Prof. Dr. Jasmin Blanchette
Jannis Limperg
Luca Maio

Ludwig-Maximilians-Universität München
Institut für Informatik
Keine Abgabe

Lösungsvorschlag zur Übung 0 zur Vorlesung

Formale Sprachen und Komplexität

Hinweis: Dieses Blatt wird nicht abgegeben und Sie können keine Bonuspunkte erwerben, aber es wird in den Übungen 18. April 2024–23. April 2024 besprochen.

FSK0-1 *Fundamentale Beweisstrategien*

In dieser Aufgabe diskutieren wir fundamentale Beweisstrategien. Diese Strategien sollten aus anderen Kursen bekannt sein, aber da FSK sehr beweislastig ist, wiederholen wir sie hier.

a) Die folgende Tabelle fasst zusammen, wie man mit Aussagen, die bestimmte logische Operationen enthalten, umgeht.

	Um eine Aussage dieser Form zu beweisen…	Wenn eine Aussage dieser Form angenommen wird…
$P \wedge Q$	beweise sowohl P als auch Q	nimm P und Q an
$P \vee Q$	beweise entweder P oder Q	beweise die gewünschte Aussage sowohl unter der Annahme P als auch unter der Annahme Q (Fallunterscheidung)
$P \Longrightarrow Q$	beweise, dass unter der Annahme P Q folgt	beweise P und nimm dann Q an
$\neg P$	beweise, dass unter der Annahme P ein Widerspruch folgt	beweise P, um einen Widerspruch herzuleiten
$\forall x,\, P(x)$	beweise, dass $P(a)$ für ein beliebiges a gilt	nimm $P(a)$ für jedes konkrete a an
$\exists x,\, P(x)$	gib ein konkretes a an und beweise $P(a)$	nimm ein beliebiges a an, für das $P(a)$ gilt

Die Biimplikation $P \Longleftrightarrow Q$ („P genau dann wenn Q“ oder „P g.d.w. Q“) ist definiert als $(P \Longrightarrow Q) \wedge (Q \Longrightarrow P)$.

Außerdem kann man, unabhängig von der zu beweisenden Aussage, immer folgende Regeln anwenden:

- Widerspruchsbeweis: um P zu beweisen nimm an, dass $\neg P$ gilt, und leite daraus einen Widerspruch ab.

- Satz vom ausgeschlossenen Dritten: für jede beliebige Aussage P nimm $P \vee \neg P$ an.

Häufig nützlich sind auch folgende Regeln:

$$\begin{aligned}
\neg(A \wedge B) &\iff \neg A \vee \neg B \\
\neg(A \vee B) &\iff \neg A \wedge \neg B \\
\neg\forall x,\, P(x) &\iff \exists x,\, \neg P(x) \\
\neg\exists x,\, P(x) &\iff \forall x,\, \neg P(x) \\
A \wedge (B \vee C) &\iff (A \wedge B) \vee (A \wedge C) \\
A \vee (B \wedge C) &\iff (A \vee B) \wedge (A \vee C) \\
(\forall x,\, P(x)) \wedge (\forall x,\, Q(x)) &\iff \forall x,\, P(x) \wedge Q(x) \\
(\exists x,\, P(x)) \vee (\exists x,\, Q(x)) &\iff \exists x,\, P(x) \vee Q(x) \\
\neg\neg A &\iff A
\end{aligned}$$

i) Zeigen Sie: $(\forall n,\, \exists k,\, k > n) \iff (\neg\exists n,\, \forall k,\, n \geq k)$

LÖSUNGSVORSCHLAG:
Wir zeigen beide Richtungen der Biimplikation:

- „$\Longrightarrow$“: Wir nehmen an $\forall n,\, \exists k,\, k > n$. Wir nehmen weiterhin an $\exists n,\, \forall k,\, n \geq k$ und leiten einen Widerspruch ab. Wähle n sodass gilt: $\forall k,\, n \geq k$. Aufgrund der ersten Annahme können wir ein k wählen mit $k > n$. Für dieses k gilt aber auch $n \geq k$, ein Widerspruch.
- „$\Longleftarrow$“: Wir nehmen an $\neg\exists n,\, \forall k,\, n \geq k$ und zeigen für ein beliebiges n die Behauptung $\exists k,\, k > n$. Widerspruchsbeweis: nimm an, es existiert kein solches k, d.h. $\forall k, n \geq k$. Das widerspricht aber der ersten Annahme.

Alternativer Beweis: Nutze die oben angegebenen Regeln über Negation und Quantoren.

$$\begin{aligned}
\neg\exists n,\, \forall k,\, n \geq k &\iff \forall n,\, \neg\forall k,\, n \geq k \\
&\iff \forall n,\, \exists k,\, \neg(n \geq k) \\
&\iff \forall n,\, \exists k,\, k > n
\end{aligned}$$

ii) Gilt die Aussage $\forall n,\, \exists k,\, k > n$

- für $n, k \in \mathbb{N}$?

LÖSUNGSVORSCHLAG:
Ja. Für ein beliebiges n wählen wir $k = n + 1$. Dann gilt $k > n$.

- für $n, k \in \mathbb{R} \cup \{\infty\}$, wobei $\infty > x$ für alle $x \in \mathbb{R}$?

LÖSUNGSVORSCHLAG:
Nein. Wir konstruieren ein Gegenbeispiel: Wir beweisen die Negation der Aussage und nehmen dazu an, dass die Aussage gilt. Daraus folgt für ∞: $\exists k,\ k > \infty$. Das ist aber unmöglich, da nach Definition keine reelle Zahl größer als ∞ ist, und ∞ auch nicht größer als ∞ selbst.
(Technisch gesehen haben wir $>$ nicht spezifiziert. Man könnte also eine Relation $>$ betrachten, bei der $\infty > \infty$ gilt. Das wäre aber eine recht sonderbare Wahl.)

Beweisen Sie Ihre Antworten.

iii) Zeigen Sie: Es gibt unendlich viele Primzahlen.

LÖSUNGSVORSCHLAG:
Wir zeigen: für jede endliche Menge $S = \{p_1, \ldots, p_n\}$ von Primzahlen gibt es eine Primzahl q mit $q \notin S$.
Sei $p = p_1 p_2 \ldots p_n$ und $q = p + 1$. Offensichtlich ist $q \notin S$. Nach dem Satz vom ausgeschlossenen Dritten ist q entweder prim oder nicht.

- Wenn q prim ist, sind wir bereits fertig.
- Wenn q nicht prim ist, existiert ein Primfaktor x, der q teilt. Nun ist x entweder in S oder nicht.
  - Wenn $x \notin S$, dann sind wir fertig.
  - Wenn $x \in S$, dann teilt x auch p, da p das Produkt der Zahlen in S ist. Da x auch q teilt, teilt x die Differenz $q - p = (p + 1) - p = 1$. Da keine Primzahl 1 teilt, ist dieser Fall unmöglich.

Siehe auch die vielen alternativen Beweise unter `https://de.wikipedia.org/wiki/Satz_des_Euklid`.

b) Die Gleichheit von Mengen ist wie folgt definiert:

$$S \subseteq T \text{ g.d.w. } \forall x,\ x \in S \Longrightarrow x \in T$$
$$S = T \text{ g.d.w. } S \subseteq T \wedge T \subseteq S$$

Zeigen Sie:

i) Für alle Mengen S und T gilt: $S = T$ g.d.w. $\forall x,\ x \in S \iff x \in T$.

LÖSUNGSVORSCHLAG:

$$\begin{aligned} S = T &\iff S \subseteq T \wedge T \subseteq S \\ &\iff (\forall x,\ x \in S \implies x \in T) \wedge (\forall x,\ x \in T \implies x \in S) \\ &\iff \forall x,\ (x \in S \implies x \in T) \wedge (x \in T \implies x \in S) \\ &\iff \forall x,\ x \in S \iff x \in T \end{aligned}$$

ii) Für alle Sprachen A, B, C über einem Alphabet Σ gilt: $A \cdot (B \cup C) = A \cdot B \cup A \cdot C$.

LÖSUNGSVORSCHLAG:
Mit dem Satz aus der vorigen Teilaufgabe ist zu zeigen:

$$\forall w,\ w \in A \cdot (B \cup C) \iff w \in A \cdot B \cup A \cdot C$$

Für ein beliebiges w gilt:

- „$\implies$“: Wenn $w \in A \cdot (B \cup C)$ ist, dann ist $w = ax$ für ein $a \in A$ und ein x in $B \cup C$. Damit ist $w = ab$ für ein $b \in B$ oder $w = ac$ für ein $c \in C$, also $w \in A \cdot B \cup A \cdot C$.
- „$\impliedby$“: Wenn $w \in A \cdot B \cup A \cdot C$ ist, dann ist $w = ab$ für ein $a \in A$ und $b \in B$ oder $w = ac$ für ein $a \in A$ und $b \in B$. Damit ist $w = ax$ für ein $x \in B \cup C$, also $w \in A \cdot (B \cup C)$.

iii) $\{n \in \mathbb{N} \mid n \text{ ist prim und } n \geq 3\} = \{n \in \mathbb{N} \mid n \text{ ist prim und ungerade}\}$.

LÖSUNGSVORSCHLAG:
Wir zeigen für ein beliebiges n:

$$\begin{aligned} & n \in \{n \in \mathbb{N} \mid n \text{ ist prim und } n \geq 3\} \\ \iff\ & n \in \{n \in \mathbb{N} \mid n \text{ ist prim und ungerade}\}. \end{aligned}$$

Diese Aussage ist gleichbedeutend mit

$$n \text{ ist prim und } n \geq 3 \iff n \text{ ist prim und ungerade}$$

und diese Biimplikation zeigen wir, wie üblich, indem wir beide Richtungen betrachten.

- „$\implies$“: Angenommen $n \geq 3$ ist prim. Widerspruchsbeweis: Wir nehmen an, dass n entweder nicht prim oder gerade ist. Wenn n

nicht prim ist, haben wir einen Widerspruch. Wenn $n \geq 3$ gerade ist, ist es teilbar durch 2 und damit nicht prim.

- „$\Longleftarrow$“: Angenommen n ist prim und ungerade. Alle Primzahlen unter 3 sind gerade (nämlich genau 2), also muss $n \geq 3$ sein.

c) Die Konkatenation $v \cdot w$ (alternativ vw) zweiter Wörter über einem Alphabet Σ ist rekursiv definiert durch

$$\begin{aligned} \varepsilon \cdot w &= w \\ av \cdot w &= a(v \cdot w) \end{aligned}$$

Alternativ kann man diese Definition auch so schreiben:

$$v \cdot w = \begin{cases} w & \text{falls } v = \varepsilon \\ a(v' \cdot w) & \text{falls } v = av' \end{cases}$$

Zeigen Sie, dass für alle Wörter u, v, w gilt: $u \cdot (v \cdot w) = (u \cdot v) \cdot w$. Verwenden Sie vollständige Induktion (siehe Skript, Kapitel 2) über die Länge von u.

LÖSUNGSVORSCHLAG:

- Für $|u| = 0$ ist $u = \varepsilon$ und $u \cdot (v \cdot w) = \varepsilon \cdot (v \cdot w) = v \cdot w = (\varepsilon \cdot v) \cdot w = (u \cdot v) \cdot w$.
- Für $|u| > 0$ ist $u = au'$ für ein $a \in \Sigma$ und $u' \in \Sigma^*$. Da $|u'| < |u|$ ist, dürfen wir als Induktionshypothese (IH) annehmen: $u' \cdot (v \cdot w) = (u' \cdot v) \cdot w$. Nun gilt

$$\begin{aligned} u \cdot (v \cdot w) = au' \cdot (v \cdot w) = a(u' \cdot (v \cdot w)) &\overset{\text{IH}}{=} a((u' \cdot v) \cdot w) \\ = a(u' \cdot v) \cdot w = (au' \cdot v) \cdot w &= (u \cdot v) \cdot w \end{aligned}$$

FSK0-2 ***Wörter, Sprachen***

a) Seien $\Sigma = \{a, b\}$, $U = \{aab, baa\}$ und $V = \{aa, bb\}$.
Geben Sie Wörter $u, v, w, x \in \Sigma^*$ an, sodass

- $u \in U^*$ und $u \notin V^*$;

LÖSUNGSVORSCHLAG: $u = aab$ (oder $aabaab, baa, baabaa, \ldots$)

- $v \notin U^*$ und $v \in V^*$;

LÖSUNGSVORSCHLAG: $v = aa$ (oder $aabb, bb, bbaa, \ldots$)

- $w \in U^*$ und $w \in V^*$;

  LÖSUNGSVORSCHLAG: $w = aabbaa$ (oder $\varepsilon, aabbaaaabbaa, \ldots$)

- $x \notin U^*$ und $x \notin V^*$.

  LÖSUNGSVORSCHLAG: $x = a$ (oder $b, aba, bab, \ldots$)

Hinweis: Für eine Menge von Symbolen S bezeichnen wir mit S^* die Menge aller endlichen Folgen von Symbolen aus S (z.B. $\{a, b\}^* = \{\varepsilon, a, b, aa, ab, ba, bb, aaa, \ldots\}$).

b) Sei $w = abababababbbbccbaaaaaaaabacaabbbbbbbaba$.

Geben Sie alle Teilwörter v von w an, auf die **alle** der folgenden Eigenschaften zutreffen:

- $|v| = 4$, die Länge von v ist 4;
- $v[1] = a$, das erste Symbol in v ist a;
- $\#_b(v) > 0$, die Anzahl von Vorkommnissen von b in v ist größer als 0.

LÖSUNGSVORSCHLAG:
Man kann prinzipiell alle Teilwörter anschauen und die richtigen heraussuchen.
Effizienter: Nur an mit a anfangenden Stellen nur Teilwörter der Länge 4 anschauen und bei denen danach darüber nachdenken, ob ein b vorkommt.

Teilwort	Kommentar
abab	Mehrmals, reicht einmal aufzuschreiben
abbb	ab-Teil damit zuende, danach erstmal keine weiteren a
aaaa	Mehrmals, kommt kein b vor
aaab	
aaba	
abac	
acaa	Kommt kein b vor
aabb	
abbb	Erneut, muss nicht aufgeschrieben werden
aba	Hier sind zwar nochmal as, aber das Wort ist zuende/zu kurz

Damit ist die vollständige Menge solcher Teilwörter $\{abab, abbb, aaab, aaba, abac, aabb\}$.

FSK0-3 ***Äquivalenzrelationen***

Eine Relation zwischen zwei Mengen M, N ist eine Menge $R \subseteq M \times N$ von Paaren bestehend je aus einem Element aus M und einem aus N. M und N können hierbei beliebige Mengen sein. Ist $(p, q) \in R$, so schreibt man auch $R(p, q)$, pRq oder $p \sim_R q$.

Ist klar, um welche Relation es sich handelt, kann man auch $p \sim q$ schreiben.

Eine Relation R heißt Äquivalenzrelation, wenn

- die zugrundeliegenden Mengen gleich sind: $M = N$;
- für alle $x \in M$ gilt xRx (d.h. R ist reflexiv);
- für alle $x, y \in M$ gilt $xRy \implies yRx$ (d.h. R ist symmetrisch);
- für alle $x, y, z \in M$ gilt $xRy \wedge yRz \implies xRz$ (d.h. R ist transitiv).

Eine Äquivalenzklasse K einer Äquivalenzrelation R ist eine maximale Menge von Elementen $u, v, w, \ldots \in M$ sodass alle Elemente von K durch R in Beziehung stehen: uRv, uRw, vRu, vRw, etc. „Maximal“ bedeutet, dass es kein Element $x \in M$ gibt, das nicht in K ist, aber mit allen Elementen von K in Beziehung steht. Der Index einer Äquivalenzrelation ist die Anzahl ihrer Äquivalenzklassen.

Beispiel: Die Relation

$$\{(u, v) \mid u, v \in \mathbb{N} \text{ und } u \text{ geteilt durch } 3 \text{ hat denselben Rest wie } v \text{ geteilt durch } 3\}$$

ist eine Äquivalenzrelation. Ihre Äquivalenzklassen sind $\{0, 3, 6, \ldots\}$, $\{1, 4, 7, \ldots\}$ und $\{2, 5, 8, \ldots\}$. Sie hat somit Index 3.

Geben Sie für die folgenden Relationen jeweils an, ob sie Äquivalenzrelationen sind. Berechnen Sie außerdem den Index von mindestens zwei der Äquivalenzrelationen.

a) $R_1 \subseteq \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$ mit $0R_11$, $2R_13$ (und sonst $\neg xR_1y$).

LÖSUNGSVORSCHLAG: Keine Äquivalenzrelation: Es gilt nicht $0R_10$.

b) $R_2 \subseteq \{0, 1, 2\} \times \{0, 1, 2\}$ mit $0R_20$, $1R_21$, $2R_22$ (und sonst $\neg xR_2y$).

LÖSUNGSVORSCHLAG: Äquivalenzrelation; Index 3 ($\{0\}$, $\{1\}$, $\{2\}$).

c) $R_3 \subseteq \{0, 1, 2\} \times \{0, 1, 2\}$ mit $0R_30$, $1R_31$, $2R_32$, $1R_32$, $2R_31$ (und sonst $\neg xR_3y$).

LÖSUNGSVORSCHLAG: Äquivalenzrelation; Index 2 ($\{0\}$, $\{1, 2\}$).

d) $R_4 = \{(p, q) \mid$ die Personen p, q haben das gleiche Geburtsjahr$\}$.

LÖSUNGSVORSCHLAG: Äquivalenzrelation.
Index: Je nachdem, wie man „Personen“ genau versteht, sind unterschiedliche Lösungen möglich. Betrachtet man nur lebende Personen, ist der Index etwa 120 (da es etwa 120 verschiedene Jahre gibt, in denen heute lebende Personen geboren wurden). Betrachtet man alle Personen, die je gelebt haben, ist der Index > 1000000. Betrachtet man ein idealisiertes mathematisches Modell, in dem unendlich lange kontinuierlich Personen geboren werden, ist der Index ∞.

e) $R_5 = \{(u, v) \mid$ die Wörter u und v über dem Alphabet $\{a, b\}$ stimmen in den ersten k Positionen überein, wobei k die Länge des kürzeren Wortes ist$\}$.

LÖSUNGSVORSCHLAG: Keine Äquivalenzrelation, denn $aa\ R_5\ a\ R_5\ ab$, aber $\neg(aa\ R_5\ ab)$.

f) $R_6 = \{(p, q) \mid p, q \in \mathbb{N},\ p + q$ ist gerade$\}$.

LÖSUNGSVORSCHLAG:
Äquivalenzrelation mit Index 2:

$$[0]_{R_6} = \{q \in \mathbb{N} \mid 0 + q \text{ ist gerade}\} = \{0, 2, 4, 6, \dots\}$$
$$[1]_{R_6} = \{q \in \mathbb{N} \mid 1 + q \text{ ist gerade}\} = \{1, 3, 5, 7, \dots\}$$

Dies sind alle Äquivalenzklassen, denn $\mathbb{N} = [0]_{R_6} \cup [1]_{R_6}$.