Institut für Informatik
Prof. Dr. J. Rothe

Sommersemester 2024
Übungsblatt 7

Übung zur Vorlesung

Kryptokomplexität II

Bearbeitungszeit: 21. Mai bis 31. Mai
Verantwortlich: Roman Zorn

Begründen Sie Ihre Antworten und bereiten Sie sie so vor, dass Sie sie in der Übung präsentieren können.

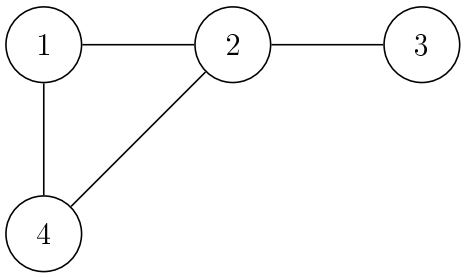
Aufgabe 1: Break-Rabin Orakel

Führen Sie den Algorithmus Random-Factor$^{\text{break-rabin}}$ durch um die Primfaktoren von $n = 161393$ zu bestimmen. Wählen Sie dabei $x = 16$.

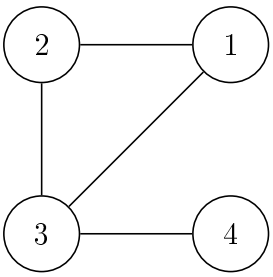
Hinweis: Das Orakel sagt 105436.

Aufgabe 2: Graphisomorphismen

Betrachten Sie die folgenden Graphen G, H:



(a) G



(b) H

(a) ▶ Geben Sie Iso(G, H) an.

(b) ▶ Zeigen oder widerlegen Sie: Für einen Graphen $G = (\{1, ..., n\}, E)$ gilt

$[\text{Aut}(G) = \mathfrak{S}_n] \Rightarrow G$ ist ein vollständiger Graph, oder hat keine Kanten (leerer Graph).

Aufgabe 3: Graph Auto- und Isomorphie

Sei $G = (V, E)$ ein ungerichteter Graph. Wir bezeichnen den Komplementgraph von G mit $\bar{G} = (V, \bar{E})$, wobei $\bar{E} = \{\{u, v\} \mid u \neq v, \{u, v\} \notin E\}$.

(a) ▶ Zeigen Sie $\textsc{Aut}(G) = \textsc{Aut}(\bar{G})$.

(b) ▶ Widerlegen Sie: Für einen Graphen $G = (V, E)$ gilt

$$G \text{ ist nicht zusammenhängend} \iff \bar{G} \text{ ist zusammenhängend.}$$

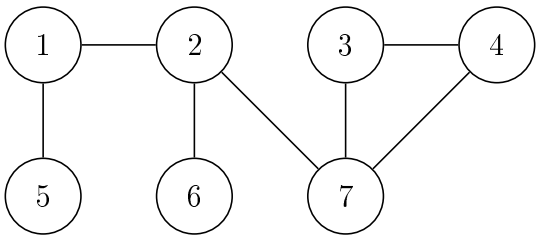
▶ Gilt wenigstens eine der beiden Richtungen? Beweisen Sie.

Aufgabe 4: Zero-Knowledge-Protokoll für Graph-Isomorphie

Betrachten Sie das Zero-Knowledge-Protokoll von Goldreich, Micali und Widgerson zum Graph-Isomorphie-Problem. Gegeben seien die Permutationen

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 3 & 7 & 1 & 5 & 6 \end{pmatrix}, \mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 3 & 6 & 2 & 7 & 5 \end{pmatrix}$$

und der Graph G_0



▶ Führen Sie das Protokoll mit den Werten $m = 0$ und $a = 1$ und dem Graphen G_0 durch. Geben Sie dabei alle relevanten Zwischenschritte an.