5.2 Sum-of-Squares und Resolution

Wir haben gesehen, dass Nullstellensatz vom Grad $o(\frac{n}{\log n})$ nicht in der Lage ist, Resolution beschränkter Weite zu simulieren (Satz 4.3).

SOS ist in der Hinsicht echt stärker als Nullstellensatz, wie der nächste Satz zeigt.

Satz 5.4

Wenn F eine Resolutionswiderlegung der Weite w besitzt, dann hat F eine SOS-Widerlegung vom Grad $2w$.

Beweis: Sei Γ eine Resolutionswiderlegung der Weite w.
Wir sagen "f hat eine Grad-$2w$ SOS-Ableitung" falls es Polynome g_i, h_j, p_ℓ gibt (mit entspr. Grad-Schranken) falls $\sum_i g_i f_{C_i} + \sum_j h_j (x_j^2 - x_j) - \sum_\ell p_\ell^2 = f$.

Wir zeigen induktiv über Γ: Für alle $C \in \Gamma$ hat f_C eine Grad-$2w$ Ableitung.

Der Satz folgt dann, da $f_\emptyset = 1$.

Induktionsanfang: trivial.

Induktionsschritt (Resolutionsregel):

Sei $C \cup D$ abgeleitet aus $C \cup \{x\}$ und $D \cup \{\bar{x}\}$.

Nach IA gibt es Polynome $g_i', h_j', p_\ell', g_i'', h_j'', p_\ell''$

mit: $$\sum_i g_i' f_{C,i} + \sum_j h_j' (x_j^2 - x_j) - \sum_\ell p_\ell'^2 = f_{C \cup \{x\}} = (1-x) f_C$$

$$\sum_i g_i'' f_{C,i} + \sum_j h_j'' (x_j^2 - x_j) - \sum_\ell p_\ell''^2 = f_{D \cup \{\bar{x}\}} = x f_D$$

Sei: $q := x f_D + (1-x) f_C - \frac{1}{2} f_C f_D$

Dann ist $q^2 = x^2 f_D^2 + (1-x) x f_C f_D - \frac{1}{2} x f_C f_D^2$

$+ (1-x) x f_C f_D + (1-x)^2 f_C - \frac{1}{2}(1-x) f_C^2 f_D$

$- \frac{1}{2} x f_C f_D^2 - \frac{1}{2}(1-x) f_C^2 f_D + \frac{1}{4} f_C^2 f_D^2$

$= \underbrace{x f_D + (1-x) f_C - \frac{3}{4} f_C f_D}_{= ML(q^2)} - \sum_j h_j (x_j^2 - x_j)$

für geeignete h_j.

$$\Rightarrow \sum_i \tfrac{4}{3}(g_i' + g_i'') f_{C,i} + \sum_j \tfrac{4}{3}(h_j' + h_j'' + h_j) (x_j^2 - x_j) - \sum_\ell p_\ell'^2 - \sum_\ell p_\ell''^2 - q^2$$

$$= f_C \cdot f_D = f_{C \cup D} - \sum_j h_j''' (x_j^2 - x_j)$$

□

5.3 Untere Schranke für Sum-of-Squares

In dieser Abschnitt beweisen wir die folgende lineare untere Schranke an den Grad einer SOS-Widerlegung.

Satz 5.5

Für alle n gibt es ein unerfüllbares lineares Gleichungssystem L über $\mathbb{F}_2$ mit n Variablen, sodass jede SOS-Widerlegung von $P_{\mathbb{F}_2} \cup \{x_i^2 - x_i \mid 1 \le i \le n\}$ Grad $\Omega(n)$ hat.

Bemerkung: Ausgehend von diesem System kann man auch zeigen, dass die Größe von SOS-Widerlegung exponentiell in der Eingabe ist und damit SOS nicht p-beschränkt ist.

Für den Beweis von Satz 5.5 verwenden wir wieder die Systeme $L_{G,\sigma}$, welche nach Satz 4.19 Grad-Rate $\Omega(n)$ haben.

Für $L = L_{\mathbb{F}_{16}}$ sei d_L die größte gerade Zahl, sodass L keine Gauß-Widerlegung vom Grad d_L besitzt. ($\Rightarrow d_L = \Omega(n)$).

Für den Beweis von Satz 5.5 zeigen wir nun, dass $P_{F_L} \cup \{x_i^2 - x_i \mid 1 \le i \le n\}$ keine Widerlegung vom Grad d_L im SOS-Kalkül besitzt.

(Satz 4.3)

Ähnlich wie in der unteren Schranke für Nullstellensatz konstruieren wir uns dazu eine Abbildung D, die jedem Polynom ein Wort aus $\mathbb{R}$ zuweist und für die gilt:

- D ist linear
- $D(1) = 1$
- $D(p^2) \ge 0$ für alle Polynome p vom Grad $\le \frac{d_L}{2}$
- $D(g_i \cdot f_{C_i}) = 0$ für alle Axiome C_i und Polynome g_i mit $\deg(g_i) + \deg(f_{C_i}) \le d_L$
- $D(h_j (x_j^2 - x_j)) = 0$ für alle Polynome h_j mit $\deg(h_j) \le d_L - 2$.

Wir betrachten zunächst wieder die Fourier-Kodierung von $L = \{ a_t + \sum_{i \in I_t} = 0 \mid 1 \le t \le m \}$

$$P_{F_L}^{\text{Fourier}} = \left\{ \prod_{i \in I_t \setminus J} \frac{1+y_i}{2} \cdot \prod_{j \in J} \frac{1-y_j}{2} \;\middle|\; \begin{array}{l} 1 \le t \le m,\ J \subseteq I_t, \\ |J| \equiv 1 - a_t \pmod 2 \end{array} \right\}$$

und zeigen:

Lemma 5.6

Es gibt eine (lineare) Abbildung $\tilde{D} : \mathbb{R}[Y_1, \dots, Y_n] \to \mathbb{R}$ mit

a) $\tilde{D}(1) = 1$

b) $\tilde{D}\left(\prod_{i \in I'} Y_i \cdot f \right) = 0$ für alle $I' \subseteq [n]$, $f \in P_{F_L}^{\text{Fourier}}$, $\deg(f) + |I'| \le d_L$.

c) $\tilde{D}\left(\prod_{i \in I'} Y_i \cdot (Y_j^2 - 1) \right) = 0$ für alle $I' \subseteq [n]$, $|I'| \le d_L - 2$, $1 \le j \le n$.

d) $\tilde{D}(p^2) \ge 0$ für alle p mit $\deg(p) \le \frac{d_L}{2}$

Beweis von Satz 5.5
(unter Verwendung von Lemma 5.6)

Ang. es gibt eine SOS-Widerlegung

$$\sum_i g_i f_{C_i} + \sum_j h_j (x_j^2 - x_j) = 1 + \sum_\ell p_\ell^2$$

vom Grad $\le d_L$. Für $f \in \mathbb{R}[X_1, \dots, X_n]$ sei $\tilde{f}$ das Polynom, in dem jedes Vorkommen

von x_i durch $\frac{1-y_i}{2}$ ersetzt wird.

Dann ist

$$\underbrace{\sum_i \tilde{g}_i \tilde{f}_{c_i} + \sum_j 4 \cdot \tilde{h}_j (y_j^2 - 1)}_{A} = \underbrace{1 + \sum_\ell \tilde{p}_\ell^2}_{B}$$

Nach Lemma 5.6 gibt es aber ein $\tilde{D} : \mathbb{R}[y_1, \dots, y_n] \to \mathbb{R}$

mit $\tilde{D}(A) = 0$ und $\tilde{D}(B) \geq 1$ ↯ □

Beweis von Lemma 5.6

Notation: $L \vdash^{d_L} \sum_{i \in I} x_i = b$ falls $\sum_{i \in I} x_i = b$ eine Ableitung der Weite d_L aus L im Gauß-Kalkül besitzt.

($\Rightarrow L \not\vdash^{d_L} 0 = 1$).

$$\tilde{D}\left(\prod_{i \in I} y_i\right) := \begin{cases} 1, & \text{falls } L \vdash^{d_L} \sum_{i \in I} x_i = 0 \\ -1, & \text{falls } L \vdash^{d_L} \sum_{i \in I} x_i = 1 \\ 0, & \text{sonst} \end{cases}$$

(Wohldefiniert, da $L \vdash^{d_L} \sum_{i \in I} x_i = 0$ & $L \vdash^{d_L} \sum_{i \in I} x_i = 1 \Rightarrow L \vdash^{d_L} 0 = 1$.)

Für nicht multilineare Terme: $\tilde{D}\left(\prod_{i \in I} y_i^{d_i}\right) := \tilde{D}\left(\prod_{\substack{i \in I, \\ d_i = 1 \pmod 2}} y_i\right)$

Beweis von Lemma 5.6 (cont.)

zu zeigen: a) – d)

a) $\widetilde{D}(1) = \widetilde{D}\left(\prod_{i \in \emptyset} y_i\right) = 1$ ✓

b) $\left(\prod_{i \in I'} y_i\right) \cdot f$

für ein $J \subseteq I_t$ mit $|J| = 1 - a_t$

$$= \left(\prod_{i \in I'} y_i\right) \cdot \prod_{i \in I_t \setminus J} \frac{1+y_i}{2} \cdot \prod_{j \in J} \frac{1-y_i}{2}$$

$$= \left(\frac{1}{2}\right)^{|I_t|} \cdot \sum_{I \subseteq I_t} (-1)^{|I \cap J|} \cdot \prod_{i \in I'} y_i \cdot \prod_{i \in I} y_i$$

$$= \left(\frac{1}{2}\right)^{|I_t|+1} \sum_{I \subseteq I_t} \left((-1)^{|I \cap J|} \cdot \prod_{i \in I'} y_i \cdot \prod_{i \in I} y_i + (-1)^{|(I_t \setminus I) \cap J|} \cdot \prod_{i \in I'} y_i \cdot \prod_{i \in I_t \setminus I} y_i \right)$$

$\underline{a_t = 0} \Rightarrow (-1)^{|I \cap J|} = -(-1)^{|(I_t \setminus I) \cap J|}$

$\underline{a_t = 1} \Rightarrow (-1)^{|I \cap J|} = (-1)^{|(I_t \setminus I) \cap J|}$

Außerdem: $L + a_t \sum_{i \in I'} y_i + \sum_{i \in I} y_i = b \iff L + a_t \underbrace{\sum_{i \in I'} y_i + \sum_{i \in I} y_i + \sum_{i \in I_t} y_i}_{= \sum_{i \in I'} y_i + \sum_{i \in I_t \setminus I} y_i} = b + a_t$

Daraus folgt:

$$(-1)^{|I\cap J|}\tilde{D}\Big(\prod_{i\in I'}y_i\cdot\prod_{i\in I}y_i\Big)+(-1)^{|(I_t\setminus I)\cap J|}\tilde{D}\Big(\prod_{i\in I'}y_i\cdot\prod_{i\in I_t\setminus I}y_i\Big)=0$$

und somit $\tilde{D}\big(\big(\prod_{i\in I'}y_i\big)\cdot f\big)=0$.

c) Folgt aus Definition

d) Sei $p=\bar{a}^T\bar{u}$ mit $\bar{u}:=\bar{u}_{n,\frac{d_t}{2}}$, $\bar{a}\in\mathbb{R}^{n^{\frac{d_t}{2}}}$

$\Rightarrow p^2=(\bar{a}^T\bar{u})^2=\bar{a}^T(\bar{u}\bar{u}^T)\bar{a}$

$\Rightarrow \tilde{D}(p^2)\neq 0$ falls $\tilde{D}(\bar{u}\bar{u}^T)\not\equiv 0$

Für Terme $\prod_{i\in I}y_i^{d_i}$ und $\prod_{j\in J}y_j^{c_j}$ vom Grad $\leq\frac{d_t}{2}$ sei

$t_1\simeq t_2 :\Leftrightarrow L\vdash^{d_t}\sum_{i\in I}x_i^{d_i \bmod 2}+\sum_{j\in J}x_j^{c_j \bmod 2}=0$ für ein $b\in\{0,1\}$

Beobachtung: $\simeq$ ist eine Äquivalenzrelation (reflexiv, transitiv, symmetrisch)

Sei S eine Menge von Termen, die aus jeder Äquivalenzklasse von $\simeq$ genau einen Term enthält.

$\Rightarrow \tilde{D}(t_1\cdot t_2)=\sum_{t\in S}\tilde{D}(t_1\cdot t)\cdot\tilde{D}(t\cdot t_2)$

Beweis von Lemma 5.6 (cont.)

Sei nun $U \in \mathbb{R}^{n^{\frac{d_L}{2}} \times |S|}$ mit

$$U_{t_n,t} = \tilde{D}(t_n \cdot t) \quad \text{für } \deg(t_n) \leq \tfrac{d_L}{2},\ t \in S.$$

Dann ist $\tilde{D}(\bar{u}\bar{u}^T) = UU^T$ und

damit $\tilde{D}(\bar{u}\bar{u}^T) \succeq 0$ nach Lemma 5.2. $\square$ (Lemma 5.6)