Institute of Information Security and Dependability
Dr. Mattias Ulbrich
https://formal.kastel.kit.edu/

Übungsblatt 12

Grundbegriffe der Informatik — Winter 2023/24

Tutor*in: | Tutorium Nr.:

Nach-,Vorname: ,

Matr.nr.:

Ausgabe: 6. Februar 2023, 14:30 Uhr
Abgabe: 16. Februar 2024, 12:30 Uhr

Bitte beachten Sie die Hinweise auf der letzten Seite.

---

*Von Tutor*in auszufüllen:*

Blatt 12: / 19 | Blätter 1 – 12: / 240

Aufgabe 1 - Sein oder nicht sein? (5 Punkte)

Beantworten Sie für alle $i \in \{1, \ldots, 6\}$, ob die Relation R_i auf der Menge M_i jeweils eine Äquivalenzrelation, eine Halbordnung, eine Totalordnung oder nichts davon ist. Begründen Sie jeweils Ihre Antwort. Falls R_i eine Äquivalenzrelation ist, geben Sie zusätzlich eine Abbildung $f_i\colon M_i \to M_i$ an, die nicht die Identität ist, aber mit R_i verträglich.

a) $R_1 = \emptyset, M_1 = \mathbb{N}_0$ (0.5 Punkte)

b) $R_2 = \{(x, y) \mid \mathrm{ggT}(x, y) = 1\}, M_2 = \mathbb{N}_+$ (0.5 Punkte)

   Dabei ist der größte gemeinsame Teiler $\mathrm{ggT}(x, y)$ von $x, y \in \mathbb{N}_+$ die größte natürliche Zahl, die sowohl x als auch y teilt.

c) $R_3 = \{(x, y) \mid x^2 + x = y^2 + y\}, M_3 = \mathbb{R}$. (1 Punkt)

d) $R_4 = E^*, M_4 = V$ wobei E die Kantenmenge und V die Knotenmenge eines azyklischen gerichteten Graphen G sind. (1 Punkt)

e) $R_5 = \{(n, m) \mid n = m^k \text{ für ein } k \in \mathbb{N}_+\}, M_5 = \mathbb{N}_+$ (1 Punkt)

f) $R_6 = \{(w_1, w_2) \mid w_1 \text{ und } w_2 \text{ haben ein gemeinsames Teilwort } w \neq \varepsilon\}$, $M_5 = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}^*$ (1 Punkt)

Lösung 1

a) R_1 ist nicht reflexiv, denn z.B. $(0, 0) \notin R_1$. Also kann R_1 weder Äquivalenzrelation noch Halb- oder Totalordnung sein.

b) Auch R_2 ist nicht reflexiv, denn zum Beispiel ggT(2, 2) = 2 und damit $(2, 2) \notin R_2$. Also kann auch R_2 weder Äquivalenzrelation noch Halb- oder Totalordnung sein.

c) R_3 ist eine Äquivalenzrelation, denn: Sowohl Reflexivität als auch Symmetrie und Transitivität von R_3 folgen direkt aus Reflexivität, Symmetrie und Transitivität von = und daraus, dass auf beiden Seiten der Gleichung der gleiche Term steht.

   R_3 ist mit der Funktion $f_3\colon \mathbb{R} \to \mathbb{R}, x \mapsto x^2 + x$ verträglich. Tatsächlich ist R_3 die Faserung von f_3.

   R_3 ist nicht antisymmetrisch, denn es gilt $0^2 + 0 = 0 = (-1)^2 - 1$, also $(0, 1), (1, 0) \in R_3$ aber $0 \neq 1$. Also ist R_3 weder Halb- noch Totalordnung.

d) $R_4 = E^* = \{(v,w) \mid \text{es gibt einen Pfad von } v \text{ zu } w\}$. Damit ist R_4 eine Halbordnung, denn:

- R_4 ist reflexiv, denn für alle $v \in V$ ist $v, v \in E^0$
- R_4 ist antisymmetrisch und nicht symmetrisch, denn G ist azyklisch und damit kann es, wenn es einen Pfad von Knoten $x \in V$ zu Knoten $y \in V$ mit $x \neq y$ gibt, keinen Pfad von y nach x geben
- R_4 ist transitiv, denn für drei beliebige Knoten $u, v, w \in V$ gilt: gibt es einen Pfad p von u zu v und einen Pfad q von v zu w, so ist $p \cdot q$ ein Pfad von u zu w

R_4 ist genau dann symmetrisch, wenn $E = \emptyset$, (denn sonst gibt es für einen Pfad von v nach v' nicht immer auch einen von v' nach v), also auch genau dann eine Äquivalenzrelation. R_4 ist genau dann total, wenn der Graph schwach zusammenhängen ist (es also zwischen zwei Knoten immer einen Pfad gibt).

e) R_5 ist keine Äquivalenzrelation, da es nicht symmetrisch ist; denn $(4,2) \in R_5$, aber $(2,4) \notin R_5$. R_5 ist nicht total, denn z. B. $(3,7) \notin R_5$, $(7,3) \notin R_5$.

R_5 ist eine Halbordnung, denn:

R_5 ist reflexiv, denn für alle $n \in \mathbb{N}_+$ gilt $n = n^1$.

R_5 ist antisymmetrisch, denn: Sei $n = m^k$, $n^l = m$. Dann ist $n = n^{lk}$, also $lk = 1$, also $l = k = 1$. Dann folgt $n = m$.

R^5 ist transitiv, denn: Sei $n = m^k$, $m = p^l$. Dann $n = p^{lk}$.

f) R_6 ist nicht transitiv, denn z.B. $(\texttt{ab}, \texttt{bc}) \in R_6$, da sie `b` teilen und $(\texttt{bc}, \texttt{cc}) \in R_6$, da sie `c` teilen, aber `ab` und `cc` haben kein gemeinsames nichtleeres Teilwort und damit $(\texttt{ab}, \texttt{cc}) \notin R_6$. Also kann R_6 weder Äquivalenzrelation noch Halb- oder Totalordnung sein.

Aufgabe 2 - Turnier (5 Punkte)

Die GBI veranstaltet ihr alljähriges Turnier im Beweisbaumstammweitwurf. Dabei treten in einer Runde genau zwei Teilnehmer gegeneinander an. Die Ergebnisse aller Runden werden in einer Relation $\prec$ auf der Menge $T = \{\alpha, \beta, \gamma, \delta, \eta\}$ der Teilnehmer festgehalten:

$$\prec_0 = \{(\alpha,\beta), (\beta,\eta), (\alpha,\gamma), (\gamma,\eta), (\beta,\delta), (\delta,\eta), (\alpha,\delta), (\gamma,\delta)\}$$

Dabei ist $a \prec_0 b$ für $a, b \in T$ genau dann, wenn a die Runde gegen b verloren hat. Leider wurden die Ergebnisse sehr unübersichtlich festgehalten. Das ganze Turnier wird auch dadurch erschwert, dass manche Teilnehmer abseits der festgelegten Runden einander herausfordern und dadurch weitere Ergebnisse erzeugen. Wer hat nun das Turnier gewonnen?

a) Die Relation $\prec_0$ ist keine Halbordnung. Welche Tupel müssen $\prec_0$ hinzugefügt werden, damit die resultierende Relation $\preccurlyeq$ eine Halbordnung ist? (1 Punkt)

b) Zeichnen Sie das Hassediagramm zu $\preccurlyeq$ auf T. Geben Sie außerdem alle maximalen und minimalen Elemente an, sowie, falls sie existieren, das kleinste und das größte Element. (2 Punkte)

Einige Agenten, denen das Aufstellen des Hassediagramms zu lange dauert, haben aus Langeweile weitere Runden gestartet. Sie haben die Ergebnisse in einer Relation $\sqsubset_0$ festgehalten und plädieren nun dafür, den Gewinner des Turniers als größtes Element der Relation $\sqsubset_0 \circ \prec_0$ zu bestimmen.

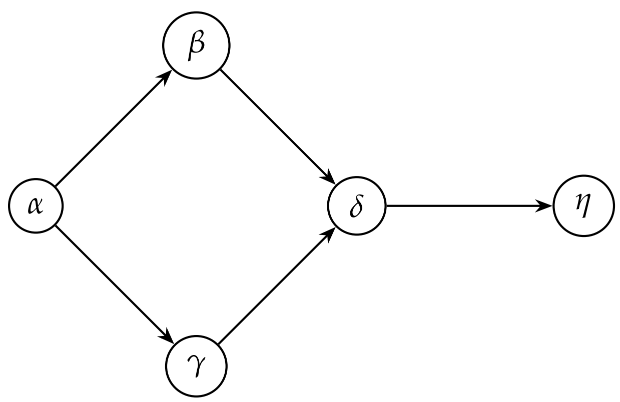
$$\sqsubset_0 = \{(\delta, \gamma), (\eta, \beta)\}$$

c) Zeichnen Sie den Graphen $(T, \sqsubset_0 \circ \prec_0)$. Kann auch $\sqsubset_0 \circ \prec_0$ um weitere Tupel zu einer Halbordnung auf T ergänzt werden? Falls ja, geben Sie diese Tupelmenge an. Ansonsten begründen Sie, warum nicht. (2 Punkte)

Lösung 2

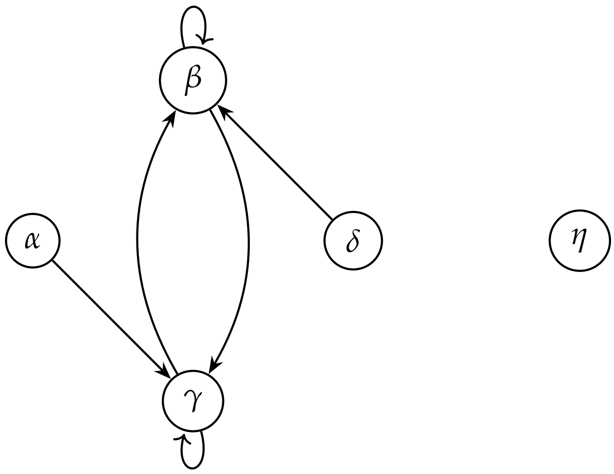
a) Die Relation $\prec_0$ ist bereits antisymmetrisch. Um Reflexivität sicherzustellen, muss für jedes $t \in T$ das Tupel (t, t) ergänzt werden. Damit $\preccurlyeq$ transitiv ist, muss sie außerdem (α, η) enthalten.

b) Hassediagramm zu $\preccurlyeq$ aus Teilaufgabe (a):



Hier lassen sich leicht das minimale Element α, welches auch das kleinste Element, und das maximale Element η, welches auch das größte Element ist, ablesen.

c) Darstellung des Graphen $(T, \sqsubset_0 \circ \prec_0)$:



Die Relation $\sqsubset_0 \circ \prec_0$ kann nicht zu einer Halbordnung ergänzt werden, denn hier ist Antisymmetrie nicht gegeben, wie an dem Zyklus (β, γ, β) zu erkennen ist.

Aufgabe 3 - Finde den Fehler (4 Punkte)

Behauptung: Jede binäre Relation $\sim$, die symmetrisch und transitiv ist, ist auch reflexiv und damit eine Äquivalenzrelation.

Beweis: Sei M eine nicht-leere Menge und sei $\sim \subseteq M \times M$ eine symmetrische und transitive Relation auf M. Seien zudem $x, y \in M$ so, dass $x \sim y$. Da $\sim$ symmetrisch ist, gilt auch $y \sim x$. Wegen der Transitivität von $\sim$ folgt aus $x \sim y$ und $y \sim x$, dass auch $x \sim x$ gilt, also ist $\sim$ reflexiv.

Hier ist etwas faul, denn: Diese Behauptung ist falsch.

a) Geben Sie eine Relation auf $\{\texttt{a}, \texttt{b}, \texttt{c}\}$ an, die zwar symmetrisch und transitiv, aber nicht reflexiv ist. Begründen Sie kurz, warum Ihre Relation nicht reflexiv ist. (1 Punkt)

b) Beschreiben Sie, wo der Fehler im obigen „Beweis" liegt und warum dieser nicht die Behauptung beweist. (2 Punkte)

c) Welche (schwächere) Aussage zeigt der Beweis stattdessen? (1 Punkt)

Lösung 3

a) Die leere Relation $\emptyset \subseteq \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$ ist z. B. symmetrisch und transitiv, aber nicht reflexiv, denn für kein $x \in M$ gilt $(x, x) \in \emptyset$.

b) Es wird angenommen, dass es für jedes Element $x \in M$ ein weiteres Element $y \in M$ gibt, welches ungleich x ist, aber mit x in Relation steht. Dies ist jedoch nicht immer gegeben. (Beispielsweise gibt es keine ganze Zahl, die mit 0 multipliziert eine Zahl ergibt, die größer 0 gibt.)

c) Es wird die folgende Aussage gezeigt:
Jede Relation, die symmetrisch, transitiv und **total** ist, auch reflexiv ist Für jede binäre Relation $\sim$ über einer beliebigen Menge M und jedes $x \in M$ gilt: Wenn $\sim$ symmetrisch und transitiv ist und es ein $y \in M$ mit $x \neq y$ so gibt, dass $x \sim y$, dann gilt $x \sim x$.

Aufgabe 4 - Schweinelatein (5 Punkte)

Weil die hartnäckige GBI ihm zunehmend Probleme bereitet, beschließt Dr. Meta vorbeugend, die Kommunikation mit seinen Gehilfen sicherer zu gestalten und sämtliche Nachrichten zu verschlüsseln. Da er vermutet, dass die meisten von lateinischen Texten abgeschreckt werden, bemüht er sich dabei, dass verschlüsselte Nachrichten möglichst Latein ähneln. Außerdem muss die Verschlüsselung schnell gehen, denn Dr. Meta hat viele Nachrichten zu verschicken!

Gegeben sei das deutsches Alphabet ohne Umlaute $A = \{\mathtt{a}, \mathtt{b}, \dots, \mathtt{z}\}$.

Um ein Wort $w \in A^+$ gemäß dem hochkomplizierten und raffinierten Verfahren von Dr. Meta zu verschlüsseln, wird zunächst das erste Zeichen von w gelöscht und an das Ende von w angefügt. Das Ergebnis wird anschließend um das Suffix `us` ergänzt. So wird zum Beispiel aus dem Wort `code` das verschlüsselte Wort `odecus`.

a) Geben Sie das Ergebnis der Verschlüsselung für die Wörter `doktor` und `meta` an. (1 Punkt)

b) Geben Sie eine Turingmaschine an, deren Lesekopf sich in jedem Schritt nach rechts bewegt und die für ein Wort aus A^+ dessen Verschlüsselung berechnet. Ihre Turingmaschine darf dabei nicht mehr als 75 Zustände haben!

   Den Tutor*innen zuliebe geben Sie Ihre Turingmaschine nicht graphisch sondern als Tupel an. (4 Punkte)

Lösung 4

a) `oktordus`, `etamus`

b) $T = (Z, z_0, A \cup \{\square\}, f, g, m)$ mit

$$
\begin{aligned}
Z &= \{z_a \mid a \in A\} \cup \{z_0, z_1, z_2, z_3\} \\
f(z,x) &= \begin{cases} z_x & \mid z = z_0 \text{ und } x \in A \\ z & \mid z \notin \{z_0, z_1, z_2, z_3\} \text{ und } x \in A \\ z_1 & \mid z \notin \{z_0, z_1, z_2, z_3\} \text{ und } x = \square \\ z_2 & \mid z = z_1 \\ z_3 & \mid z = z_2 \end{cases} \\
g(z,x) &= \begin{cases} \square & \mid z = z_0 \text{ und } x \in A \\ x & \mid z \notin \{z_0, z_1, z_2, z_3\} \text{ und } x \in A \\ a & \mid z = z_a \text{ für ein } a \in A \notin \text{ und } x = \square \\ \texttt{u} & \mid z = z_1 \\ \texttt{s} & \mid z = z_2 \end{cases} \\
m(z,x) &= R \text{ wenn } f, g \text{ definiert für } (z,x)
\end{aligned}
$$

Erklärung (nicht gefordert): Ausgehend vom initialen Zustand z_0 wird sich das erste Zeichen des Eingabewortes über den Zustand gespeichert, in welchen von z_0 gegangen wird, wenn das erste Zeichen gelöscht wird. Entsprechend gibt es für jedes der 26 Zeichen in A genau einen dieser Zustände.

Anschließend wird der Rest der Eingabe unverändert in diesem Zustand abgelaufen, bis das erste $\square$ gelesen wird. An dessen Stelle wird nun das erste Zeichen geschrieben und in z_1 übergegangen. Mit Hilfe von zwei weiteren Übergängen wird das Suffix `us` anstelle der nächsten zwei $\square$ geschrieben.

Bitte beachten Sie die folgenden Hinweise:

- Lösungen **müssen** handschriftlich erstellt werden
- Ihre Abgabe sollte die erste Seite dieser Datei als Deckblatt haben
- Ihre Abgabe muss **rechtzeitig** erfolgen

Außerdem, wenn Sie Ihre Ausarbeitung über die Abgabekästen im Keller des Informatik-Gebäudes abgeben:

- Ihre Abgabe muss in der oberen **linken** Ecke zusammengeheftet werden
- Tablet-Ausdrucke sind zulässig

Wenn Sie Ihre Ausarbeitung online über ILIAS abgeben, dann achten Sie darauf:

- Ihre Abgabe muss **genau eine** PDF-Datei sein
- Scans und lesbare Fotos sind zulässig
- Abgabe erfolgt unter „Tutorien“ im Ordner **Ihres** Tutoriums