Institut für Informatik
Prof. Dr. J. Rothe

Sommersemester 2024
Übungsblatt 7

Lösungsvorschläge

Kryptokomplexität II

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

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.

Lösungsvorschlag: Wir wählen $x = 16 \in \mathbb{Z}_n^*$.

$$c = x^2 \equiv 256 \mod 161393$$
$$m = \text{BREAK-RABIN}(\langle 161393, 256 \rangle)$$

BREAK-RABIN gibt ein m zurück mit $c = m^2 \mod n$, mögliche m sind hier also

$$m_1 \equiv 16 \mod n, \quad m_2 \equiv -16 \mod n,$$

$$m_3 \equiv 105436 \mod n, \quad m_4 \equiv -105436 \mod n.$$

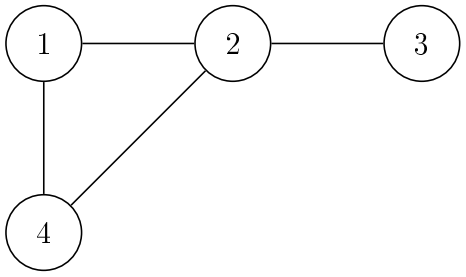
Die trivialen Fälle m_1 und m_2 führen zu einem Fehler und Programmabbruch.
Für $m_3 = 105436$ wird berechnet:

$$\begin{aligned} p &= \text{ggT}\,(m - x, n) = \text{ggT}\,(105436 - 16, 161393) \\ &= \text{ggT}\,(105420, 161393) = 251 \\ q &= \frac{n}{p} = \frac{161393}{251} = 643 \end{aligned}$$

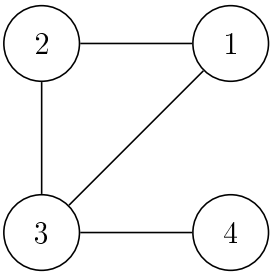
Aufgabe 2: Graphisomorphismen

Betrachten Sie die folgenden Graphen G, H:

(a) ▶ Geben Sie ISO(G, H) an.



(a) G



(b) H

Lösungsvorschlag: Es gilt, dass $\pi(2) = 3$ sein muss, da nur Knoten 2 in G und 3 in H den Grad drei besitzen. Ähnliches gilt für $\pi(3) = 4$ wegen Knotengrad 1.

Die einzigen verbleibenden Permutationen sind $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ und $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$.

(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).

Lösungsvorschlag: Für G sind **alle** Permutationen $\pi \in \mathfrak{S}_n$ auch Automorphismen. D.h. für jede Permutation $\pi \in \mathfrak{S}_n$ gilt

$$\{i, j\} \in E(G) \iff \{\pi(i), \pi(j)\} \in E(G).$$

Wir können im folgenden o.B.d.A. annehmen, dass $|V(G)| \geq 3$, denn für $|V(G)| \leq 2$ gilt die Aussage trivialerweise, weil diese Graphen immer vollständig oder leer sind.

Beweis per Widerspruch: Angenommen $\text{AUT}(G) = \mathfrak{S}_n$ aber der Graph ist nicht vollständig oder leer. Dann gibt es drei Knoten $a, b, c \in V(G)$ mit $\{a, b\} \in E(G)$ aber $\{b, c\} \notin E(G)$. Betrachte nun eine Permutation $\pi' \in \mathfrak{S}_n$, mit $\pi'(a) = b, \pi'(b) = c, \pi'(c) = a$. Nun gilt $\{a, b\} \in E(G)$ aber $\{\pi'(a), \pi'(b)\} = \{b, c\} \notin E(G)$. Also ist $\pi' \notin \text{AUT}(G)$ und somit $\text{AUT}(G) \neq \mathfrak{S}_n$, was ein Widerspruch zur Annahme ist.

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 $\textsc{Aut}(G) = \textsc{Aut}(\bar{G})$.

Lösungsvorschlag:

$$\begin{aligned}
\pi \in \textsc{Aut}(G) &\iff [\forall i,j \in V, i \neq j : \{i,j\} \in E \iff \{\pi(i),\pi(j)\} \in E] \\
&\iff [\forall i,j \in V, i \neq j : \{i,j\} \notin E \iff \{\pi(i),\pi(j)\} \notin E] \\
&\overset{\text{Def. } \bar{E}}{\iff} [\forall i,j \in V, i \neq j : \{i,j\} \in \bar{E} \iff \{\pi(i),\pi(j)\} \in \bar{E}] \\
&\overset{\bar{G}=(V,\bar{E})}{\iff} \pi \in \textsc{Aut}(\bar{G})
\end{aligned}$$

(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.

Lösungsvorschlag: Es gilt tatsächlich

$$G \text{ ist nicht zusammenhängend} \Rightarrow \bar{G} \text{ ist zusammenhängend,}$$

aber **nicht** die Rückrichtung.

Zunächst zeigen wir

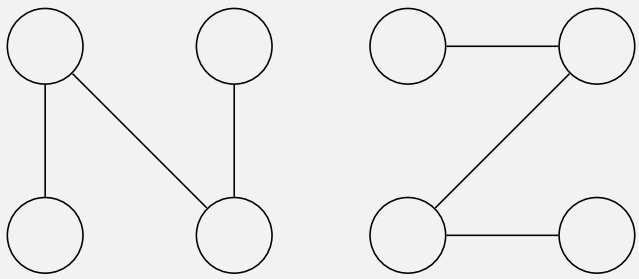
$$G \text{ ist nicht zusammenhängend} \Rightarrow \bar{G} \text{ ist zusammenhängend.}$$

Angenommen G ist nicht zusammenhängend und es gibt mehrere Zusammenhangskomponenten $Z_1, ..., Z_k \subset V$ mit $k \geq 2$. In $\bar{G}$ ist nun jeder Knoten $v \in Z_i$ mit jedem Knoten aus Z_j mit $j \neq i$ verbunden. Die einzigen Knoten, zu denen v nicht direkt verbunden ist, sind andere Knoten aus Z_i. Aber zu diesen Knoten gibt es dann einen Pfad über einen Knoten aus Z_j. Also ist $\bar{G}$ zusammenhängend.

Jetzt zeigen wir

$$G \text{ ist nicht zusammenhängend} \not\Leftarrow \bar{G} \text{ ist zusammenhängend.}$$

Dazu genügt ein Gegenbeispiel: Links ist G und rechts $\bar{G}$. Offenbar sind beide Zusammenhängend.

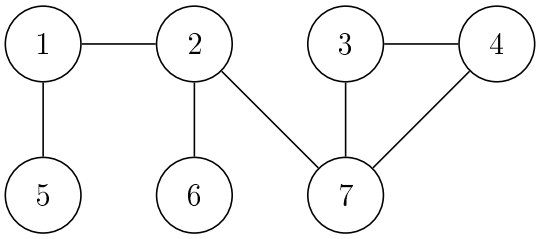


Aufgabe 4: Zero-Knowledge-Protokoll für Graph-Isomorphie

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

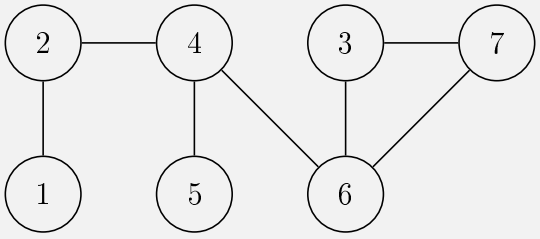
$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 3 & 7 & 1 & 5 & 6 \end{pmatrix}, \mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 3 & 6 & 2 & 7 & 5 \end{pmatrix}$$

und der Graph G_0



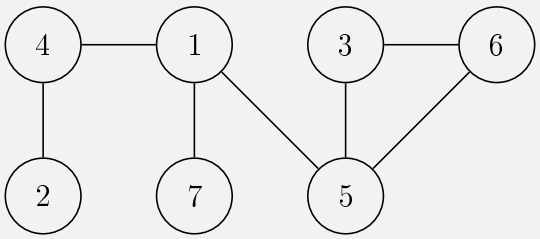
▶ Führen Sie das Protokoll mit den Werten $m = 0$ und $a = 1$ und dem Graphen G_0 durch. Geben Sie dabei alle relevanten Zwischenschritte an.

Lösungsvorschlag:
Schritt 1: Bestimme $G_1 = \pi(G)$.



Schritt 2: Merlin versendet (G_0, G_1) an Arthur.

Schritt 3: Merlin berechnet $H = \mu(G_m) = \mu(G_0)$:



Schritt 4: Merlin versendet H an Arthur.

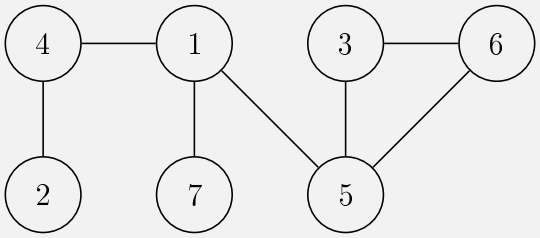
Schritt 5+6: Arthur bittet Merlin um ein $\alpha \in \text{Iso}(G_a, H) = \text{Iso}(G_1, H)$

Schritt 7: Da $m = 0 \neq a = 1$ berechnet Merlin $\alpha = \pi^{-1}\mu$.Es gilt

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

Schritt 8: Merlin sendet α an Arthur.

Schritt 9: Arthur verifiziert $\alpha(G_1) = H$:



Arthur akzeptiert.