Universität Siegen
Lehrstuhl Theoretische Informatik
Markus Lohrey und Eric Nöth



# Übungsblatt 10

**Aufgabe 1** (Miller-Rabin)**.** Lesen Sie [AB09, Kapitel 7.1,7.2.2.]). Definieren Sie die Komplexitätsklasse BPP, und fassen Sie den probabilistischen Algorithmus zum Primzahlentesten zusammen (Miller-Rabin).

**Aufgabe 2** (ZPP, RP, coRP, PP)**.** Entnehmen Sie die Definitionen der Komplexitätsklassen ZPP,RP und PP aus Wikipedia,[AB09], oder irgendeinem anderen Buch über Komplexitätstheorie.

1. Warum gilt $\mathrm{ZPP} = \mathrm{RP} \cap \mathrm{coRP}$?
2. Warum gilt $\mathrm{BPP} \subseteq \mathrm{PP}$?
3. Warum gilt $\mathrm{NP} \subseteq \mathrm{PP}$?

**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** (Zero-Knowledge Proof)**.** Im Graph 1 sei $E$ der Eingang zu einer Höhle, $A$ eine Abzweigung (die vom Eingang nicht sichtbar ist) und $B$, $C$ jeweils die Enden der Höhle. Alice behauptet, es gäbe einen Geheimgang zwischen $B$ und $C$; sie möchte nun Bob überzeugen, dass es einen Pfad zwischen $B$ und $C$ gibt, ohne dass Bob ihn erfährt und ohne dass er anschließend andere von diesem Pfad überzeugen kann (Bob hat eine Videokamera!). Wie ist das möglich (aus [QQQ$^+$89])?

## Literatur

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity - A Modern Approach*. Cambridge University Press, 2009.

[QQQ$^+$89] Jean-Jacques Quisquater, Myriam Quisquater, Muriel Quisquater, Michaël Quisquater, Louis C. Guillou, Marie Annick Guillou, Gaïd Guillou, Anna Guillou, Gwenolé Guillou, Soazig Guillou,

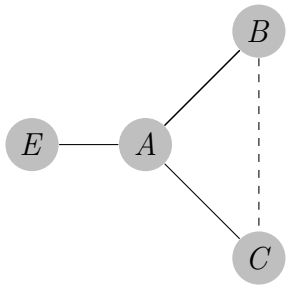


Abbildung 1: Eine Höhle.

and Thomas A. Berson. How to explain zero-knowledge protocols to your children. In *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, pages 628–631, 1989.