F ist erfüllbar

$\iff$

Das System $\{ f_C = 0 \mid C \in F \} \cup \{ x^2 - x = 0 \mid x \in VAR(F) \}$ hat eine Lösung über $\mathbb{F}$.

- Alle Polynome sind syntaktisch in Monom-Schreibweise dargestellt.

⇒ Für $C = x_1 \vee \dots \vee x_k$ hat $f_C = \sum_{I \subseteq [k]} (-1)^{|I|} \cdot \prod_{i \in I} x_i$

2^k Monome.

⇒ Damit die Codierung einer Klauselmenge F als Polynomgleichungen polynomiell in F ist, betrachte wir nur k-KNF (für konstante k).

4.2 Nullstellensatz

Sei $\mathbb{F}$ ein Körper.

Eine Nullstellensatz-Widerlegung über $\mathbb{F}$ einer unerfüllbaren k-KNF $F = \{C_1, \dots, C_m\}$ mit n Variablen $x_1, \dots, x_n$ ist eine Folge $(g_1, \dots, g_m, h_1, \dots, h_n)$ von Polynomen aus $\mathbb{F}[x_1, \dots, x_n]$ so dass

$$\sum_{i=1}^{m} g_i \cdot f_{C_i} + \sum_{j=1}^{n} h_j (x_j^2 - x_j) = 1 .$$

Der Grad der Widerlegung ist der Maximalgrad aller Polynome $g_i \cdot f_{C_i}$ und $h_j (x_j^2 - x_j)$.

Beispiel von Nullstellensatz-Widerlegungen:

Klauselmenge: $\{ x \vee y,\ y \vee z,\ x \vee z,\ \bar{x} \vee \bar{y},\ \bar{y} \vee \bar{z},\ \bar{x} \vee \bar{z} \}$

$\hat{=}$ Polynomen $\{ xy,\ yz,\ xz,\ (1-x)(1-y),\ (1-y)(1-z),\ (1-x)(1-z) \}$

<u>Widerlegung über $\mathbb{R}$:</u> (ist auch Widerlegung über allen Körpern $\mathbb{F}$)

$$
\begin{aligned}
& 1 \cdot xy \\
+\ & (1-x) \cdot yz \\
+\ & (1-y) \cdot xz \\
+\ & 1 \cdot (1-x)(1-y) \\
+\ & x \cdot (1-y)(1-z) \\
+\ & y \cdot (1-x)(1-z)
\end{aligned}
\quad = \quad
\begin{aligned}
& xy \\
& -xyz + yz \\
& -xyz + xz \\
& +xy - x - y + 1 \\
& +xyz - xy - xz + x \\
& +xyz - xy - yz + y
\end{aligned}
\quad = 1
$$

<u>Widerlegung über $\mathbb{F}_2$:</u>

$$\sum_i 1 \cdot f_{c_i} = 2xy + 2yz + 2xz - 2x - 2y - 2z + 3 \overset{\text{über } \mathbb{F}_2}{=} 1$$

(Zur Erinnerung $\mathbb{F}_2$ ist der Körper mit Elementen $0, 1$ und

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

$2 := (1+1)$
$3 := (1+1+1)$
$\vdots$)

▷ Die Korrektheit von Nullstellensatz ist leicht zu sehen. Vollständigkeit folgt aus dem Hilbertschen Nullstellensatz, kann für Klauselmengen aber auch direkt gezeigt werden.

Satz 4.1

Jede unerfüllbare Klauselmenge über n Variablen hat eine Nullstellensatzwiderlegung vom Grad $\leq n$ über jedem Körper $\mathbb{F}$.

Beweis:

Für $\alpha : \{x_1, \dots, x_n\} \to \{0,1\}$ sei $f_\alpha := \prod_{\alpha(x_i)=1} x_i \cdot \prod_{\alpha(x_i)=0} (1-x_i)$.

① $\sum_\alpha f_\alpha = 1$ (Beweis: Induktion über n.)

② Für C Klausel über $\{x_1, \dots, x_n\}$ mit $\alpha \not\models C$ gilt f_C teilt f_α. (Beweis: $f_\alpha = f_C \cdot f_{\alpha|_{\{x_1,\dots,x_n\} \setminus Vars(C)}}$)

Sei $V_1 \dot\cup \dots \dot\cup V_m = \{\alpha \mid \alpha : \{x_1, \dots, x_n\} \to \{0,1\}\}$ Partition aller Belegungen mit $\alpha \in V_i \Rightarrow \alpha \not\models C_i$.

(Für unerfüllbare $F = C_1 \wedge \dots \wedge C_m$ ist jedes α in einem V_i.)

Dann ist $$1 = \sum_{\alpha} f_\alpha = \sum_{i=1}^{m} \sum_{\alpha \in V_i} f_\alpha$$

$$= \sum_{i=1}^{m} f_{c_i} \cdot \left(\sum_{\alpha \in V_i} \frac{f_\alpha}{f_{c_i}} \right)$$

eine Nullstellensatzwiderlegung vom Grad n. □

4.3 Der Polynomkalkül ("polynomial calculus")

Der Polynomkalkül ist eine Erweiterung von Nullstellensatz. Ausgehend von einem System von Polynomgleichungen $\{f_i = 0 \mid 1 \le i \le m\}$ können folgende Polynome abgeleitet werden.

Axiom $\dfrac{}{f_i}$, Linearkombination $\dfrac{f \quad g}{af + bg}$ für $a, b \in \mathbb{F}$

und Multiplikation $\dfrac{f}{xf}$ für eine Variable x.

Eine <u>Widerlegung</u> ist eine Ableitung von 1.
Der Grad einer Ableitung ist der größte Grad eines Polynoms in der Ableitung.

Korrektheit:

Wenn f aus $f_1, \dots, f_m$ abgeleitet wurde, dann gilt für alle Belegungen α: $\overset{\text{aus}}{\checkmark} f_i(\alpha) = 0$ für $i = 1 \dots m$ folgt $f(\alpha) = 0$. (Beweis: Induktion.)

Vollständigkeit:

Folgt aus Vollständigkeit für Nullstellensatz und der Beobachtung, dass der Polynomkalkül Nullstellensatz p-simuliert.

Wie auch der Nullstellensatz interessieren wir uns für Widerlegungen von kleinem Grad. Das nächste Lemma besagt, dass der kleinste Grad einer Widerlegung einer Klauselmenge durch die kleinste Weite (plus 1) einer Resolutionswiderlegung beschränkt ist.

Lemma 4.2

Jede unerfüllbare Klauselmenge F hat eine Widerlegung vom Grad $\leq w(F \vdash \emptyset) + 1$ im Polynomkalkül.

Beweis

Wir zeigen induktiv, dass für alle C in einer Resolutionswiderlegung Π von F das Polynom f_C eine Ableitung ~~der~~ vom Grad $\leq w(\Pi)+1$ besitzt.

IA: trivial

IS: sei $C' = C \cup D$ mit $\dfrac{C \cup \{x\} \quad D \cup \{\bar{x}\}}{C \cup D}$

$$f_{C\cup\{x\}} = (1-x)\cdot f_C \quad , \quad f_{D\cup\{\bar{x}\}} = x \cdot f_D$$

Durch multiplizieren von $f_{D\setminus C}$ bzw. $f_{C\setminus D}$ *)
erhalte wir $(1-x) f_{C\cup D}$ und $x f_{C\cup D}$
(der Grad dieser Polynome ist höchstens $w(C\cup D)+1$).
Addition der Polynome liefert uns $f_{C\cup D}$. □

*) Für alle f, g gibt es eine Ableitung von $g\cdot f$ aus f.

Wenn wir für jede Variable x eine zusätzliche Variable x^{neg} und die Axiome $x + x^{neg} - 1 = 0$ hinzufügen, folgt sogar, dass der Polynomkalkül Resolution p-simuliert (über jeden Körper $\mathbb{F}$).

Die Aussage von Lemma 4.2. gilt nicht für Nullstellensatz, wie der nächste Satz zeigt:

Satz 4.3 (n-Variablen)

Es gibt eine 3-KNF F mit $w(F \vdash \emptyset) = 3$, für die jede Nullstellensatzwiderlegung Grad $\Omega\left(\frac{n}{\log n}\right)$ hat.

Beweis

Sei $F = PEB_G$ für Graphen G aus Bemerkung 2.11 mit $P = Peb_G(S_G, T_G) = \Omega\left(\frac{n}{\log n}\right)$.

Wir zeigen, dass F keine Nullstellensatzwiderlegung von Grad $P-1$ besitzt.

Beweis von Satz 4.3 (Cont.)

(Die Variablen von F sind x_v für $v \in V(G)$.)

Wir definieren eine Abbildung D, die jedem Polynom vom Grad $\leq p-1$ einen Wert aus $\mathbb{F}$ zuweist.

Für Monome $\prod_{v \in T} x_v^{c_v}$ (einschließlich des leeren Monoms $\prod_{v \in \emptyset} x_v^{d_v} := 1$)

definieren wir:

$$D\left(\prod_{v \in T} x_v^{d_v}\right) := \begin{cases} 1, & \text{falls die Position } T \text{ (alle Black-Pebble sind auf Elemente aus } T\text{) im Black-Pebble-Spiel mit} \\ & \leq p-1 \text{ Spielsteinen erreichbar ist,} \\ 0, & \text{sonst.} \end{cases}$$

Die Abbildung D ist linear, d.h. wir setzen für Polynome $f = \sum_i a_i \cdot \prod_{v \in T_i} x_v^{d_v}$

$$D(f) := \sum_i a_i \cdot D\left(\prod_{v \in T_i} x_v^{d_v}\right).$$

Angenommen es gibt nun eine Nullstellendarstellung mit

$$\sum_{i=1}^{m} g_i f_{C_i} + \sum_{j=1}^{n} h_j \left(x_j^2 - x_j\right) = 1$$

vom Grad $\leq p-1$.

Beweis von Satz 4.3 (cont.)

Dann gilt

1. $D(h_j(x_j^2 - x_j)) = 0$ für alle $1 \le j \le n$,
2. $D(g_i f_{C_i}) = 0$ für alle $1 \le i \le m$,
3. $D(1) = 1$

$$\Rightarrow 0 = D\left(\sum_{i=1}^{m} g_i f_{C_i} + \sum_{j=1}^{n} h_j (x_j^2 - x_j)\right) = D(1) = 1 \quad \lightning$$

zu 1.: Gilt wegen Linearität und $D\left(\prod_{v \in T} x_v^{d_v}\right) \overset{(*)}{=} D\left(\prod_{v \in T} x_v\right)$.

zu 3.: Position $T = \emptyset$ ist erreichbar.

zu 2.:

Wir zeigen, dass für alle $C \in F$ und $T \subseteq V(G)$ mit $\deg\left(\prod_{v \in T} x_v \cdot f_C\right) \le d-1$ gilt: $D\left(\prod_{v \in T} x_v \cdot f_C\right) = 0$.

Axiome sind

a) $x_t = 0$, $t \in T_G$ $\Rightarrow D\left(\prod_{v' \in T \cup \{t\}} x_{v'}\right) = 0$

b) $(1 - x_s) = 0$, $s \in S_G$ $\Rightarrow D\left(\prod_{v' \in T} x_{v'}\right) = D\left(\prod_{v' \in T \cup \{s\}} x_{v'}\right)$

c) $x_u x_v (1 - x_w) = 0$, $N^-(v) = \{u, v\}$ $\Rightarrow D\left(\prod_{v' \in T \cup \{u,v\}} x_{v'}\right) = D\left(\prod_{v' \in T \cup \{u,v,w\}} x_{v'}\right)$.

$\Rightarrow$ 1. mit Linearität und $(*)$. $\square$