5. Sum-of-Squares

5.1. Einführung

Im Folgenden betrachten wir (multivariate) Polynome über $\mathbb{R}$ und nutzen die Standart-kodierung einer Klauselmenge $P_F = \{f_C \mid C \in F\}$, $\{x_j^2 - x_j \mid 1 \leq j \leq n\}$ aus Kap. 4.

Wenn es eine erfüllende Belegung $\alpha : \{x_1, \ldots, x_n\} \to \{0, 1\}$ für F gibt, dann ist $\alpha\left(\sum_{i=1}^{m} g_i \cdot f_{C_i} + \sum_{j=1}^{n} h_j (x_j^2 - x_j)\right) = 0$

für Polynome g_i, h_j.

$\Rightarrow$ Falls $\sum_{i=1}^{n} g_i f_{C_i} + \sum_{j=1}^{n} h_j (x_j^2 - x_j) > 0$ für alle Belegungen (aus $\mathbb{R}$) erhalten wir einen Wider-spruch.

Ein erster Versuch ist zu zeigen, dass

$\sum_i g_i f_{C_i} + \sum_j h_j (x_j^2 - x_j) = 1$: das ist

Nullstellensatz über R.

▶ Wenn es eine Nullstellensatzwiderlegung vom Grad d gibt, kann sie mit Hilfe eines Linearen Gleichungssystems der Größe $n^{O(d)}$ gefunden werden.

→ Die Variablen sind alle Koeffizienten der Polynome g_i, h_j (also $m \cdot O(n^d) + n \cdot O(n^d)$)

→ Die Gleichungen besagen, dass für jeden Term vom Grad $d' \leq d$ sich die Koeffizienten

- zu 0 addieren, falls $d' > 0$
- zu 1 addieren, falls $d' = 0$ (das leere Monom).

Ein zweiter Ansatz zu zeigen, dass $\sum_i g_i f_{C_i} + \sum_j h_j (x_j^2 - x_j)$ überall > 0 ist, wäre zu zeigen, dass

$$(*) \quad \sum_i g_i f_{C_i} + \sum_j h_j (x_j^2 - x_j) = 1 + p$$

wobei $p = \sum_I a_I \cdot \prod_{i \in I} x_i^2$ ein Polynom ist, das nur positive Koeffizienten $a_I \geq 0$ besitzt.

Offenbar gilt $p(x_1, \dots, x_n) \geq 0$ für alle $(x_1, \dots, x_n) \in \mathbb{R}^n$.

- Eine Widerlegung der Form ⊛ vom Grad d kann mit Hilfe eines linearen Programms der Größe $n^{O(d)}$ gefunden werden.
  - → Wie zuvor sind die Variablen Koeffizienten der Polynome g_i, h_j und p
  - → Gleichungen stellen sicher, dass die Polynome gleich sind.
  - → Zusätzlich haben wir die Bedingungen $a_I \geq 0$, was das Gleichungssystem zu einem linearen Programm macht.

Nun kommen wir zum eigentlichen Beweissystem in diesem Abschnitt.

Eine sum-of-squares (SOS) -Widerlegung vom Grad d ist eine Folge $(g_1, \ldots, g_m, h_1, \ldots, h_n, p_1, \ldots, p_s)$ von Polynomen mit

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

Hierbei ist $\deg(g_i \cdot f_{C_i}) \leq d$,

$$\deg(h_j \cdot (x_j^2 - x_j)) \leq d,$$

und $\deg(p_e) \leq \lfloor \frac{d}{2} \rfloor$.

▶ Eine SOS-Widerlegung vom Grad d kann durch ein semidefinites Programm der Größe $n^{O(d)}$ gefunden werden. (Das zeigen wir nach einer kurzen Einführung in die Thematik.)

Definition 5.1.

Eine symmetrische quadratische Matrix $M \in \mathbb{R}^{n \times n}$ ist positiv semidefinit, falls $\overline{v}^T M \overline{v} \geq 0$ für alle Spaltenvektoren $\overline{v} \in \mathbb{R}^n$. (Schreibweise $M \succeq 0$)

Lemma 5.2.

Sei $M \in \mathbb{R}^{n \times n}$ symmetrisch, dann sind die folgenden Aussagen äquivalent:

a) M ist positiv semidefinit.

b) alle Eigenwerte von M sind ≥ 0.

c) es gibt $U \in \mathbb{R}^{n \times m}$ mit $M = UU^T$

(Hier ohne Beweis.)

▶ Sei $n_{d'} := \binom{n+d'}{d'}$ die Anzahl der Terme vom Grad $\leq d'$ über n Variablen.

▶ Sei $\overline{u}_{n,d'}$ ein (eindeutiger) $n_{d'}$-dimensionaler Vektor mit allen Termen vom Grad $\leq d'$ über $\{X_1, \dots, X_n\}$.

<u>Bsp.:</u> $\overline{u}_{3,2} = (X_1X_2, X_2X_3, X_1X_3, X_1^2, X_2^2, X_3^2, X_1, X_2, X_3, 1)$.

Lemma 5.3

Sei p ein Polynom aus $\mathbb{R}[X_1, \dots, X_n]$ mit $\deg(p) = d$ und $d' := \left\lfloor \frac{d}{2} \right\rfloor$; dann sind die folgenden Aussagen äquivalent:

- $p = \sum_{\ell=1}^{s} p_\ell^2$ ist eine Summe von Quadraten,

- Es gibt eine symmetrische positiv semidefinite Matrix $M \in \mathbb{R}^{n_{d'} \times n_{d'}}$ mit
$$p = \overline{u}_{n,d'}^T \cdot M \cdot \overline{u}_{n,d'}$$

<u>Beweis:</u>

„$\Longrightarrow$" Wir haben $\deg(p_\ell) \leq d'$. Sei $\overline{a}_\ell \in \mathbb{R}^{n_{d'}}$ mit
$$p_\ell = \overline{a}_\ell^T \, \overline{u}_{n,d'}.$$

$$p = \sum_{l=1}^{s} p_l^2 = \sum_{l=1}^{s} \left(\bar{a}_l^T \bar{u}_{n,d'}\right)^2$$

$$= \sum_{l=1}^{s} \bar{u}_{n,d'}^T \bar{a}_l \bar{a}_l^T \bar{u}_{n,d'}$$

$$= \bar{u}_{n,d'}^T \left(\sum_{l=1}^{s} \bar{a}_l \bar{a}_l^T \right) \bar{u}_{n,d'}$$

$$= \bar{u}_{n,d'}^T A A^T \bar{u}_{n,d'} \quad \text{mit } A = \begin{pmatrix} | & & | \\ \bar{a}_1 & \cdots & \bar{a}_s \\ | & & | \end{pmatrix} \in \mathbb{R}^{n^{d'} \times s}$$

(AA^T symm. pos. semidef. und Lemma 5.2)

"$\Leftarrow$"

Sei $p = \bar{u}_{n,d'}^T \cdot M \cdot \bar{u}_{n,d'}$ und $M = AA^T$, $A \in \mathbb{R}^{n^{d'} \times s}$ nach Lemma 5.2.

Sei $A = \begin{pmatrix} | & & | \\ \bar{a}_1 & \cdots & \bar{a}_s \\ | & & | \end{pmatrix}$ und $p_l := \bar{a}_l^T u_{n,d'}$.

$\Rightarrow$ (wie oben) $p = \sum_{l=1}^{s} p_l^2$. $\square$

▶ Mit Lemma 5.3 folgt, dass es genau dann eine SOS-Widerlegung vom Grad d gibt, wenn es Koeffizientenvektoren $\overline{a}_1, \dots, \overline{a}_m, \overline{b}_1, \dots, \overline{b}_n \in \mathbb{R}^{n_d}$

und eine symm. pos. semidefinite Matrix $M \in \mathbb{R}^{n_{d'} \times n_{d'}}$ gibt ($d' = \lfloor \frac{d}{2} \rfloor$) mit

$$\sum_{i=1}^{m} \left(\overline{a}_i^T \overline{u}_{n,d}\right) f_{C_i} + \sum_{j=1}^{n} \left(\overline{b}_j^T \overline{u}_{n,d}\right)\left(x_j^2 - x_j\right) = 1 + \overline{u}_{n,d'}^T M \overline{u}_{n,d'} .$$

Diese Bedingung kann wieder durch lineare Gleichungen formalisiert werden.

Durch die Zusatzbedingung $M \succeq 0$ erhalten wir ein semidefinites Programm (SDP), dass ähnlich wie ein lineares Programm in Polynomialzeit gelöst werden kann.