Formale Grundlagen der Informatik I
2. Übungsblatt

Fachbereich Mathematik
Prof. Dr. Martin Ziegler
Davorin Lešnik, Ph.D.
Carsten Rösnick

Sommersemester 2013
22. 04. 2013

Gruppenübung

Aufgabe G4 (Stern-Operation)
L und M seien Σ-Sprachen.

(a) Zeigen Sie, dass $L \subseteq L^*$ und $\big(L \subseteq M^* \implies L^* \subseteq M^*\big)$.

(b) Schließen Sie aus (a), dass $(L^*)^* = L^*$ und $\big(L \subseteq M \implies L^* \subseteq M^*\big)$.

(c) Zeigen Sie, dass $(L \cup M)^* = (L^*M^*)^*$.

Lösung:

(a) Wir erinnern uns an die Definition des Stern-Operators:

$$L^* = \{l_1 \cdot \ldots \cdot l_n \mid l_1, \ldots, l_n \in L, n \in \mathbb{N}\}\,.$$

Für $n = 0$ heißt das, dass $\varepsilon \in L^*$, und für $n = 1$, dass $L = \{l_1 \mid l_1 \in L\} \subseteq L^*$.
Nehmen wir jetzt an, dass $L \subseteq M^*$, und sei $l \in L^*$. Das heißt, dass es ein $n \in \mathbb{N}$ und $l_1, \ldots, l_n \in L$ gibt, so dass sich l als $l = l_1 \cdot \ldots \cdot l_n$ schreiben lässt. Da $L \subseteq M^*$ ist jedes l_i Element von M^* und kann deshalb als $l_i = m_{i,1} \cdot \ldots \cdot m_{i,k_i}$ für bestimme $k_1, \ldots, k_n \in \mathbb{N}$ geschrieben werden. Deshalb ist

$$l = \underbrace{\big(m_{1,1} \cdot \ldots \cdot m_{1,k_1}\big)}_{=l_1} \cdot (\ldots) \cdot \underbrace{\big(m_{n,1} \cdot \ldots \cdot m_{n,k_n}\big)}_{=l_n} \in M^*.$$

Damit gilt $L \subseteq M^* \implies L^* \subseteq M^*$.

(b) Zur ersten Aussage: Mit der ersten Aussage aus (a) folgt zunächst $(L^*) \subseteq (L^*)^*$. Für die verbleibende Inklusion, $(L^*)^* \subseteq (L^*)$, nutzen wir die zweite Aussage aus (a): $\big((L^*) \subseteq L^*\big) \implies \big((L^*)^* \subseteq L^*\big)$.
Zur zweiten Aussage: Aus $L \subseteq M$ folgt, dass $L \subseteq M \subseteq M^*$ und (mit (a)) $L^* \subseteq M^*$.

(c) $(L \cup M)^* \subseteq (L^*M^*)^*$: es genügt zu beweisen, dass $L \cup M \subseteq L^*M^*$. Sei deshalb $w \in L \cup M$. Dann gilt $w \in L$ oder $w \in M$. Nehmen wir erst an, dass $w \in L$. Dann auch $w \in L^*$, und $w = w \cdot \varepsilon \in L^*M^*$. Der Fall $w \in M$ geht analog.
$(L^*M^*)^* \subseteq (L \cup M)^*$: es genügt zu beweisen, dass $L^*M^* \subseteq (L \cup M)^*$. Aus $L \subseteq L \cup M \subseteq (L \cup M)^*$ folgt, dass $L^* \subseteq (L \cup M)^*$. Analog gilt auch $M^* \subseteq (L \cup M)^*$, woraus $L^*M^* \subseteq (L \cup M)^*$ folgt. (Hier haben wir das folgende Prinzip verwendet:

$$L \subseteq N^*, M \subseteq N^* \implies LM \subseteq N^*.$$

Beweis: nehmen wir an $L \subseteq N^*$ und $M \subseteq N^*$, und sei $w \in LM$. Letztes heißt, dass $w = lm$ mit $l \in L$ und $m \in M$. Weil $L \subseteq N^*$ und $M \subseteq N^*$, können wir $l = n_1 \cdot \ldots n_j$ und $m = n'_1 \cdot \ldots n'_k$ schreiben mit $n_i, n'_i \in N$. Deshalb $w = n_1 \cdot \ldots n_j \cdot n'_1 \cdot \ldots n'_k \in N^*$.)

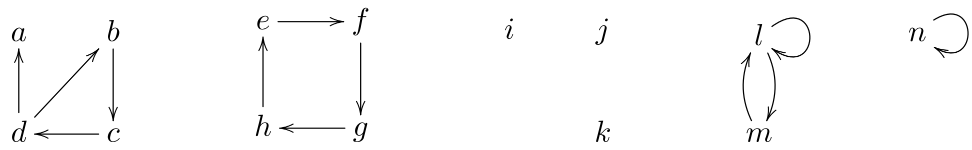
Aufgabe G5 (Wahrheitswertetafeln)
Zeigen Sie anhand von Wahrheitswertetafeln, dass die folgenden aussagenlogischen Formeln äquivalent sind:

$$\neg(p \to q), \qquad p \wedge \neg q, \qquad (p \vee q) \wedge \neg q.$$

Lösung:

p	q	$p \to q$	$\neg(p \to q)$	$\neg q$	$p \wedge \neg q$	$p \vee q$	$(p \vee q) \wedge \neg q$
0	0	1	0	1	0	0	0
0	1	1	0	0	0	1	0
1	0	0	1	1	1	1	1
1	1	1	0	0	0	1	0

Aufgabe G6 (Graphhomomorphismen)
Ein *gerichteter Graph* $G = (V, E)$ besteht aus einer endlichen Menge V von Knoten und einer Teilmenge $E \subseteq V \times V$ von Kanten. Gegeben seien die folgenden fünf gerichteten Graphen:



G_1 G_2 G_3 G_4 G_5

Der Graph $G_1 = (V_1, E_1)$ ist beispielsweise wie folgt formal gegeben:

$$V_1 = \{a, b, c, d\}$$
$$E_1 = \{(d, a), (d, b), (b, c), (c, d)\}$$

Geben Sie an, zwischen welchen der Graphen Homomorphismen existieren, und geben Sie auch gegebenenfalls einen Homomorphismus an.

Lösung: Zur Erinnerung: Ein Homomorphismus zwischen zwei Graphen $G = (V, E), G' = (V', E')$ ist eine Abbildung $\varphi\colon V \to V'$, für die gilt

$$(x, y) \in E \implies (\varphi(x), \varphi(y)) \in E'. \tag{1}$$

- Von dem Graphen G_3 gibt es Homomorphismen in alle anderen Graphen. Das liegt daran, dass G_3 keine Kanten enthält, die Bedingung (1) damit immer wahr ist und für φ eine beliebige Abbildung gewählt werden kann. Z.B. wäre ein Homomorphismus von G_3 zu G_1 die Abbildung $\varphi\colon V_3 \to V_1$ mit $\varphi(x) = a$.

  Es gibt keinen Homomorphismus in den Graphen G_3, denn jeder andere Graph besitzt mindestens eine Kante, die nach (1) wieder auf eine Kante in G_3 abgebildet werden müsste.
- G_1, G_2: Angenommen es gäbe einen Homomorphismus φ von G_1 nach G_2. Da G_2 symmetrisch ist, dürfen wir ohne Beschränkung der Allgemeinheit annehmen, dass $\varphi(b) = f$ gilt. Da $(b, c) \in E_1$, müsste auch $\varphi(c) = g$ gelten und damit auch $\varphi(d) = h$. Da $(d, b) \in E_1$ müsse jetzt auch $(h, f) \in E_2$. Das ist aber nicht der Fall. Also existiert ein solcher Homomorphismus nicht.

  Ähnlich kann man auch sehen, dass es keinen Homomorphismus von G_2 nach G_1 gibt.
- G_1 nach G_4: Setze $\varphi(a) = \varphi(b) = \varphi(d) = l$, $\varphi(c) = m$.
- G_2 nach G_4: Setze $\varphi(e) = \varphi(f) = \varphi(g) = l$, $\varphi(h) = m$.

- G_4 nach G_5: Setze $\varphi(l) = \varphi(m) = n$.
- G_4, G_5 nach G_1, G_2: Sowohl G_1 als auch G_2 enthalten keine Schleifen. Deswegen kann es keinen Homomorphismus von G_4 oder G_5 nach G_1 oder G_2 geben.
- G_5 nach G_4: Setze $\varphi(n) = l$.

Alle anderen Aussagen (beispielsweise die Existenz eines Homomorphismus von G_1 nach G_5) folgen per Transitivität aus den obigen.

Hausübung

Aufgabe H3 (Äquivalenzrelationen, Injektivität, Surjektivität, Bijektivität) (6 Punkte)
Sei $f\colon A \to B$ eine beliebige Abbildung.

(a) Sei auf A durch

$$x \sim y :\Leftrightarrow f(x) = f(y)$$

für $x, y \in A$ die Relation $\sim$ definiert. Zeigen Sie, dass $\sim$ eine Äquivalenzrelation ist.

(b) Sei $q\colon A \to A/{\sim}$ durch $q(x) := [x]_\sim$ definiert. Zeigen Sie, dass q eine surjektive Abbildung ist.

(c) Zeigen Sie, dass die Inklusionsabbildung $i\colon \text{Bild}(f) \to B$, $i(x) := x$, injektiv ist.

(d) Sei durch $\overline{f}([x]) := f(x)$ eine Abbildung $\overline{f}\colon A/{\sim} \to \text{Bild}(f)$ definiert. Zeigen Sie, dass $\overline{f}$ wohldefiniert ist und dass sie bijektiv ist.

(e) Schließen Sie, dass sich jede Abbildung als eine Verkettung einer surjektiven, bijektiven und injektiven Abbildung darstellen lässt.

Lösung:

(a) $\boxed{\text{1 P.}}$ Reflexivität von $\sim$ bedeutet $f(x) = f(x)$, Symmetrie bedeutet $f(x) = f(y) \implies f(y) = f(x)$ und Transitivität bedeutet $f(x) = f(y) \land f(y) = f(z) \implies f(x) = f(z)$ für alle $x, y, z \in A$. Also folgen alle diese Eigenschaften für $\sim$ aus diesen Eigenschaften für $=$.

(b) $\boxed{\text{1 P.}}$ Die Elemente von $A/{\sim}$ sind genau die Äquivalenzklassen $[x]_\sim$, wo $x \in A$. Um Surjektivität von q zu zeigen, müssen wir für jedes solche $[x]_\sim$ ein Element aus A finden, das mit q zu $[x]_\sim$ abgebildet wird. Das haben wir, denn $q(x) = [x]_\sim$.

(c) $\boxed{\text{1 P.}}$ Injektivität einer Funktion g bedeutet $g(x) = g(y) \implies x = y$ für alle x, y. Für i bekommen wir die Bedingung $x = y \implies x = y$, was natürlich stimmt.

(d) $\boxed{\text{1 P.}}$ Wohldefiniertheit einer Funktion bedeutet, dass jedes Element genau zu einem Element abgebildet wird. In unserem Fall heißt das, dass für alle $[x]_\sim, [y]_\sim \in A/{\sim}$ mit $[x]_\sim = [y]_\sim$ gilt $\overline{f}([x]_\sim) = \overline{f}([y]_\sim)$. Wir können so folgern:

$$[x]_\sim = [y]_\sim \implies x \sim y \implies f(x) = f(y) \implies \overline{f}([x]_\sim) = \overline{f}([y]_\sim).$$

$\boxed{\text{1 P.}}$ Beachte, dass alle diese Implikationen eigentlich Äquivalenzen sind, also haben wir auch die Implikation in die andere Richtung $\overline{f}([x]_\sim) = \overline{f}([y]_\sim) \implies [x]_\sim = [y]_\sim$ und somit ist $\overline{f}$ injektiv.

Für beliebiges Element $b \in \text{Bild}(f)$ existiert nach Definition des Bildes ein $x \in A$ mit $f(x) = b$. Das heißt $\overline{f}([x]_\sim) = b$ und somit ist $\overline{f}$ surjektiv.

(e) $\boxed{\text{1 P.}}$ Für beliebiges $x \in A$ haben wir

$$i\Big(\overline{f}\big(q(x)\big)\Big) = i\Big(\overline{f}\big([x]_\sim\big)\Big) = i\big(f(x)\big) = f(x).$$

Also kann jede beliebige Funktion $f\colon A \to B$ als Verkettung $f = i \circ \overline{f} \circ q$ geschrieben werden, wo q surjektiv, $\overline{f}$ bijektiv und i injektiv ist.

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "q", "\text{surj.}"'] & B \\
A/\sim \arrow[r, "\overline{f}", "\text{bij.}"'] & \mathrm{Bild}(f) \arrow[u, "i", "\text{inj.}"']
\end{tikzcd}$$

Aufgabe H4 (4 Punkte)

Sei $\Sigma := \{a, b\}$.

(a) Sei L_1 die kleinste Sprache über Alphabet Σ, für die gilt:
- $aaaababa \in L_1$,
- wenn das Wort aw ($w \in \Sigma^*$) zu L_1 gehört, so auch $w \in L_1$,
- wenn das Wort wa ($w \in \Sigma^*$) zu L_1 gehört, so auch $w \in L_1$.

Geben Sie alle Wörter in der Sprache L_1 an.

(b) Sei noch eine Sprache L_2 definiert durch $w \in L_2 \iff ww \in L_1$. Geben Sie L_2, $L_1 \cup L_2$ und $L_1 \cdot L_2$ an.

Lösung:

(a) $\boxed{\text{1 P.}}$ Die Wörter in L_1 sind genau die, die man aus $aaaababa$ so bekommen kann, dass man ein paar a am Anfang und/oder am Ende löscht. Also

$$L_1 = \{aaaababa, aaababa, aababa, ababa, baba, aaaabab, aaabab, aabab, abab, bab\}.$$

(b) $\boxed{\text{1 P.}}$ $L_2 = \{ba, ab\}$

$\boxed{\text{1 P.}}$

$$L_1 \cup L_2 = \{aaaababa, aaababa, aababa, ababa, baba, aaaabab, aaabab, aabab, abab, bab, ba, ab\}$$

$\boxed{\text{1 P.}}$

$$\begin{aligned} L_1 \cdot L_2 = \{&aaaabababa, aaabababa, aababababa, abababa, bababa,\\ &aaaababba, aaababba, aababba, ababba, babba,\\ &aaaababaab, aaababaab, aababaab, ababaab, babaab,\\ &aaaababab, aaababab, aababab, ababab, babab\} \end{aligned}$$

Minitest

Aufgabe M4

Sei $\Sigma = \{a, b, c\}$. Die Relation $R_1 = \{(v, w) \in \Sigma^* \times \Sigma^* \mid v \text{ ist Präfix von } w\}$ ist

- ☐ reflexiv
- ☐ symmetrisch
- ☐ transitiv

Lösung:

- ☒ reflexiv
- ☐ symmetrisch

☒ transitiv

Reflexiv, da jedes Wort Präfix von sich selbst ist.
Nicht symmetrisch, denn jedes (nicht leere) Wort $a \in \Sigma^*$ ist Präfix von $a \cdot a$, aber nicht umgekehrt.
Transitiv, denn wenn u Präfix von v und v Präfix von w ist, dann gilt per Definition $v = u \cdot v'$ für ein Wort v' und $w = v \cdot w'$ für ein Wort w'. Zusammen also $w = u \cdot v' \cdot w'$ und damit ist u auch Präfix von w.

Aufgabe M5
Die Relation $R_2 = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \cdot b \neq 0\}$ ist

☐ reflexiv

☐ symmetrisch

☐ transitiv

Lösung:

☐ reflexiv

☒ symmetrisch

☒ transitiv

Nicht reflexiv: $(0, 0) \notin R_2$. Symmetrie und Transitivität folgen aus der Beobachtung, dass $(a, b) \in R_1$ genau dann, wenn $a \neq 0$ und $b \neq 0$.

Aufgabe M6
Seien A und B endliche Mengen und $f\colon A \to B$ eine Funktion.

(a) Ist f injektiv, so folgt stets
 ☐ $|A| \leq |B|$
 ☐ $|A| \geq |B|$

(b) Ist f surjektiv, so folgt stets
 ☐ $|A| \leq |B|$
 ☐ $|A| \geq |B|$

Lösung:

(a) ☒ $|A| \leq |B|$
 ☐ $|A| \geq |B|$
 Wenn f injektiv ist, dann gibt es für jedes $y \in B$ maximal ein $x \in A$, so dass $f(x) = y$. Damit kann es nicht mehr Elemente in A geben als in B.

(b) ☐ $|A| \leq |B|$
 ☒ $|A| \geq |B|$
 Wenn f surjektiv ist, dann gibt es für jedes $y \in B$ mindestens ein $x \in A$, so dass $f(x) = y$. Damit kann A nicht weniger Elemente als B enthalten.