Grundbegriffe der Informatik — Aufgabenblatt 2
Lösungsvorschläge

Tutorium Nr.:		Tutor*in:	
Matr.nr. 1:			
Nach-,Vorname 1:		,	
Matr.nr. 2:			
Nach-,Vorname 2:		,	

Ausgabe: 29. Oktober 2020, 12:00 Uhr

Abgabe: 05. November 2020, 12:30 Uhr
in dem Holzkasten neben dem Raum -119
im UG des Info-Gebäudes (50.34)

Lösungen werden nur korrigiert, wenn sie
- handschriftlich erstellt sind (Tablet-Ausdruck erlaubt) und
- mit dieser Seite als Deckblatt
- in der oberen **linken** Ecke zusammengeheftet

rechtzeitig abgegeben werden.

Abgaberegeln für Teilnehmer der Online-Tutorien:
- handschriftlich erstellt (lesbare Fotos akzeptiert)
- **rechtzeitig**, mit diesem Deckblatt in **genau einer** PDF-Datei
- direkt an den entsprechenden Tutor abgeben.

---

*Von Tutor*in auszufüllen:* erreichte Punkte

Blatt 2:	/ 20	Blätter 1 – 2, Stud. 1:	/ 40
		Blätter 1 – 2, Stud. 2:	/ 40

Du bist auf Festen immer dabei und fragst dich, was da im Hintergrund ablaufen muss? Schau doch einfach vorbei am **8. November 2021 um 20 Uhr im Raum -120 im Infobau** zum ersten Orgatreffen für das Eulenfest, das Winterfest der Fachschafft Mathematik / Informatik. Hier organisieren traditionell Erstsemester alles von der Musik bis zum Transport, unterstützt von einer Gruppe festerfahrener Studierenden aus höheren Semestern. Hast du schon irgendwelche Ideen? Dann freuen wir uns auf dich!

Aufgabe 2.1 (1 + 1,5 + 1,5 + 1 + 2 = 7 Punkte)

In dieser Aufgabe geht es erneut um Tupelmengen. (Definition siehe Aufgabe 1.5)
Sei also $\mathcal{M} \subset \mathcal{P}(A \times \mathbb{N})$ die Menge aller *legalen* Tupelmengen. Hierbei bezeichnet $\mathcal{P}(X)$ die Potenzmenge einer Menge X. Ferner sei die Tupelmengenoperation $+$ wie in der Musterlösung von Aufgabe 1.5 d) definiert, hier als binäre Relation $+ \subseteq \mathcal{M}^2 \times \mathcal{M}$, mit $((M,N), M+N) \in +$ aufgefasst.

a) Zeigen oder widerlegen Sie: $+$ ist linkstotal
b) Zeigen oder widerlegen Sie: $+$ ist rechtstotal
c) Zeigen oder widerlegen Sie: $+$ ist linkseindeutig
d) Zeigen oder widerlegen Sie: $+$ ist rechtseindeutig
e) Die bereits bekannte Mengenoperation $\cup$ kann analog zu $+$ auch als binäre Relation $\cup \subseteq \mathcal{M}^2 \times \mathcal{M}$ aufgefasst werden. Welche der Eigenschaften linkstotal, rechtstotal, linkseindeutig, rechtseindeutig hat diese Relation und welche nicht? (Nennung genügt)

Lösung 2.1

a) $+$ ist linkstotal, da es für zwei beliebige legale Tupelmengen M, N stets eine legale Tupelmenge $O = M + N$ gibt, da $+$ nach Definition stets eine legale Tupelmenge erzeugt.
b) $+$ ist rechtstotal, da sich jede beliebige legale Tupelmenge M z.B. als Summe der legalen Tupelmengen $M + N$ mit $N = \emptyset$ bilden lässt. Somit gibt es für jede Tupelmenge $M \in \mathcal{M}$ stets zwei $N, O \in \mathcal{M}$ mit $M = N + O$.
c) $+$ ist nicht linkseindeutig, da sich z.b. die Tupelmenge $\{(a,5)\}$ als Summe mehrerer Tupelmengen bilden lässt. Beispiele: $\{(a,5)\} + \emptyset$, bzw. $\{(a,1)\} + \{(a,4)\}$, ...
d) $+$ ist rechtseindeutig, da jede Summe aus zwei beliebigen Tupelmengen $M, N \in \mathcal{M}$ nach Definition genau eine Tupelmenge $O \in \mathcal{M}$ ergibt. (Also insbesondere nicht mehrere.)
e) $\cup$ ist rechtstotal und rechtseindeutig, aber nicht linkstotal und nicht linkseindeutig. $\cup$ ist nicht linkstotal, da z.b. für $\{(a,1)\}$und$\{(a,2)\}$ die Vereinigung $\{(a,1),(a,3)\}$ keine *legale* Tupelmenge ist und folglich $\notin \mathcal{M}$ ist. Ergo gibt es für diese beiden "Eingaben" keine "Ausgabe" im Wertebereich.

Aufgabe 2.2 (1 + 1 + 3 = 5 Punkte)

Seien A, B, C beliebige Mengen und $f : A \to B$, sowie $g : B \to C$ zwei beliebige Abbildungen. Sei ferner $h : A \to C$, mit $h(x) = g(f(x))$.

a) Zeigen Sie: Sind f und g injektiv, so ist auch h injektiv.

b) Zeigen Sie: Sind f und g surjektiv, so ist auch h surjektiv.
c) Beweisen oder widerlegen sie folgende Aussagen: Wenn h injektiv ist, dann ist auch immer g injektiv. Wenn h surjektiv ist, dann ist auch immer f surjektiv.

Lösung 2.2

a) Mathematisch formuliert:
Da f injektiv gilt für $x \neq y$: $f(x) \neq f(y)$ und da g injektiv: $g(f(x)) \neq g(f(y))$.
Alternativ in natürlicher Sprache argumentiert:
Da g injektiv ist, bildet g keine zwei verschiedenen Elemente aus B auf das gleiche Element aus C ab. Da f injektiv ist, bildet f keine zwei verschiedenen Elemente aus A auf das gleiche Element aus B ab. Folglich ist $h(x) = g(f(x))$ für jedes $x \in A$ eindeutig.
b) Da g surjektiv ist, bildet g auf alle $c \in C$ ab. Sofern also f auf den gesamten Definitionsbereich von g abbildet, ist h surjektiv. Dies ist aufgrund der Surjektivität von f gegeben.
c) Beide Aussagen lassen sich gleichzeitig mittels folgendem Gegenbeispiel widerlegen: Sei $A = \{a\}, B = \{b_1, b_2\}, C = \{c\}$ und $f(a) = b_1$, $g(b_1) = g(b_2) = c$.

Aufgabe 2.3 (2 + 3 + 3 = 8 Punkte)

Ein (selbsternannter) genialer Superschurke namens Dr. Meta treibt bereits seit mehreren Jahren in den Übungsblättern des KIT sein Unwesen. Sein Ziel: Nichts Geringeres als die Weltherrschaft. Dabei ist er ebenso hartnäckig wie bisher erfolglos. Dieses Semester macht er sich aufs Neue auf, gewappnet mit den Lehren der Fehlern der Vergangenheit, sowie endlosem genial bösem Genie.

a) Bei der Inspektion der Kommunikationsabteilung fällt Dr. Meta auf, dass die Chance seine genial bösen Pläne geheim zu halten, durch verschlüsselten Nachrichtenaustausch deutlich steigen könnte. Eine Verschlüsselung kann als Relation zwischen der Menge aller Klartext Nachrichten $\mathcal{N}$ und der Menge aller möglichen Chiffrate $\mathcal{C}$ angesehen werden. Erklären Sie Dr. Meta in (möglichst wenigen) leicht verständlichen Sätzen, warum es sinnvoll ist, hier eine linkstotale und linkseindeutige Relation zu verwenden.
b) Dr. Meta plant einen DoS Angriff auf die Rechenzentralen aller Nachrichtendienste der Welt. Sein (genial böser) Plan: Er will deren Computer mit einer Aufgabe beschäftigen, die in endlicher Zeit nicht zu lösen ist. Hierzu will er sie eine Abbildung berechnen lassen, die von $\mathbb{N}$ auf eine unendliche Menge von unendlichen Teilmengen von $\mathbb{N}$ abbildet. Von Ihnen braucht er nur ein kleines Detail: Die Abbildung. Aus Gründen die nur er versteht, muss diese unbedingt injektiv sein!
Nutzen Sie das Format evil(n) := {*endlos genial böse Definition hier*}.
c) Zur Finanzierung seiner Pläne hat Dr. Meta viele Ressourcen in die Entwicklung eines Cryptotradingprognosealgorithmus investiert. Diesen plant er an diverse Trader gegen Gewinnbeteiligung auszuliefern. Dieser "Algorithmus" besteht im Moment nur aus einer "kaputten Funktion" $p : T \to C$, die für einen gegebenen Zeitpunkt $t \in T$ potentiell lukrative Investments aus der Menge aller Investitionsmöglichkeiten C angibt. Leider ist dieser Algorithmus "launisch": Für manche Zeitpunkte gibt er einfach keine Ausgabe aus, für Andere gleich mehrere Verschiedene. Trader wollen aber einen Algorithmus, der ihnen zu jedem Zeitpunkt zuverlässig die besten Trades vorhersagt. Definieren Sie die Relation p geschickt zu einer Abbil-

dung p' um, um die Trader zufrieden zu stellen. Geben sie die Definition von p' samt Definitions- und Bildmenge an, sowie stichhaltige Argumente mit denen sie die manchmal mangelnde, bzw. uneindeutige Ausgabe den Tradern schmackhaft machen können.

Lösung 2.3

a) Linkstotalität stellt sicher, dass auch zu jeder Nachricht ein Chiffrat existiert. Linkseindeutigkeit verhindert, dass zwei verschiedene Nachrichten zum gleichen Chiffrat verschlüsselt werden und stellt so erfolgreiche Entschlüsselbarkeit sicher.

b) Für $x \in \mathbb{N}$ sei $G(x) := \{y \in \mathbb{N} | y > x\}$ und
evil(x) := $\{T \subset \mathbb{N} |$ T enthält genau ein Element aus $G(x)$ nicht$\}$
Erklärung: (nicht gefordert)
evil(x) ist linkstotal und rechtseindeutig, da für jedes $x \in \mathbb{N}$ genau eine Menge definiert ist. Die Funktion ist injektiv, weil $G(x)$ für jedes $x \in \mathbb{N}$ eindeutig ist. Folglich gibt es für jedes $x \in \mathbb{N}$ in evil(x) eindeutige Kombination von Mengen.

c) Definiere $p' : T \to \mathcal{P}(C)$, mit: $p'(t) := \{c \mid p(t, c)\}$
Hierbei werden Zeitpunkte $t \in T$ für die es kein $p(t)$ gibt auf $\emptyset$ abgebildet. Dies verkaufen wir den Tradern als: Zum Zeitpunkt t lohnt sich kein Trade. Für $t \in T$, für die es mehrere $p(t)$ gibt, gilt $|p'(t)| > 1$, aber $p'(t)$ ist dennoch eindeutig. Dies Verkaufen wir den Tradern als: Zu diesem Zeitpunkt lohnen sich all diese Trades.