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

Version vom 20. Juni 2017

# Einführung in die Beweiskomplexität

Sommersemester 2017

## Übungsblatt 4

*Zu bearbeiten bis 26. Juni 2017*

*Bitte geben Sie die schriftlichen Lösungen der Übungsaufgaben vor der Lehrveranstaltung am 26. Juni ab. Sie dürfen die Aufgaben zu zweit bearbeiten und abgeben. Bitte beachten Sie dabei, dass jeder von Ihnen in der Lage sein muss, die Lösung aller bearbeiteten Aufgaben in der Lehrveranstaltung zu präsentieren.*

### Aufgabe 1: (12 Punkte)

Betrachten Sie folgende Variante *PCR* ("polynomial calculus with resolution") des Polynomkalküls über einem Körper $\mathbb{F}$. Für eine Klauselmenge $F$ über Variablen $x_1, \dots, x_n$ sei

$$P_F^{\mathrm{PCR}} := \Big\{ \prod_{i \in I} x_i \cdot \prod_{j \in J} \widetilde{x}_j \;\Big|\; \bigvee_{i \in I} x_i \vee \bigvee_{j \in J} \overline{x}_j \in F \Big\} \cup \Big\{ x_i^2 - x_i \;\Big|\; 1 \leqslant i \leqslant n \Big\}$$
$$\cup \Big\{ \widetilde{x}_i^2 - \widetilde{x}_i, \;\Big|\; 1 \leqslant i \leqslant n \Big\} \cup \Big\{ x_i + \widetilde{x}_i - 1 \;\Big|\; 1 \leqslant i \leqslant n \Big\}$$

eine Menge von Polynomen über den Variablen $x_1, \dots, x_n, \widetilde{x}_1, \dots, \widetilde{x}_n$. Eine *PCR-Widerlegung* von $F$ ist eine Ableitung von 1 aus $P_F$ im Polynomkalkül. Die Größe einer Ableitung ist die Größe der Kodierung aller Polynome in Monomschreibweise. Zeigen Sie, dass PCR ein Beweissystem für UNSAT ist, das Resolution p-simuliert.

### Aufgabe 2: (12 Punkte)

Sei $\mathbb{F}$ ein Körper der Charakteristik $\neq 2$. Die Fourier-Repräsentation einer Klauselmenge $F$ über $\mathbb{F}$ ist

$$P_F^{\mathrm{Fourier}} := \Big\{ \prod_{i \in I} \frac{1 - y_i}{2} \cdot \prod_{j \in J} \frac{1 + y_j}{2} \;\Big|\; \bigvee_{i \in I} y_i \vee \bigvee_{j \in J} \overline{y}_j \in F \Big\}.$$

Zeigen Sie, dass $P_F^{\mathrm{Fourier}} \cup \{ y_i^2 - 1 \mid 1 \leqslant i \leqslant n \}$ genau dann eine Widerlegung vom Grad $d$ im Polynomkalkül besitzt, wenn die Standardkodierung $\{ f_C \mid C \in F \} \cup \{ x_i^2 - x_i \mid 1 \leqslant i \leqslant n \}$ eine Widerlegung vom Grad $d$ besitzt.

*Tipp:* Substituieren Sie $y_i \leftarrow 1 - 2x_i$ bzw. $x_i \leftarrow (1 - y_i)/2$.

*— auf der nächsten Seite geht's weiter —*

**Aufgabe 3:** **(12 Punkte)**

Wenden Sie $\text{BASIS}_2$ auf $F = \left\{(xy, yz, xz, (1-x)(1-y), (1-y)(1-z), (1-x)(1-z))\right\}$ über $\mathbb{R}$ an, um eine Basis für $V_2(F)$ über $\mathbb{R}$ zu berechnen. Entscheiden Sie, ob $F$ eine Widerlegung vom Grad 2 im Polynomkalkül über $\mathbb{R}$ besitzt.

**Aufgabe 4:** **(12 Punkte)**

Zeigen Sie, dass $F = \left\{(xy, yz, xz, (1-x)(1-y), (1-y)(1-z), (1-x)(1-z))\right\}$ keine Nullstellensatzwiderlegung vom Grad 2 über $\mathbb{R}$ hat.

*Tipp:* Konstruieren Sie eine Abbildung $D$ wie im Beweis von Satz 4.3.