Humboldt-Universität zu Berlin
Institut für Informatik
Lehrstuhl Logik in der Informatik
Dr. Christoph Berkholz

Version vom 04. Juli 2017

Einführung in die Beweiskomplexität

Sommersemester 2017

Übungsblatt 5

Zu bearbeiten bis 11. Juli 2017

Sei $L = \{a_t + \sum_{i \in I_t} x_i = 0 \mid 1 \leqslant t \leqslant m\}$ ein lineares Gleichungssystem über $\mathbb{F}_2$ mit $\mathrm{var}(L) = \{x_1, \ldots, x_n\}$ und $|I_t| \leqslant k$ für $1 \leqslant t \leqslant m$.

$$F_L := \Big\{ \bigvee_{i \in I_t \setminus J} x_i \vee \bigvee_{j \in J} \overline{x}_j \quad \Big| \quad 1 \leqslant t \leqslant m, J \subseteq I, |J| \equiv 1 - a_t \pmod 2 \Big\},$$

$$P_{F_L}^{\text{Fourier}} := \Big\{ \prod_{i \in I_t \setminus J} \frac{1 + y_i}{2} \cdot \prod_{j \in J} \frac{1 - y_j}{2} \quad \Big| \quad 1 \leqslant t \leqslant m, J \subseteq I, |J| \equiv 1 - a_t \pmod 2 \Big\}.$$

$$P_L^{\text{Fourier}} := \Big\{ \prod_{i \in I_t} y_i - (-1)^{a_t} \quad \Big| \quad 1 \leqslant t \leqslant m \Big\}.$$

Aufgabe 1: **(12 Punkte)**

Zeigen Sie, dass jedes Polynom $f \in P_{F_L}^{\text{Fourier}}$ eine Ableitung vom Grad höchstens $k+1$ aus $P_L^{\text{Fourier}} \cup \{y_i^2 - 1 \mid 1 \leqslant i \leqslant n\}$ im Polynomkalkül besitzt.

Aufgabe 2: **(12 Punkte)**

Zeigen Sie folgende “Umkehrung” von Lemma 4.10 aus der Vorlesung: Wenn L eine Widerlegung der Weite w im Gauß-Kalkül besitzt, dann hat $P_L^{\text{Fourier}} \cup \{y_i^2 - 1 \mid 1 \leqslant i \leqslant n\}$ eine Widerlegung vom Grad $\leqslant w + 1$ im Polynomkalkül.

Tipp: Übersetzen Sie eine lineare Gleichung der Form $a + \sum_{i \in I'} x_i + \sum_{i \in I''} x_i = 0$ in die Polynomgleichung $\prod_{i \in I'} y_i - (-1)^a \prod_{i \in I''} y_i = 0$.

Aufgabe 3: **(12 Punkte)**

Zeigen Sie, dass $4x^2 + x^2y^2 + 2xyz + y^2z^2 + z^2$ eine Summe von quadrierten Polynomen ist.

Aufgabe 4: **(12 Punkte)**

Für $k < n$ sei M die $\binom{n}{k} \times \binom{n}{k}$-Matrix mit Einträgen $M_{I,J} := |I \cap J|$ für $I, J \subseteq [n]$; $|I| = |J| = k$. Zeigen Sie, dass M positiv semidefinit ist.

Tipp: Finden Sie eine $\binom{n}{k} \times n$-Matrix U mit $M = UU^T$.