

Übungsblatt 4

Definition. Eine Sprache L ist in der Klasse **PP** genau dann, wenn eine randomisierte Turingmaschine M mit folgenden Eigenschaften existiert:

- M läuft auf allen Eingaben in polynomieller Zeit.
- Wenn $x \in L$, dann wird x von M mit Wahrscheinlichkeit $> \frac{1}{2}$ akzeptiert.
- Wenn $x \notin L$, dann wird x von M mit Wahrscheinlichkeit $\leq \frac{1}{2}$ akzeptiert.

Aufgabe 1. Zeigen Sie, dass wenn $L \in \mathbf{PP}$, dann auch $(\Sigma^* \setminus L) \in \mathbf{PP}$.

Aufgabe 2. MAJSAT enthält eine boolesche Formel $F(x_1, x_2, \dots, x_n)$ genau dann, wenn F in mehr als der Hälfte aller möglichen Belegungen erfüllt ist. Zeigen Sie, dass $\text{MAJSAT} \in \mathbf{PP}$.

Aufgabe 3 (Interaktive Socken). Alice hat eine rote Socke und eine grüne Socke. Bob hat eine Rot-Grün-Schwäche und glaubt Alice nicht, dass ihre Socken unterschiedliche Farben haben. Geben Sie ein interaktives Protokoll an, mit dem Alice Bob überzeugen kann, dass ihre Socken tatsächlich unterschiedliche Farben haben.

Aufgabe 4 (3-Färbbarkeit). Sei $G = (V, E)$ ein Graph, für den Alice eine 3-Färbung kennt. Sie möchte nun Bob davon überzeugen, ohne Bob die genaue 3-Färbung mitzuteilen (Zero Knowledge). Geben Sie dazu ein interaktives Protokoll an.

Aufgabe 5. Geben Sie ein einfacheres interaktives Protokoll an, das zu einer gegebenen Booleschen Formel zeigt, dass sie unerfüllbar ist.