Theoretische Informatik I

Übungsblatt 5: Abbildungen

Duale Hochschule Baden-Württemberg – Lörrach
Studiengang Informatik – TIF21

N, ν – Ny Ξ, ξ – Xi O, o – Omikron

1. In dieser Aufgabe seien

$$f : [0,1] \to [3,5]$$
$$x \mapsto 2 \cdot x + 3$$

und

$$g : [3,5] \to [0,1]$$
$$x \mapsto \frac{x-3}{2}.$$

Zeigen oder widerlegen Sie: f und g sind invers zueinander.

Lösung:
Wir wollen zeigen, dass f und g invers zueinander sind.
Also müssen wir zeigen: $g \circ f = id_{[0,1]}$ und $f \circ g = id_{[3,5]}$.

- Wir wollen zunächst zeigen, dass $g \circ f = id_{[0,1]}$ gilt.
  Dazu wollen wir zeigen, dass für alle $m \in [0,1]$ gilt: $(g \circ f)(m) = id_{[0,1]}(m)$.

  Sei $a \in [0,1]$.
  Wir müssen zeigen: $(g \circ f)(a) = id_{[0,1]}(a)$.

  Es gilt $(g \circ f)(a) = g(f(a)) = g(2 \cdot a + 3) = \frac{2 \cdot a + 3 - 3}{2} = \frac{2 \cdot a}{2} = a = id_{[0,1]}(a)$,
  also gilt $(g \circ f)(a) = id_{[0,1]}(a)$.

  Damit haben wir gezeigt, dass für alle $m \in [0,1]$ gilt: $(g \circ f)(m) = id_{[0,1]}(m)$.
  Damit haben wir gezeigt, dass $g \circ f = id_{[0,1]}$ gilt.

- Nun wollen wir zeigen, dass $f \circ g = id_{[3,5]}$ gilt.
  Dazu wollen wir zeigen, dass für alle $m \in [3,5]$ gilt: $(f \circ g)(m) = id_{[3,5]}(m)$.

  Sei $a \in [3,5]$.
  Wir müssen zeigen: $(f \circ g)(a) = id_{[3,5]}(a)$.

  Es gilt $(f \circ g)(a) = f(g(a)) = f(\frac{a-3}{2}) = 2 \cdot \frac{a-3}{2} + 3 = a - 3 + 3 = a = id_{[3,5]}(a)$,
  also gilt $(f \circ g)(a) = id_{[3,5]}(a)$.

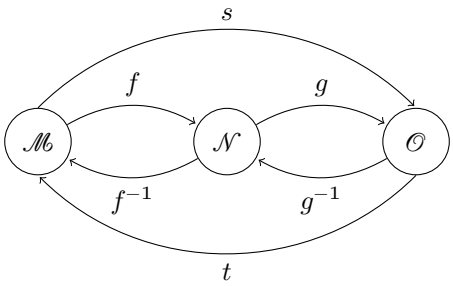
  Damit haben wir gezeigt, dass für alle $m \in [3,5]$ gilt: $(f \circ g)(m) = id_{[3,5]}(m)$.
  Damit haben wir gezeigt, dass $f \circ g = id_{[3,5]}$ gilt.

Also haben wir $g \circ f = id_{[0,1]}$ und $f \circ g = id_{[3,5]}$ gezeigt.

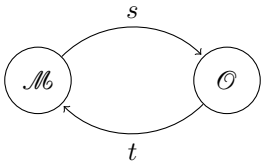
Damit haben wir gezeigt, dass f und g invers zueinander sind.

2. Seien $f : \mathscr{M} \to \mathscr{N}, g : \mathscr{N} \to \mathscr{O}$ invertierbar.
Zeigen oder widerlegen Sie: $g \circ f$ ist invertierbar und $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Lösung:
Wir setzen zum besseren Verständnis $s := g \circ f$ und $t := f^{-1} \circ g^{-1}$.
(Damit haben wir Abbildungen $s : \mathscr{M} \to \mathscr{O}$ und $t : \mathscr{O} \to \mathscr{M}$.)
Zur Illustration ein Bild der vorliegenden Situation:



Zu zeigen ist also: s ist invertierbar und $s^{-1} = t$.



Also müssen wir zeigen: $t \circ s = id_{\mathscr{M}}$ und $s \circ t = id_{\mathscr{O}}$.
Da wir wissen, dass f und g invertierbar sind, wissen wir:

$$\begin{aligned} f^{-1} \circ f &= id_{\mathscr{M}} \quad (1), \\ f \circ f^{-1} &= id_{\mathscr{N}} \quad (2). \\ g^{-1} \circ g &= id_{\mathscr{N}} \quad (3), \\ g \circ g^{-1} &= id_{\mathscr{O}} \quad (4). \end{aligned}$$

Wir sehen einerseits

$$t \circ s = (f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f \overset{(3)}{=} f^{-1} \circ (id_{\mathscr{N}}) \circ f = f^{-1} \circ f \overset{(1)}{=} id_{\mathscr{M}},$$

also

$$t \circ s = id_{\mathscr{M}},$$

und andererseits

$$s \circ t = (g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} \overset{(2)}{=} g \circ (id_{\mathscr{N}}) \circ g^{-1} = g \circ g^{-1} \overset{(4)}{=} id_{\mathscr{O}},$$

also

$$s \circ t = id_{\mathscr{O}}.$$

Also ist s invertierbar und $s^{-1} = t$.
Also ist $g \circ f$ invertierbar und $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Dies war zu zeigen.

3. Anwendungen

(a) Herr Dr. Bröhrmeier arbeitet an einem Kompressionsverfahren, mit dem sich jede Datei verkleinern und aus der komprimierten Datei wiederherstellen lässt. Bitte helfen Sie ihm.

Lösung:
Versuchen Sie ihn zu überzeugen, dass sein Vorhaben Unsinn ist. Ein solches Verfahren muss eine injektive Abbildung modellieren, andernfalls kann eine Datei nicht mehr wiederhergestellt werden. Betrachten wir die Menge aller Dateien, die genau aus n Bit bestehen. Ein solches Kompressionsverfahren muss jede dieser Dateien auf eine Datei mit höchstens $n-1$ Bit abbilden. Es gibt 2^n Dateien mit n Bit, aber nur $\sum_{k=0}^{n-1} 2^k = 2^n - 1$ Dateien mit höchstens $n-1$ Bit. Das Verfahren kann nicht injektiv sein (wir haben hier noch nicht einmal berücksichtigt, wohin Dateien mit weniger als n Bit abgebildet werden sollten).

Falls Sie jemandem, der nichts von Injektivität weiß, die Aussichtslosigkeit eines solchen Verfahrens erklären möchten, können Sie wie folgt argumentieren: Wähle drei verschiedene Dateien D_1, D_2, D_3 mit je n Bit. Komprimiere jede so oft, bis die komprimierte Datei nur noch aus 1 Bit besteht (dies ist nach höchstens $n-1$ Schritten der Fall). Falls ohne Einschränkung D_1 auf 0 und D_2 auf 1 abgebildet wird, dann ist für D_3 nichts mehr übrig.

(b) Für kryptographische Zwecke wird häufig eine Abbildung $\{0,1\}^* \to \{0,1\}^{160}$ verwendet, bei der die Forderung erhoben wird, dass zwei verschiedene Texte (Bitströme) nicht auf denselben Wert abgebildet werden. Ist dies eine sinnvolle Forderung?

Falls ja, geben Sie kurz an, wie eine solche Hashfunktion aussehen könnte.

Falls nein, geben Sie an, wieso dann diese Forderung erhoben wird.

Lösung:
Die Forderung verlangt die Injektivität der Abbildung. Da aber $\{0,1\}^{161} \subseteq \{0,1\}^*$ und $|\{0,1\}^{161}| = 2^{161} > 2^{160} = |\{0,1\}^{160}|$ gilt, kann eine solche Abbildung niemals injektiv sein. Die Forderung bezieht sich denn auch eher auf die Praxis als die Theorie. Wenn Sie sich vergegenwärtigen, wie groß die Zahl 2^{160} ist, dann sehen Sie vielleicht ein, dass es auf Erden niemals so viele verschiedene Texte geben wird – zumindest nicht innerhalb der nächsten Jahrmillionen. Eine Hashfunktion soll einen Text auf einen mehr oder weniger willkürlichen Wert abbilden. Die Wahrscheinlichkeit, dass dann zwei zufällige Texte denselben Wert erhalten, soll kleiner sein als die Wahrscheinlichkeit, dass der Inhalt einer Tasse Kaffe plötzlich aus der Tasse tunnelt (dieses Beispiel dient lediglich der Illustration, ich habe das nicht nachgerechnet).