# Logik und Grundlagen der Mathematik

*5. Übung am 05.11.2020*

Richard Weiss Florian Schager Fabian Zehetgruber

**Aufgabe 1** (100)**.** Sei $\psi$ eine Formel mit der freien Variable $z$. Seien $x$ und $y$ zwei (verschiedene) Variablen, die nicht in $\psi$ vorkommen. Wir schreiben $\psi(x)$ und $\psi(y)$ statt $\psi(z/x)$ bzw. $\psi(z/y)$.
Zeigen Sie $\neg\exists y\psi(y) \vdash \exists y\psi(y) \to \chi$ und $\exists x\psi(x) \vdash \exists x(\varphi \to \psi(x))$ für alle Formeln $\chi, \varphi$ und schließen Sie daraus $\vdash \exists x(\exists y\psi(y) \to \psi(x))$.
(Die Formel $\exists yA \to B$) wird als $(\exists yA) \to B$ gelesen.)

*Lösung.* Formaler Beweis für $\neg\exists y\psi(y) \vdash \exists y\psi(y) \to \chi$:

$1 : \neg\exists y\psi(y)$

$2 : \neg\exists y\psi(y) \to \exists y\psi(y) \to \chi$ (Tautologie (1))

$3 : \exists y\psi(y) \to \chi$ MP(2,1)

Formaler Beweis für $\exists x\psi(x) \vdash \exists x(\varphi \to \psi(x))$:

$1 : \exists x\psi(x)$

$2 : \exists x\psi(x) \to \neg\forall x\neg\psi(x)$ (Existenz-Axiom)

$3 : \forall x(\neg(\varphi \to \psi(x)) \to \neg\psi(x))$ (Allquantor vor Tautologie (2) = Axiom)

$4 : \forall x(\neg(\varphi \to \psi(x)) \to \neg\psi(x)) \to \forall x(\neg(\varphi \to \psi(x))) \to \forall x\neg\psi(x)$ (Distributivität)

$5 : \forall x(\neg(\varphi \to \psi(x))) \to \forall x\neg\psi(x)$ (MP(4,3))

$6 : (\forall x(\neg(\varphi \to \psi(x))) \to \forall x\neg\psi(x)) \to (\neg\forall x\neg\psi(x) \to \neg\forall x(\neg(\varphi \to \psi(x))))$ (Tautologie (3))

$7 : \neg\forall x\neg\psi(x) \to \neg\forall x(\neg(\varphi \to \psi(x)))$ (MP(6,5))

$8 : \neg\forall x\neg\psi(x)$ (MP(2,1))

$9 : \neg\forall x(\neg(\varphi \to \psi(x)))$ (MP(7,8))

$10 : \neg\forall x(\neg(\varphi \to \psi(x))) \to \exists x(\varphi \to \psi(x))$ (Existenz-Axiom)

$11 : \exists x(\varphi \to \psi(x))$ (MP(10,9))

Hier eine Liste der verwendeten Tautologien:

$$\neg p \to (p \to q) \tag{1}$$
$$\neg(p \to q) \to \neg q \tag{2}$$
$$(p \to q) \leftrightarrow (\neg q \to \neg p) \tag{3}$$
$$(p \to q) \to ((q \to r) \to (p \to r))) \tag{4}$$

Für den (halbformalen) Beweis von $\vdash \exists x(\exists y\psi(y) \to \psi(x))$ verwenden wir zunächst zweimal das Deduktionstheorem, sowie eine schwache Einführung des Existenzquantors und erhalten für die Wahl $\chi = \phi(x)$ und $\varphi = \exists y\psi(y)$:

$\vdash \neg\exists y\psi(y) \to \exists y\psi(y) \to \psi(x)$ (Deduktion)

$\vdash \neg\exists y\psi(y) \to \exists z(\exists y\psi(y) \to \psi)$ (schwache Einführung von $\exists$)

$\vdash \exists x\psi(x) \to \exists x(\exists y\psi(y) \to \psi(x))$ (Deduktion)

Weiters wissen wir bereits $\vdash \exists x\psi(x) \to \exists y\psi(y)$. Damit ist die Aussage mittels der Tautologie (4) und Beweis durch Fallunterscheidung gezeigt. □

**Aufgabe 2** (104 + 105)**.**

1. Beweisen Sie die starke $\exists$-Einführung. Das heißt: Wenn $\Phi \vdash A \to B$, und $x$ weder in $\Phi$ noch in $B$ frei vorkommt, dann $\Phi \vdash \exists x A \to B$.
   *Hinweis:* Verwenden Sie die starke $\forall$-Einführung.

2. Formulieren und beweisen Sie die schwache $\exists$-Einführung.

*Lösung.*

1. Unter Verwendung der starken Einführung des Allquantors erhalten wir den halbformalen Beweis:

   $\Phi \vdash A \to B$

   $\Phi \vdash (A \to B) \to (\neg B \to \neg A)$ (Tautologie (3))

   $\Phi \vdash \neg B \to \neg A$ (MP)

   $\Phi \vdash \neg B \to \forall x \neg A$ (starke Einführung von $\forall$)

   $\Phi \vdash \exists x A \to \neg\forall x \neg A$ (Existenz-Axiom)

   $\Phi \vdash (\neg B \to \forall x \neg A) \to (\exists x A \to \neg\forall x\neg A) \to (\exists x A \to B)$ (Tautologie (5))

   $\Phi \vdash (\exists x A \to \neg\forall x\neg A) \to (\exists x A \to B)$ (MP)

   $\Phi \vdash \exists x A \to B$ (MP)

   Hier noch weitere verwendete Tautologien:

   $$(\neg p \to q) \to ((r \to \neg q) \to (r \to p)) \tag{5}$$

2. Formulierung der schwachen $\exists$-Einführung:

   $$\frac{\Phi \vdash \varphi \to \psi[x/t]}{\Phi \vdash \varphi \to \exists x\psi}, \qquad \text{wenn die Substitution erlaubt ist.}$$

   Nun der halbformale Beweis (Tautologien bitte dazudenken):

   $\Phi \vdash \neg\psi[x/t] \to \neg\varphi$ (Tautologie (3) + MP)

   $\Phi \vdash \forall x\neg\psi \to \neg\psi[x/t]$ (Substitutions-Axiom)

   $\Phi \vdash \forall x\neg\psi \to \neg\varphi$ (Tautologie (4) + MP)

   $\Phi \vdash \varphi \to \exists x\psi$ (Existenzaxiom + Tautologien (3) und (4) + MP)

□

**Aufgabe 3** (109)**.** Skizzieren Sie einen (halb-)formalen Beweis einer der Formeln aus den vorigen beiden Beispielen.

*Lösung.* Wir skizzieren den Beweis für $[\forall x A(x)] \wedge [\forall x B(x)] \to \forall x[A(x) \wedge B(x)]$:
Wir zeigen dazu $\{\forall x A(x), \forall x B(x)\} \vdash \forall x[A(x) \wedge B(x)]$ und erhalten einen Beweis für die eigentliche Formel

durch zweimaliges Anwenden des Deduktionstheorem und einer geeigneten Tautologie (6).

$$
\begin{aligned}
&1: \forall x A(x), \forall x B(x) \vdash (\forall x A(x)) \to A(x) && \text{(Substitution)}\\
&2: \forall x A(x), \forall x B(x) \vdash (\forall x B(x)) \to B(x) && \text{(Substitution)}\\
&3: \forall x A(x), \forall x B(x) \vdash \forall x A(x) && \text{(Axiom)}\\
&4: \forall x A(x), \forall x B(x) \vdash \forall x B(x) && \text{(Axiom)}\\
&5: \forall x A(x), \forall x B(x) \vdash A(x) && \text{(MP)}\\
&6: \forall x A(x), \forall x B(x) \vdash B(x) && \text{(MP)}\\
&7: \forall x A(x), \forall x B(x) \vdash A(x) \to B(x) \to A(x) \wedge B(x) && \text{(Tautologie (7))}\\
&8: \forall x A(x), \forall x B(x) \vdash B(x) \to A(x) \wedge B(x) && \text{(MP)}\\
&9: \forall x A(x), \forall x B(x) \vdash A(x) \wedge B(x) && \text{(MP)}\\
&27: \forall x A(x), \forall x B(x) \vdash \forall x[A(x) \wedge B(x)] && \text{(Generalisierungstheorem)}
\end{aligned}
$$

Noch mehr Tautologien:

$$(p \to (q \to r)) \to ((p \wedge q) \to r) \tag{6}$$

$$p \to (q \to (p \wedge q)) \tag{7}$$

□

**Aufgabe 4** (110)**.** Skizzieren Sie einen weiteren (halb-)formalen Beweis einer der Formeln aus den vorigen beiden Beispielen.

*Lösung.* Wir skizzieren den Beweis für $\exists x[A(x) \wedge B(x)] \to [\exists x A(x)] \wedge [\exists x B(x)]$:
Wir beweisen stattdessen $[\forall x \neg A(x)] \wedge [\forall x \neg B(x)] \to \forall x[\neg(A(x) \wedge B(x))]$ und schließen dann mit Tautologien auf die eigentliche Formel. Wir kennen bereits einen (halbformalen) Beweis von $[\forall x \neg A(x)] \wedge [\forall x \neg B(x)] \to \forall x[\neg A(x) \wedge \neg B(x)]$. Jetzt müssen wir nur noch die offensichtliche Tautologie mit dem Distributivitäts-Axiom kombinieren und wir sind fertig:

$$
\begin{aligned}
&\vdash [\forall x \neg A(x)] \wedge [\forall x \neg B(x)] \to \forall x[\neg A(x) \wedge \neg B(x)] && \\
&\vdash \forall x \underbrace{(\neg A(x) \wedge \neg B(x))}_{C} \to \underbrace{(\neg(A(x) \wedge B(x)))}_{D} && \text{(Allquantor vor Tautologie)}\\
&\vdash [\forall x (C \to D)] \to [\forall x C \to \forall x D] && \text{(Distributivität)}\\
&\vdash \forall x C \to \forall x D && \text{(MP)}\\
&\vdash [\forall x \neg A(x)] \wedge [\forall x \neg B(x)] \to \forall x[\neg(A(x) \wedge B(x))] && \text{(Tautologie + MP)}
\end{aligned}
$$

□

*Lösung.* Wir skizzieren den Beweis für $\exists x[A(x) \wedge B(x)] \to [\exists x A(x)] \wedge [\exists x B(x)]$:

$$
\begin{aligned}
&\vdash (\forall x \neg A(x)) \to \neg A(y) && \text{(Substitutionsaxiom)}\\
&\vdash A(y) \to \exists x A(x) && \text{(Tautologie (3) + Existenzaxiom + MP)}\\
&\vdash B(y) \to \exists x B(x) && \text{(analog)}\\
&\vdash [A(y) \wedge B(y)] \to [\exists x A(x)] \wedge [\exists x B(x)] && \text{(Tautologie (8) + MP)}\\
&\vdash \exists y[A(y) \wedge B(y)] \to [\exists x A(x)] \wedge [\exists x B(x)] && \text{($\exists$-Einführung stark)}\\
&\vdash [\forall y \neg P(y)] \to [\forall x \neg P(x)] && \text{(haben wir bereits bewiesen)}\\
&\vdash [\exists x P(x)] \to [\exists y P(y)] && \text{(Tautologien (3) und (4) + Existenzaxiom + MP)}\\
&\vdash \exists x[A(x) \wedge B(x)] \to [\exists x A(x)] \wedge [\exists x B(x)] && \text{(Tautologie (4) + MP)}
\end{aligned}
$$

Tautologien

$$(p \to q) \to ((r \to s) \to ((p \wedge r) \to (q \wedge s))) \tag{8}$$

□

**Aufgabe 5** (113)**.** Sei $\mathscr{L}$ eine Sprache der Prädikatenlogik, $\Sigma$ eine vollständige konsistente Theorie in $\mathscr{L}$. Zeigen Sie für alle geschlossenen Formeln $A$ und $B$:

- $\Sigma \vdash A \vee B$ genau dann, wenn $\Sigma \vdash A$ oder $\Sigma \vdash B$.
- $\Sigma \vdash A \wedge B$ genau dann, wenn $\Sigma \vdash A$ und $\Sigma \vdash B$.
- $\Sigma \vdash \neg A$ genau dann, wenn $\Sigma \nvdash A$.

*Lösung.*

- Gelte $\Sigma \vdash A \vee B$, $\Sigma \nvdash A$ und $\Sigma \nvdash B$:
  Aus der Vollständigkeit von $\Sigma$ erhalten wir dadurch $\Sigma \vdash \neg A$ und $\Sigma \vdash \neg B$. Mit der Tautologie $\neg A \to \neg B \to \neg(A \vee B)$ erhalten wir damit auch $\Sigma \vdash \neg(A \vee B)$, was einen Widerspruch zur Konsistenz von $\Sigma$ liefert.
  Gelte umgekehrt $\Sigma \vdash A$. Dann folgt mit der Tautologie $A \to A \vee B$ auch $\Sigma \vdash A \vee B$. Analoges gilt unter der Voraussetzung $\Sigma \vdash B$.
- Gelte $\Sigma \vdash A \wedge B$. Mit der Tautologie $(A \wedge B) \to A$ gilt schließen wir $\Sigma \vdash A$ und $\Sigma \vdash B$.
  Gelte umgekehrt $\Sigma \vdash A$ und $\Sigma \vdash B$. Jetzt finden wir wieder eine Tautologie mit $A \to B \to A \wedge B$ und erhalten mit Modus Ponens $\Sigma \vdash A \wedge B$.
- Angenommen es gilt $\Sigma \vdash \neg A$ und $\Sigma \vdash A$. Dann können wir die Tautologie $A \to (\neg A \to \perp)$ verwenden und $\Sigma \vdash \perp$ schließen. Widerspruch zur Konsistenz.
  Gelte $\Sigma \nvdash A$. Wegen der Vollständigkeit muss dann $\Sigma \vdash \neg A$ gelten.

□

**Aufgabe 6** (114)**.** Die 3 Äquivalenzen in der vorigen Aufgabe lassen sich in der Form von 6 Implikationen schreiben. Welche dieser 6 Implikationen

- ... gelten für alle Theorien $\Sigma$?
- ... gelten für alle konsistenten Theorien $\Sigma$?
- ... implizieren Vollständigkeit von $\Sigma$? (Unter der Voraussetzung, dass $\Sigma$ konsistent ist.)

*Lösung.* Sicher gelten die Folgenden Implikationen, denn da kann man den Beweis einfach übernehmen:

- Rückrichtungen von 1. und Äquivalenz von 2.
- Rückrichtungen von 1. und Äquivalenz von 2. und Hinrichtung von 3.
- Rückrichtung von 3.

Sei nun eine konsistente Theorie $\Sigma$ gegeben für welche die Hinrichtung von 1. gilt. Wir wählen eine beliebige geschlossene Formel $A$. Es gilt $\Sigma \vdash A \vee \neg A$, da es sich um eine Tautologie handelt. Wegen der Hinrichtung von 1. gilt also $\Sigma \vdash A$ oder $\Sigma \vdash \neg A$. Gälten beide so könnten wir mit der Tautologie $A \to (\neg A \to \perp)$ auch den Beweis $\Sigma \to \perp$ führen, ein Widerspruch zur konsitenz. Also impliziert auch die Hinrichtung von 1. schon Vollständigkeit.
Als Gegenbeispiel dafür, dass die Hinrichtung von 3. nicht für alle Theorien gilt nehmen wir eine beliebige geschlossene Formel $\sigma$ und definieren $\Sigma := \{\sigma, \neg\sigma\}$. Dann gilt natürlich $\Sigma \vdash \sigma$ und $\Sigma \vdash \neg\sigma$.
Als Gegenbeispiel für eine konsistente Theorie, für welche die Hinrichtung von 1. und die Rückrichtung nicht beweisbar ist, nehmen wir eine beliebige konsistente und nicht vollständige Theorie $\Sigma$. Darin finden wir eine Aussage $A$ mit $\Sigma \nvdash A$ und $\Sigma \nvdash \neg A$. Nun gilt aber, da es sich bei $A \vee \neg A$ um eine Tautologie handelt, $\Sigma \vdash A \vee \neg A$.

□

## Außer Konkurrenz

**Aufgabe 7** (117)**.** Sei $\mathscr{L}$ eine (möglicherweise überabzählbare) Sprache der Prädikatenlogik, $\Sigma_0$ eine konsistente Theorie in $\mathscr{L}$. Sei $P$ die Menge aller konsistenten Theorien $\Sigma \supseteq \Sigma_0$ in der Sprache $\mathscr{L}$. Durch die Relation $\subseteq$ wird $P$ partiell geordnet.
Zeigen Sie:

- Jede Kette in $P$ (also jede durch $\subseteq$ total geordnete Teilmenge $K \subseteq P$) ist beschränkt. (Das heißt, für jede Kette $K \subseteq P$ gibt es $\Sigma^* \in P$, sodass für alle $\Sigma \in K$ die Beziehung $\Sigma \subseteq \Sigma^*$ gilt.)
- Wenn $\Sigma \in P_{\mathscr{L}}$ maximal ist (also: Es gibt kein $\Sigma' \subsetneq$ in $P$), dann ist $\Sigma$ vollständig.
- Schließen Sie aus dem Lemma von Zorn, dass es zu jeder konsistenten Theorie $\Sigma_0$ eine vollständige konsistente Theorie $\Sigma_1 \supseteq \Sigma_0$ gibt.

*Lösung.*

$\square$

# Logik und Grundlagen der Mathematik

*5. Übung am 05.11.2020*

Richard Weiss Florian Schager Fabian Zehetgruber

## Vollständige Theorien

**Aufgabe 1** (117)**.** Sei $\mathscr{L}$ eine (möglicherweise überabzählbare) Sprache der Prädikatenlogik, $\Sigma_0$ eine konsistente Theorie in $\mathscr{L}$. Sei $P$ die Menge aller konsistenten Theorien $\Sigma \supseteq \Sigma_0$ in der Sprache $\mathscr{L}$. Durch die Relation $\subseteq$ wird $P$ partiell geordnet.
Zeigen Sie:

- Jede Kette in $P$ (also jede durch $\subseteq$ total geordnete Teilmenge $K \subseteq P$) ist beschränkt. (Das heißt, für jede Kette $K \subseteq P$ gibt es $\Sigma^* \in P$, sodass für alle $\Sigma \in K$ die Beziehung $\Sigma \subseteq \Sigma^*$ gilt.)
- Wenn $\Sigma \in P_{\mathscr{L}}$ maximal ist (also: Es gibt kein $\Sigma' \subsetneq$ in $P$), dann ist $\Sigma$ vollständig.
- Schließen Sie aus dem Lemma von Zorn, dass es zu jeder konsistenten Theorie $\Sigma_0$ eine vollständige konsistente Theorie $\Sigma_1 \supseteq \Sigma_0$ gibt.

*Lösung.*

- Sei $K$ beliebige Kette in $P$. Dann gilt sicher für alle $\Sigma \in K : \Sigma \subseteq \bigcup K$.
  Es bleibt also noch zu zeigen, dass $\bigcup K \in P$: Es gilt sicher $\Sigma_0 \subseteq \bigcup K$.
  Angenommen, $\bigcup K$ wäre nicht konsistent, also $\bigcup K \vdash \perp$. Aus Aufgabe 96 wissen wir bereits, dass es eine endliche Teilmenge $\Sigma^* \subseteq \bigcup K$ gibt mit $\Sigma^* \vdash \perp$. Da $K$ eine Kette ist gibt es ein $\Sigma' \in K$ mit $\Sigma^* \subseteq \Sigma'$ und daher $\Sigma' \vdash \perp$. Ein Widerspruch zur Konsistenz aller $\Sigma \in K$.
- Sei $\Sigma^* \in P_{\mathscr{L}}$ maximal: Angenommen $\Sigma^*$ wäre nicht vollständig, also finden wir eine geschlossene Formel $\sigma$ in $\mathscr{L}$, sodass weder $\Sigma^* \vdash \sigma$ noch $\Sigma^* \vdash \neg\sigma$. Nun können wir eine der beiden Formeln zu $\Sigma^*$ hinzufügen und bleiben vollständig. Warum? Wäre dem nicht so, dann könnten wir $\Sigma^* \cup \sigma \vdash \perp$ und $\Sigma^* \cup \neg\sigma \vdash \perp$ herleiten. Nach zweimaliger Anwendung des Deduktionstheorem haben wir hiermit einen halbformalen Beweis durch Fallunterscheidung für $\Sigma^* \vdash \perp$ dastehen. Widerspruch! Damit ist $\Sigma^*$ nicht maximal, nochmal Widerspruch!
  Also muss $\Sigma^*$ bereits vollständig sein.
- Jetzt müssen wir die Resultate nur noch zusammenfügen. In Punkt 1 haben wir die Voraussetzung für das Lemma von Zorn überprüft, also gibt es maximale Elemente $\Sigma_1 \subseteq \Sigma_0$, welche laut Punkt 2 bereits vollständig sein müssen.

$\square$

**Aufgabe 2** (118)**.** Sei $\Sigma$ vollständige Henkintheorie, und sei $\mathscr{M}$ die zugehörige in der Vorlesung definierte Struktur (Äquivalenzklassen von geschlossenen Termen). Zeigen Sie, dass für alle geschlossenen Terme $t$ die Gleichung $t^{\mathscr{M}} = [t]_\sim$ gilt. (Was ist mit der linken Seite gemeint?)

*Lösung.* In der Vorlesung haben wir definiert:

$$\mathscr{M} : M = \{[c]_\sim : c \text{ Konstantensymbol}\} = [t]_\sim$$
$$c \sim d :\Longleftrightarrow \Sigma \vdash c = d.$$
$$f^{\mathscr{M}}([t_1]_\sim, \dots, [t_n]_\sim) := [f(t_1, \dots, t_m)]_\sim$$

Zuerst wollen wir uns überlegen, wie die Gleichung zu interpretieren ist. Für jeden geschlossenen Term $t$ erhalten wir mit dem Substitutionsaxiom, einem Existenzaxiom, einem Gleichheitsaxiom, einem Leibnizaxiom, sowie (zumindest) einer Tautologie und ein paar Mal Modus Ponens $\Sigma \vdash \exists x(x = t)$. Da $\Sigma$ eine Henkintheorie ist bekommen wir damit eine Konstante $c_t$ mit $\Sigma \vdash c_t = t$. Also ist $[t]_\sim := [c_t]_\sim$. Aufgrund der Gleichheitsaxiome ist die Definition unabhängig vom Repräsentanten.
Im Folgenden wollen wir, ohne dies zu beweisen, verwenden, dass die Menge aller geschlossenen Terme die kleinste Menge ist, welche alle Konstanten enthält und bezüglich Funktionen abgeschlossen ist. So können wir also die geschlossenen Terme aufbauen, für Konstanten ist $c^{\mathscr{M}}$ ohnehin definiert, für $t = f(t_1, \ldots, t_k)$ definieren wir $t^{\mathscr{M}} := f^{\mathscr{M}}(t_1^{\mathscr{M}}, \ldots, t_k^{\mathscr{M}})$.
Nun beweisen wir die Aussage mit Induktion nach dem Aufbau der geschlossenen Terme.
Für alle Konstantensymbole folgt die Aussage direkt aus der Definition: $c^{\mathscr{M}} = [c]_\sim$.
Sei $t = f(t_1, \ldots, t_k)$ beliebig, wobei $t_1^{\mathscr{M}} = [t_1]_\sim, \ldots, t_k^{\mathscr{M}} = [t_k]_\sim$. Ganz formal gilt

$$t^{\mathscr{M}} := f^{\mathscr{M}}(t_1^{\mathscr{M}}, \ldots, t_k^{\mathscr{M}}) = f^{\mathscr{M}}([t_1]_\sim, \ldots, [t_k]_\sim) = [f(t_1, \ldots, t_k)]_\sim = [t]_\sim.$$

Wir zeigen noch, dass $f^{\mathscr{M}}$ wohldefiniert, also unabhängig von der Wahl der Repräsentanten ist. Sei also $[s_1]_\sim = [t_1]_\sim, \ldots, [s_k]_\sim = [t_k]_\sim$. Nach obiger Definition gibt es Konstanten $c_1, \ldots, c_k$, sodass für alle $i \in \{1, \ldots, k\}$ die Ausdrücke $(\Sigma \vdash c_i = t_i)$ und $(\Sigma \vdash c_i = s_i)$ gelten. Mit den Gleichheitsaxiomen und den Leibniz-Axiomen leitet man schnell $\Sigma \vdash f(s_1, \ldots, s_k) = f(t_1, \ldots, t_k)$ her. Für $d \in [c]_\sim$ gilt $\Sigma \vdash c = d$ und daher $c^{\mathscr{M}} = d^{\mathscr{M}}$. Also sind alle Definitionen unabhängig von den Repräsentanten. □

## Kompaktheitssatz

Der Kompaktheitssatz der Prädikatenlogik besagt: Wenn $\Sigma \vDash \varphi$, dann gibt es eine endliche Menge $\Sigma' \subseteq \Sigma$ mit $\Sigma' \vDash \varphi$.
Sei $n \geq 2$. Mit $\exists^n$ (oder genauer $\exists^{\geq n}$) kürzen wir die Formel $\forall x_2 \cdots \forall x_n \exists y\,(y \neq x_2 \wedge \cdots \wedge y \neq x_n)$ ab.
(Oder: Die dazu beweisbar äquivalente Formel $\exists x_1 \cdots \exists x_n\,(x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge \cdots \wedge x_{n-1} \neq x_n)$.)

**Aufgabe 3** (128)**.** Wir betrachten die Sprache der Gruppentheorie (ein zweistelliges Funktionssymbol $*$, ein einstelliges $^{-1}$, ein Konstantensymbol 1). Lösen Sie möglichst viele der folgenden Probleme (bzw. zeigen Sie gegebenenfalls, dass sie unlösbar sind):

- Finden Sie eine Formel $\sigma_G$, sodass Mod $(\sigma_G)$ die Klasse aller Gruppen ist.
- Finden Sie eine Formel $\sigma_{eG}$, sodass Mod $(\sigma_{eG})$ die Klasse aller endlichen Gruppen ist.
- Finden Sie eine Formel $\sigma_{uG}$, sodass Mod $(\sigma_{uG})$ die Klasse aller unendlichen Gruppen ist.
- Finden Sie eine Formelmenge $\Sigma_{eG}$, sodass Mod $(\Sigma_{eG})$ die Klasse aller endlichen Gruppen ist.
- Finden Sie eine Formelmenge $\Sigma_{uG}$, dass Mod $(\Sigma_{uG})$ die Klasse aller unendlichen Gruppen ist.

*Hinweis:* Verwenden Sie für den Nachweis der Unlösbarkeit die Formeln $\exists^{\geq n}$ und den Kompaktheitssatz.

*Lösung.* Wir wissen, dass zu jedem positiven $n \in \mathbb{N}$ eine (zyklische) Gruppe der Ordnung $n$ existiert, sowie Gruppen von unendlicher Ordnung.

- $$\begin{aligned}\sigma_G = \forall x \forall y \forall z (x * (y * z) = (x * y) * z) \wedge\\ \exists e \forall x (e * x = x = x * e) \wedge\\ \forall x (x * x^{-1} = x^{-1} * x = e)\end{aligned}$$
- Angenommen, es existiert eine Formel $\sigma_{eG}$, sodass Mod $(\sigma_{eG})$ die Klasse aller endlichen Gruppen ist. Dann ist $\Sigma := \{\exists^{\geq n} : n \in \mathbb{N}\} \cup \{\sigma_{eG}\}$ erfüllbar, da jede endliche Teilmenge erfüllbar ist. $\Sigma$ selbst ist aber klarerweise unerfüllbar. Widerspruch!

- Angenommen, es existiert eine Formel $\sigma_{uG}$, sodass Mod $(\sigma_{uG})$ die Klasse aller unendlichen Gruppen ist. Dann ist $\Sigma = \{\neg\sigma_{uG}, \sigma_G\}$ eine Formelmenge, die alle endlichen Gruppen beschreibt, was allerdings laut dem nächsten Punkt nicht möglich ist.

- Angenommen, es existiert eine Formelmenge $\Sigma_{eG}$, sodass $\mathrm{Mod}(\Sigma_{eG})$ die Klasse aller endlichen Gruppen ist. Betrachte mal wieder $\Sigma := \{\exists^{\geq n} : n \in \mathbb{N}\} \cup \Sigma_{eG}$. Wieder ist jede endliche Teilmenge davon erfüllbar, aber um $\Sigma$ zu erfüllen, müssten wir eine endliche Gruppe finden, deren Ordnung jedes $n \in \mathbb{N}$ übersteigt. Widerspruch!

- $\Sigma_{uG} = \{\exists^{\geq n} : n \in \mathbb{N}\} \cup \{\sigma_G\}$

$\square$

**Aufgabe 4** (130)**.** Sei $\mathscr{M}$ eine unendliche abzählbare Struktur. Zeigen Sie, dass es in Mod (Th $(\mathscr{M})$) eine überabzählbare Struktur gibt.
*Hinweis:* Vollständigkeitssatz und Kompaktheitssatz gelten auch für überabzählbare Sprachen. Verwenden Sie überabzählbar viele Konstantensymbole.

*Lösung.* Mit $\mathrm{Mod}(\Sigma)$ bezeichnen wir die Klasse aller Strukturen $\mathscr{M}$ (einer vorgegebenen Sprache), die $\mathscr{M} \vDash \Sigma$ erfüllen. Sei $\mathfrak{M}$ eine Klasse von Strukturen. Mit Th $(\mathfrak{M})$ bezeichnen wir die Theorie von $\mathfrak{M}$, also die Menge aller geschlossenen Formeln $\varphi$, die in jedem $\mathscr{M} \in \mathfrak{M}$ erfüllt sind.
In unserem Fall gilt $\mathrm{Th}(\mathscr{M}) = \{\sigma : \mathscr{M} \vDash \sigma\}$. Bezeichne $\mathscr{L}$ die Sprache von $\mathscr{M}$ und sei $C$ eine überabzählbare Menge von neuen Konstantensymbolen. Definiere $\mathscr{L}' := \mathscr{L} + C$, sowie $\Sigma := \mathrm{Th}\,(\mathscr{M}) \cup \{c \neq d : c, d \in C, c \neq d\}$. Jede endliche Teilmenge davon ist erfüllbar, daher muss mit der Kontraposition des Kompaktheitssatzes auch $\Sigma$ erfüllbar sein. Also existiert ein $\mathscr{M}'$ mit $\mathscr{M}' \vDash \mathrm{Th}\,(\mathscr{M}) \cup \{c \neq d : c, d \in C, c \neq d\}$, insbesondere ist $\mathscr{M}' \in$ Mod (Th $(\mathscr{M})$). Die hinzugefügten Formeln garantieren, dass verschiedene Konstantensymbole der neuen überabzählbaren Konstantenmenge $C$ auch unterschiedlich interpretiert werden. Damit muss $\mathscr{M}'$ ebenso eine überabzählbare Struktur sein.

$\square$

**Aufgabe 5** (133)**.** Zeigen Sie (mit Hilfe des Kompaktheitssatzes, aber ohne Auswahlaxiom, Lemma von Zorn oder den Hausdorffschen Kettensatz zu verwenden), dass es auf jeder Menge eine lineare Ordnung gibt. Wenn das zu einfach ist: Zu jeder partiellen Ordnung $(P, \leq)$ gibt es eine lineare Ordnung $(P, \leq')$ mit $\forall x \forall y : (x \leq y \implies x \leq' y)$.
*Hinweis:* Betrachten Sie eine Sprache, die ein zweistelliges Relationssymbol enthält, sowie für jedes Element Ihrer Menge eine neue Konstante.

*Lösung.* Wir bewegen uns in einer Sprache $\mathscr{L}$ mit einem zweistelligen Relationssymbol $\leq$ und einer Konstantenmenge $C = \{c_p : p \in P\}$. Definiere

$$\Sigma := \{(c \leq c) \wedge (c \leq d \to d \leq c \to c = d) \wedge (c \leq d \vee d \leq c) \wedge (c \leq d \to d \leq e \to c \leq e) : c, d, e \in C\}$$

Jede endliche Teilmenge von $\Sigma$ ist erfüllbar. Dafür betrachte die endliche Menge $M$ an Konstantensymbole die in $\Sigma$ vorkommen. Diese Menge können wir nun mit einer linearen Ordnung versehen, z.B. betrachten wir die nach der Definition der Endlichkeit existierende Bijektion $f : M \to \{1, \ldots, n\}$ für ein $n \in \mathbb{N}$ und definieren $m_1 \leq m_2 :\iff f(m_1) \leq_{\mathbb{N}} f(m_2)$ für $m_1, m_2 \in M$. Nach dem Kompaktheitssatz ist dann auch $\Sigma$ erfüllbar. Also existiert eine Struktur $\mathscr{L}$, welche $\Sigma$ erfüllt. Nun definiere

$$p \leq q :\iff c_p^{\mathscr{M}} \leq^{\mathscr{M}} c_q^{\mathscr{M}}, \quad p, q \in P.$$

Diese Vorschrift ist wohldefiniert, da wir unsere Konstantensymbolmenge so gewählt haben, dass es zu jedem $p \in P$ genau ein wohlunterschiedenes Konstantensymbol $c_p$ gibt. Nun gilt es noch nachzuprüfen, dass dadurch tatsächlich eine lineare Ordnung definiert wird: Reflexivität, Transivität und Totalität übertragen sich direkt aufgrund den Gesetzen in $\Sigma$. Die Antisymmetrie folgt ebenso aus den Gesetzen, sowie der Voraussetzung, dass $c_p, c_q$ für $p \neq q$ unterschiedliche Konstantensymbole bezeichnen. $\square$

**Aufgabe 6** (134)**.** Wir betrachten eine Theorie $\Sigma$ in der Sprache mit einem zweistelligen Relationssymbol $E$. Die Theorie verlangt, dass $E$ (genauer: $E^{\mathscr{M}}$ für jedes $\mathscr{M}$, welches $\Sigma$ erfüllt) eine Äquivalenzrelation ist, in der jede Klasse unendlich viele Elemente enthält. Weiters definieren wir $\Sigma_2 := \Sigma \cup \{\forall x \forall y \forall z(xEy \lor yEz \lor xEz)\}$.

a. Geben Sie die Formeln in $\Sigma$ an.

b. Wie viele abzählbar unendliche Modelle hat $\Sigma_2$ bis auf Isomorphie? Geben Sie alle an.

c. Geben Sie mindestens 3 (nichtisomorphe) Modelle von $\Sigma_2$ an, deren Universum $\mathbb{R}$ ist.

d. Finden Sie alle vollständigen konsistenten Theorien $\Sigma' \supseteq \Sigma_2$ (wobei wir zwei Theorien als gleich betrachten, wenn sie dieselben Konsequenzen haben).
*Hinweis:* Verwenden Sie den Vollständigkeitssatz sowie Ihr Resultat aus Punkt b.

*Lösung.*

a. Definiere dafür die Formel

$$\exists^{\geq n} = \forall x \exists x_1 \cdots \exists x_n \, (x_1 \neq x_2 \land x_1 \neq x_3 \land \cdots \land x_{n-1} \neq x_n \land xEx_1 \land \cdots \land xEx_n)$$
$$\Sigma = \{\forall x \, (xEx), \forall x \forall y \, (xEy \to yEx), \forall x \forall y \forall z \, (xEy \to yEz \to xEz)\} \cup \{\exists^{\geq n} : n \in \mathbb{N}\}$$

b. Wir behaupten dass es bis auf Isomorphie nur zwei unterschiedliche Modelle von $\Sigma_2$ gibt. Zuerst bemerken wir dafür, dass die Gesetze in $\Sigma_2$ bereits erzwingen, dass es in allen Modellen $\mathscr{M}$ von $\Sigma_2$ maximal zwei Äquivalenzklassen geben kann. Gäbe es nämlich mindestens drei, so könnten wir $x, y, z \in M$ aus jeweils unterschiedlichen Äquivalenzklassen wählen, welche dann die Formel $\forall x \forall y \forall z(xEy \lor yEz \lor xEz)$ verletzen würden.
Jetzt gilt es also noch zu zeigen, dass alle Modelle von $\Sigma_2$ mit der gleichen Anzahl an Äquivalenzklassen paarweise isomorph sind. Für Modelle mit einer einzigen Äquivalenzklasse ist die Interpretation von $E$ bereits zwangsläufig die Allrelation und somit stellt jede Bijektion zwischen den Universen bereits eine mit den Interpretationen von $E$ verträgliche Abbildung, also eine Isomorphie dar. So eine Bijektion exisitiert immer, da wir hier nur von abzählbaren Modellen sprechen.
Für Modelle $\mathscr{M}_1, \mathscr{M}_2$ mit jeweils zwei Äquivalenzklassen müssen wir also eine Bijektion finden, welche mit der von den Interpretationen von $E$ induzierten Partitionen $M_1 = P_1 \cup Q_1, M_2 = P_2 \cup Q_2$ verträglich ist, also $f(P_1) = P_2, f(Q_1) = Q_2$ beispielsweise. Dies ist immer möglich, da die Modelle $\mathscr{P} : P_1, E|_{P_1 \times P_1}$, usw. allesamt Modelle von $\Sigma_2$ mit nur einer einzigen Äquivalenzklasse sind, wo denen wir bereits wissen, dass sie paarweise isomoprh sind. Wir erhalten also Isomorphien $f_p : P_1 \to P_2, p_q : Q_1 \to Q_2$. Schließlich ist $f = f_p \cup f_q$ die gesuchte Bijektion zwischen $\mathscr{M}_1$ und $\mathscr{M}_2$.

c. Wir geben drei Partitionen auf $\mathbb{R}$ an:

1) $\{\mathbb{R}\}$
2) $\{\mathbb{R} \backslash \mathbb{Q}, \mathbb{Q}\}$
3) $\{\mathbb{R}^+ \cup \{0\}, \mathbb{R}^-\}$

Klarerweise ist die induzierte Äquivalenzrelation von 1) nichtisomorph zu 2) und 3). Die Äquivalenzrelationen von 2) und 3) sind nicht isomorph, weil es keine Bijektion von $\mathbb{Q}$ nach $\mathbb{R}^+ \cup \{0\}$ oder $\mathbb{R}^-$ gibt.

d. Wir wissen, dass wir alle konsistenten Theorien vervollständigen können, also existiert zumindest eine vollständige Theorie $\Sigma' \subseteq \Sigma_2$. In einer vollständigen Theorie wird auf jeden Fall die Formel $\sigma' = \forall x \forall y(xEy)$ entschieden. Damit wird auf jeden Fall die Anzahl der Äquivalenzklassen festgelegt. Wir können zu $\Sigma_2$ sowohl $\sigma'$, als auch $\neg\sigma'$ hinzufügen und bleiben konsistent. Damit gibt es genau zwei mögliche Vervollständigungen von $\Sigma_2$: Eine lässt nur eine unendliche Äquivalenzklasse zu, die andere erlaubt nur Modelle mit zwei unendlichen Äquivalenzklassen.
Was ist mit abzählbar / nicht abzählbar unendlichen Äquivalenzklassen? Kommen da noch mehr vollständige Theorien dazu? Was heißt "dieselben Konsequenzen" genau?

□

# Henkintheorien

**Aufgabe 7** (138)**.** Geben Sie explizit eine konsistente Henkintheorie an, deren Sprache nur ein einziges Konstantensymbol (möglicherweise aber weitere Prädikaten- und/oder Funktionssymbole) enthält.
Wenn das zu leicht ist: Geben Sie zwei derartige Theorien an, wobei die eine vollständig und die andere unvollständig sein soll.

*Lösung.* Bezeichne $c$ das einzige Konstantensymbol in unserer Sprache. Wir definieren die Theorie

$$\Sigma = \{\forall x \forall y\,(x = y)\}.$$

Ein Modell erüllt die Theorie genau dann, wenn es einelementig ist. Da es einelementige Modelle gibt ist die Theorie also erfüllbar, nach dem Gödelschen Vollständigkeitssatz daher auch konsistent. Sei nun $\mathfrak{M}$ ein Modell das $\Sigma$ erfüllt, dann ist dieses Modell schon einelementig mit dem Element $m$ und daher $c^{\mathfrak{M}} = m$. Klarerweise ist jede Formel der Form $\exists x \varphi(x) \to \varphi(c)$ erfüllt, nach dem Vollständigkeitssatz gilt also $\Sigma \vdash (\exists x \varphi(x) \to \varphi(c))$ und daher ist $\Sigma$ eine Henkintheorie. $\Sigma$ ist aber nicht vollständig, da die geschlossene Formel $\exists x R(x)$ nicht entscheidbar ist.

$$\Sigma' = \{\forall x \forall y\,(x = y = c), \exists x R(x), R(c)\}$$

ist dafür eine vollständige, konsisente Henkintheorie. □

# Außer Konkurrenz

**Aufgabe 8** (132)**.** Sei $M$ eine nichtleere Menge, $\mathscr{L}$ eine prädikatenlogische Sprache, und sei $X$ die Menge aller $\mathscr{L}$-Strukturen mit Universum $M$. Zeigen Sie:

a. Die Familie $\{\mathrm{Mod}\,(\sigma) : \sigma \text{ geschlossene Formel }\}$ bildet Basis einer 0-dimensionalen Topologie $\tau$ auf $X$. Eine Topologie heißt 0-dimensional, wenn es eine Basis gibt, die unter Komplementsen abgeschlossen ist, oder äquivalent: Wenn es eine Basis gibt, deren Mengen alle clopen, also offen und abgeschlossen, sind. Das klassische Beispiel eines 0-dimensionalen, aber nicht diskreten Raums ist die Cantormenge.

b. Im allgemeinen ist $(X, \tau)$ kein Hausdorffraum. Geben Sie eine sinnvolle Äquivalenzrelation $\sim$ auf $X$ und eine sinnvolle Topologie $\tau_\sim$ auf $X/\sim$ an, sodass $X/\sim$ Hausdorffraum ist.

c. $(X, \tau)$ ist kompakt, ebenso $(X/\sim, \tau_\sim)$, also jede offene Überdeckung hat eine endliche Teilüberdeckung.

*Lösung.*

□

**Aufgabe 9** (137)**.** Sei $\mathcal{L}$ eine prädikatenlogische Sprache, und sei $\Sigma$ eine konsistente Henkin-Theorie in der Sprache $\mathcal{L}$ mit der folgenden Eigenschaft:

Für alle Konstantensymbole $c, d$ in $\mathcal{L}$ gilt entweder $\Sigma \vdash c = d$ oder $\Sigma \vdash c \neq d$.

Weiters habe $\Sigma$ die Eigenschaft, dass es zwei Konstantensymbole $0, 1$ mit $\Sigma \vdash 0 \neq 1$ gibt. Zeigen Sie, dass $\Sigma$ vollständig sein muss.

*Lösung.*

□

**Aufgabe 10** (139)**.** Geben Sie eine Sprache $\mathscr{L}$ und zwei $\mathscr{L}$-Strukturen $\mathscr{M}_1$ und $\mathscr{M}_2$ an, sodass $\mathrm{Th}\,(\mathscr{M}_1)$ eine Henkin-Theorie ist, nicht aber $\mathrm{Th}\,(\mathscr{M}_2)$.

*Lösung.*

□

**Aufgabe 11** (140)**.** Jede Theorie mit der schwachen Henkin-Eigenschaft hat auch die starke Henkin-Eigenschaft.
*Hinweis:* Verwenden Sie die Formel $\exists x(\exists y\psi(y) \implies \psi(x))$, siehe Aufgabe 100.

*Lösung.*

□

# Logik und Grundlagen der Mathematik

*7. Übung am 19.11.2020*

Richard Weiss  Florian Schager  Fabian Zehetgruber

## Skolemtheorien

Sei $\Sigma$ eine Theorie in der Sprache $\mathscr{L}$. Wir nennen $\Sigma$ eine Skolem-Theorie, wenn es für alle $n \geq 0$ und alle Formeln der Form $\exists y \psi$ mit den freien Variablen $x_1, \ldots, x_n$ ein $n$-stelliges Funktionssymbol $f$ gibt, sodass $\Sigma \vdash \exists y \psi \to \psi[y/f(\overline{x})]$ (wobei wir $f(\overline{x})$ statt $f(x_1, \ldots, x_n)$ schreiben).
Für zwei $\mathscr{L}$-Strukturen $\mathscr{M}_1$ und $\mathscr{M}_2$ mit $M_1 \subseteq M_2$ sagen wir $\mathscr{M}_1 \leq \mathscr{M}_2$ ("$\mathscr{M}_1$ ist Unterstruktur von $\mathscr{M}_2$"), wenn für alle Funktionssymbole $f$ in $\mathscr{L}$ gilt, dass $f^{\mathscr{M}_1} = f^{\mathscr{M}_2} \restriction M_1$ (genauer: $f^{\mathscr{M}_1} = f^{\mathscr{M}_2} \restriction M_1^k$) wenn $k$ die Stelligkeit von $f$ ist), sowie $c^{\mathscr{M}_1} = c^{\mathscr{M}_2}$ für alle Konstantensymbole, und $R^{\mathscr{M}_1} = R^{\mathscr{M}_2} \cap M^k$ für alle ($k$-stelligen) Relationssymbole $R$.
Wir schreiben $\mathscr{M}_1 \preccurlyeq \mathscr{M}_2$, wenn erstens $\mathscr{M}_1 \leq \mathscr{M}_2$ gilt, und überdies für jede Formel $\varphi$ und jede Belegung $b$ mit Werten in $M_1 : \mathscr{M}_1 \vDash \varphi[b] \iff \mathscr{M}_2 \vDash \varphi[b]$.

**Aufgabe 1** (142)**.** Finden Sie ein möglichst interessantes Beispiel $\mathscr{L}, \mathscr{M}_1, \mathscr{M}_2, \varphi, b$, sodass zwar $\mathscr{M}_1 \leq \mathscr{M}_2$ gilt, aber nicht $\mathscr{M}_1 \preccurlyeq \mathscr{M}_2$ (letzteres belegt durch $\varphi$ und $b$).

*Lösung.* Sei $\mathscr{L} = (+, 0)$ die Sprache der Monoide,

$$\mathscr{M}_1 = (\mathbb{N}, +_{\mathbb{N}}, 0_{\mathbb{N}}),$$
$$\mathscr{M}_2 = (\mathbb{Z}, +_{\mathbb{Z}}, 0_{\mathbb{Z}})$$

Es gilt mit Sicherheit

$$\mathbb{N} \subseteq \mathbb{Z}, 0_{\mathbb{N}} = 0_{\mathbb{Z}}, +_{\mathbb{N}} = +_{\mathbb{Z}} \restriction \mathbb{N} \implies \mathscr{M}_1 \leq \mathscr{M}_2.$$

Die Formel

$$\varphi = \exists y \, (x + y = 0)$$

ist sicher allgemeingültig in $\mathbb{Z}$, also insbesondere unter allen Belegungen mit Werten in $\mathbb{N}$ wahr, aber $\varphi$ ist in $\mathbb{N}$ unter jeder Belegung $b$ mit $b(x) \neq 0$ falsch. □

*Lösung.* Ein vielleicht weniger interessantes Beispiel. Wir betrachten die Sprache $\mathscr{L} = \{\leq\}$ und die Modelle $\mathscr{M}_1 = \{0\}$ und $\mathscr{M}_2 = \{0, 1\}$. Außerdem betrachten wir die Formel $\forall x \forall y (x \leq y)$. Da es sich um eine geschlossene Formel handelt ist die Belegung egal, in $\mathscr{M}_1$ ist sie jedenfalls wahr und in $\mathscr{M}_2$ nicht. □

**Aufgabe 2** (143)**.** Finden Sie ein Beispiel $\mathscr{L}, \mathscr{M}_1, \mathscr{M}_2$, sodass $\mathscr{M}_1 \preccurlyeq \mathscr{M}_2$ und $M_1 \neq M_2$.

*Lösung.* Da wir das Gleichheitssymbol ohnehin in unserer Sprache haben wollen wir uns nicht weiter belasten und nicht mehr in unsere Sprache aufnehmen, also keine Konstantensymbole, Funktionssymbole oder weitere Relationssymbole. Wäre $M_1$ endlich mit $n \in \mathbb{N}$ Elementen, dann gelten wegen $|M_2| > |M_1| = n$ die Aussagen

$$\mathscr{M}_1 \nvDash \exists^{\geq n+1} \, [b], \quad \mathscr{M}_2 \vDash \exists^{\geq n+1} \, [b]$$

Also müssen $M_1$ und $M_2$ mindestens abzählbar undendlich viele Elemente haben. Wir wählen $\mathscr{M}_1 = \mathbb{N} \setminus \{0\}$ sowie $\mathscr{M}_2 = \mathbb{N}$. Wir zeigen zuerst mittels Induktion nach Formelaufbau

$$\forall \varphi \forall x \forall b \exists k \in \mathbb{N} \setminus \{0\} \forall l \geq k(x \text{ Variable }, \varphi \text{ Formel }, b \text{ Belegung mit Werten in } M_1 \Rightarrow \widehat{b_{x\to 0}}(\varphi) = \widehat{b_{x\to l}}(\varphi))$$

Für eine Atomformel der Form $x = x$ ist die Aussage Trivial, für eine der Form $x = y$ wählen wir $k > b(y)$. Exemplarisch rechnen wir

$$\widehat{b_{x\to 0}}(\varphi_1 \wedge \varphi_2) = \widehat{b_{x\to 0}}(\varphi_1) \wedge_B \widehat{b_{x\to 0}}(\varphi_2) = \widehat{b_{x\to k_1}}(\varphi_1) \wedge_B \widehat{b_{x\to k_2}}(\varphi_2) = b_{x\to \widehat{\max\{k_1,k_2\}}}(\varphi_1 \wedge \varphi_2).$$

Weiters gilt

$$\widehat{b_{x\to 0}}(\forall \varphi) = \inf\{\widehat{(b_{x\to 0})_{y\to m}}(\varphi) \mid m \in M_1\} = \inf\{\widehat{(b_{y\to m})_{x\to 0}}(\varphi) \mid m \in M_1\} = \inf\{\widehat{(b_{y\to m})_{x\to k_m}}(\varphi) \mid m \in M_1\}$$

Hier weiß ich nicht mehr weiter... □

**Aufgabe 3** (144)**.** Geben Sie ein explizites Beispiel einer konsistenten Skolemtheorie an.

*Lösung.* Wir betrachten die Theorie

$$\Sigma := \{\forall x \forall y(x = y)\}.$$

$\Sigma$ wird von jedem ein-elementigen Modell erfüllt und ist somit konsistent. Wählen wir nun eine beliebige Formel der Form $\exists y \psi$ mit den freien Variablen $x_1, \ldots, x_n$, wobei $n \in \mathbb{N}$. Aus der Vorlesung wissen wir bereits

$$\Sigma \vdash \exists y \psi \to \psi[y/f(\overline{x})] \Leftrightarrow \Sigma \vDash \exists y \psi \to \psi[y/f(\overline{x})]$$

also reicht es wenn wir zeigen, dass der rechte Ausdruck wahr ist. Nehmen wir also ein Modell $\mathscr{M}$ in dem $\Sigma$ gilt. Die Theorie sagt uns, dass unser Modell genau ein Element $m$ hat. Nun berechnen wir für eine Belegung $b$ mit $\widehat{b}(\exists \psi) = 1$ den Wert

$$\widehat{b}(\psi[y/f(\overline{x})]) = \widehat{b_{y\to \overline{b}(f(\overline{x}))}}(\psi) = \widehat{b_{y\to m}}(\psi) = \sup\{\widehat{b_{x\to k}}(\psi) \mid k \in M\} = \widehat{b}(\exists \psi) = 1$$

wobei unsere Sprache ein $n$-stelliges Funktionssymbol $f$ enthalten soll. Damit gilt für jede beliebige Belegung $b$, jede Formel $\psi$ mit freien Variablen $\overline{x}$ und jedes Modell $\mathscr{M}$ mit $\mathscr{M} \vDash \Sigma$

$$\hat{b}(\exists y \psi \to \psi[y/f(\overline{x})]) = 1 \implies \mathscr{M} \vDash \exists y \psi \to \psi[y/f(\overline{x})] \implies \Sigma \vDash \exists y \psi \to \psi[y/f(\overline{x})].$$

Also ist unsere Theorie eine Skolemtheorie. □

**Aufgabe 4** (146)**.** Sei $\Sigma$ eine Theorie, die

- Zu jeder Formel $\varphi$ gibt es eine reine Allformel $\varphi'$ (also eine Formel in Pränexformel ohne Existenzquantoren) mit $\Sigma \vdash \varphi \leftrightarrow \varphi'$

erfüllt, und seien $\mathscr{M}_1 \leq \mathscr{M}_2$ Modelle, in denen $\Sigma$ gilt. Zeigen Sie $\mathscr{M}_1 \preccurlyeq \mathscr{M}_2$.

*Lösung.* Notation: Sei $b$ Belegung mit Werten in $M_1 \subseteq M_2$:

$$\overline{b}_i := \overline{b}_{\mathscr{M}_i}, \quad i = 1, 2$$
$$\hat{b}_i := \hat{b}_{\mathscr{M}_i}, \quad i = 1, 2.$$

In einem ersten Schritt wollen wir für alle quantorenfreien Formeln $\psi$ und alle Belegungen $b$ mit Werten in $M_1$ zeigen, dass

$$\mathscr{M}_1 \vDash \varphi[b] \iff \mathscr{M}_2 \vDash \varphi[b]$$

gilt. Zuerst kümmern wir uns um die Terme.

$$\begin{aligned}
\overline{b}_1(c) &= c^{\mathscr{M}_1} = c^{\mathscr{M}_2} = \overline{b}_2(c), \\
\overline{b}_1(x) &= b(x) = \overline{b}_2(x), \\
\overline{b}_1(f(t_1, \ldots, t_k)) &= f^{\mathscr{M}_1}(\overline{b}_1(t_1), \ldots, \overline{b}_1(t_k)) = f^{\mathscr{M}_1} \underbrace{(\overline{b}_2(t_1), \ldots, \overline{b}_2(t_k))}_{\in M_1^k} = f^{\mathscr{M}_2}(\overline{b}_2(t_1), \ldots, \overline{b}_2(t_k)) = \overline{b}_2(f(t_1, \ldots, t_k))
\end{aligned}$$

Also wissen wir jetzt $\overline{b}_1 = \overline{b}_2$ und schreiben stets einfach $\overline{b}$. Insbesondere hat $\overline{b}$ nur Werte in $M_1$. Als nächstes kommen die Atomformeln. Wir berechnen

$$\widehat{b}_1(R(t_1, \ldots, t_k)) = 1 \Leftrightarrow (\overline{b}(t_1), \ldots, \overline{b}(t_k)) \in R^{\mathscr{M}_1} \Leftrightarrow (\overline{b}(t_1), \ldots, \overline{b}(t_k)) \in R^{\mathscr{M}_2} \Leftrightarrow \widehat{b}_2(R(t_1, \ldots, t_k)) = 1.$$

Schließlich berechnen wir in einem letzten Schritt exemplarisch

$$\widehat{b}_1(\psi_1 \wedge \psi_2) = \widehat{b}_1(\psi_1) \wedge_B \widehat{b}_1(\psi_2) = \widehat{b}_2(\psi_1) \wedge_B \widehat{b}_2(\psi_2) = \widehat{b}_2(\psi_1 \wedge \psi_2)$$

und haben die Aussage für alle quantorenfreien Formeln also gezeigt.

" $\Leftarrow$ " Gegeben also eine Formel $\varphi$ und eine Belegung $b$ mit Werten in $M_1$ mit $\mathscr{M}_2 \vDash \varphi\ [b]$. Nun gilt $\mathscr{M}_2 \vDash \Sigma$ und $\Sigma \vDash \varphi \leftrightarrow \varphi'$, wobei $\varphi'$ eine reine Allformel ist. Also gilt

$$\mathscr{M}_2 \vDash \varphi'\ [b], \quad \varphi' = \forall x_n \ldots \forall x_1(\psi).$$

wobei $\psi$ die Matrix, also quantorenfrei ist. Wir behaupten

$$\begin{aligned}
&\forall n \in \mathbb{N}\, \forall \psi\, \forall b\, (b \text{ Belegung mit Werten in } M_1 \wedge \psi \text{ quantorenfrei}) \\
&\qquad \Rightarrow (\mathscr{M}_2 \vDash \forall x_n \ldots \forall x_1(\psi)[b] \Rightarrow \mathscr{M}_1 \vDash \forall x_n \ldots \forall x_1(\psi)[b])
\end{aligned}$$

Ist $n = 0$ bleibt nur die quantorenfreie Formel $\psi$ stehen und die Behauptung stimmt aufgrund des oben gezeigten. Angenommen wir wissen es nun schon für $n \geq 0$, so gilt

$$\begin{aligned}
1 = \widehat{b}_2(\forall x_{n+1} \ldots \forall x_1(\psi)) &= \inf\{(\widehat{b_{x_{n+1} \to m}})_2(\forall x_n \ldots \forall x_1(\psi)) \mid m \in M_2\} \\
&\leq \inf\{(\widehat{b_{x_{n+1} \to m}})_2(\forall x_n \ldots \forall x_1(\psi)) \mid m \in M_1\} \\
&\leq \inf\{(\widehat{b_{x_{n+1} \to m}})_1(\forall x_n \ldots \forall x_1(\psi)) \mid m \in M_1\} \\
&= \widehat{b}_1(\forall x_{n+1} \ldots \forall x_1(\psi)).
\end{aligned}$$

Also gilt $\mathscr{M}_1 \vDash \varphi'\ [b]$ und wegen $\mathscr{M}_1 \vDash \varphi \leftrightarrow \varphi'$ kommen wir wieder zurück zu $\mathscr{M}_1 \vDash \varphi\ [b]$.

" $\Rightarrow$ " Hier bemerken wir, dass es zu jeder Formel $\varphi$ eine reine Existenzformel $\varphi'$ gibt mit $\Sigma \vDash \varphi \leftrightarrow \varphi'$. Um das einzusehen betrachten wir $\neg\varphi$ und finden eine reine Allformel $\tilde{\varphi}$ mit $\Sigma \vDash \neg\varphi \leftrightarrow \tilde{\varphi}$. Mit einer Tautologie folgt

$$\begin{aligned}
&\Sigma \vDash \varphi \leftrightarrow \neg\tilde{\varphi} \\
&\neg\tilde{\varphi} = \neg\forall x_1 \cdots \forall x_k\, \psi \leftrightarrow \exists x_1 \neg\forall x_1, \cdots \forall x_k \leftrightarrow \cdots \leftrightarrow \exists x_1 \cdots \exists x_k\, \neg\psi
\end{aligned}$$

und von da an kommen wir mit den Existenzaxiomen auf eine reine Existenzformel $\varphi'$. Nun können wir die andere Richtung fast vollständig wiederverwerten.
Gegeben also eine Formel $\varphi$ und eine Belegung $b$ mit Werten in $M_1$ mit $\mathscr{M}_1 \vDash \varphi\ [b]$. Nun gilt $\mathscr{M}_1 \vDash \Sigma$ und $\Sigma \vDash \varphi \leftrightarrow \varphi'$, wobei $\varphi'$ eine reine Existenzformel ist. Also gilt

$$\mathscr{M}_1 \vDash \varphi'\ [b], \quad \varphi' = \exists x_n \ldots \exists x_1(\psi).$$

wobei $\psi$ die Matrix, also quantorenfrei ist. Wir behaupten

$$\begin{aligned}\forall n \in \mathbb{N} \forall \psi \forall b((b \text{ Belegung mit Werten in } M_1 \wedge \psi \text{ quantorenfrei })\\ \Rightarrow (\mathscr{M}_1 \vDash \exists x_n \ldots \exists x_1(\psi)[b] \Rightarrow \mathscr{M}_2 \vDash \exists x_n \ldots \exists x_1(\psi)[b])\end{aligned}$$

Ist $n = 0$ bleibt nur die quantorenfreie Formel $\psi$ stehen und die Behauptung stimmt aufgrund des oben gezeigten. Angenommen wir wissen es nun schon für $n \geq 0$, so gilt

$$\begin{aligned}1 = \widehat{b}_1(\exists x_{n+1} \ldots \exists x_1(\psi)) &= \sup\{(\widehat{b_{x_{n+1} \to m}})_1(\exists x_n \ldots \exists x_1(\psi)) \mid m \in M_1\}\\ &\leq \sup\{(\widehat{b_{x_{n+1} \to m}})_1(\exists x_n \ldots \exists x_1(\psi)) \mid m \in M_2\}\\ &\leq \sup\{(\widehat{b_{x_{n+1} \to m}})_2(\exists x_n \ldots \exists x_1(\psi)) \mid m \in M_2\}\\ &= \widehat{b}_2(\exists x_{n+1} \ldots \exists x_1(\psi)).\end{aligned}$$

Also gilt $\mathscr{M}_2 \vDash \varphi' \; [b]$ und wegen $\mathscr{M}_2 \vDash \varphi \leftrightarrow \varphi'$ kommen wir wieder zurück zu $\mathscr{M}_2 \vDash \varphi \; [b]$.

□

# Skolemisierung

**Aufgabe 5** (173)**.** Finden Sie (durch Skolemisierung) eine Formel in Pränexform ohne Existenzquantoren, die zur Formel

$$\exists x \exists y \forall z \, ((P(x) \vee P(y)) \wedge \neg P(z))$$

erfüllungsäquivalent ist.

*Lösung.* Wir wissen aus der Vorlesung, dass für eine Formel $\psi$ und eine Konstante $c$, welche nicht in $\psi$ vorkommt, die Formeln

$$\begin{aligned}&\exists x \, \psi \quad \text{und}\\ &\psi[x/c]\end{aligned}$$

erfüllungsäquivalent ist. Wenden wir diese Erfüllungsäquivalent zweimal an, dann erhalten wir mit Konstanten $c, d$, welche nicht in $P$ vorkommen:

$$\forall z \, ((P(c) \vee P(d)) \wedge \neg P(z))$$

□

**Aufgabe 6** (174)**.** Finden Sie (durch Skolemisierung) eine Formel in Pränexform ohne Existenzquantoren, die zur Formel

$$\forall z \exists x \exists y \, ((P(x) \vee P(y)) \wedge \neg P(z))$$

erfüllungsäquivalent ist.

*Lösung.* Hier verwenden wir zweimal die Erfüllungsäquivalenz von

$$\begin{aligned}&\forall x \, \exists y \, \psi \quad \text{und}\\ &\forall x \, \psi[y/f(x)],\end{aligned}$$

wobei wir voraussetzen, dass $P$ eine bereinigte Formel ist. Wir erhalten also:

$$\forall z \, ((P(g(z)) \vee P(f(z))) \wedge \neg P(z)).$$

□

**Aufgabe 7** (176)**.** Finden Sie eine Formel $\forall x\, \exists y\, \varphi$, die das Funktionssymbol $f$ enthält, sodass $\forall x\, \exists y\, \varphi$ nicht erfüllbarkeitsäquivalent ist zu $\forall x\, \varphi(y/f(x))$.

*Lösung.* Wenn wir die Gleichheitsrelation verwenden dürfen:

$$\phi = \neg(y = f(x))$$

Dann ist $\forall x\, \exists y\, y = f(x)$ erfüllbar, zum Beispiel von jedem Modell mit mindestens zwei Elementen.

$$\forall x\, \neg(f(x) = f(x))$$

ist aber aufgrund den Leibniz-Axiomen nicht erfüllbar. □

*Lösung.* Wenn wir die Gleichheitsrelation nicht verwenden dürfen:

$$\varphi = (y \leq f(x)) \wedge \neg(f(x) \leq y)$$

Dann ist $\forall x\, \exists y\, ((y \leq f(x)) \wedge \neg(f(x) \leq y))$ erfüllbar, zum Beispiel von jedem Modell mit mindestens zwei Elementen, indem für die Relation $\leq$ Antisymmetrie gilt.

$$\forall x\, ((f(x) \leq f(x)) \wedge \neg(f(x) \leq f(x)))$$

ist klarerweise unerfüllbar. □

# Logik und Grundlagen der Mathematik

*8. Übung am 26.11.2020*

Richard Weiss Florian Schager Fabian Zehetgruber

## Resolution

Unter einer „Instanz“ einer Formel $\varphi$ (die meist als Klausel gegeben ist), verstehen wir jede Formel $\varphi[x_1/t_1, \ldots, x_n/t_n]$, die man durch (beliebig viele) sinnvolle Substitutionen erhält. Unter einer Grundinstanz verstehen wir eine Instanz ohne freie Variablen.

**Aufgabe 1** (182)**.** Zeigen Sie mit Hilfe der Resolutionsmethode, dass die Formeln

1. $\exists x\, \exists y\, \forall z\, ((P(x) \vee P(y)) \wedge \neg P(z))$
2. $\forall z\, \exists x\, \exists y\, ((P(x) \vee P(y)) \wedge \neg P(z))$

unerfüllbar sind.

*Lösung.*

1. Im ersten Schritt schreiben wir die Formel zur erfüllungsäquivalenten Formel von letzter Woche um:

$$\forall z\, ((P(c) \vee P(d)) \wedge \neg P(z))$$

Also betrachten wir folgende Klauselmenge:

$$\{\{P(c), P(d)\}; \{\neg P(z)\}\}$$

Resolutionsableitung:

$$\begin{aligned} &C_1 = \{P(c), P(d)\} \\ &C_2 = \{\neg P(z)\} \\ &C_3 = \mathrm{Res}(C_1, C_2) = \{P(c)\} && (\sigma : z \mapsto d) \\ &C_4 = \mathrm{Res}(C_2, C_3) = \emptyset && (\sigma : z \mapsto c) \end{aligned}$$

2. Im ersten Schritt schreiben wir die Formel zur erfüllungsäquivalenten Formel von letzter Woche um:

$$\forall z\, ((P(g(z)) \vee P(f(z))) \wedge \neg P(z))$$

Also betrachten wir folgende variablendisjunkte Klauselmenge:

$$\{\{P(g(z)), P(f(z))\}; \{\neg P(x)\}\}$$

Resolutionsableitung:

$$\begin{aligned} &C_1 = \{P(g(z)), P(f(z))\} \\ &C_2 = \{\neg P(x)\} \\ &C_3 = \mathrm{Res}(C_1, C_2) = \{P(g(z))\} && (\sigma : x \mapsto f(z)) \\ &C_4 = \mathrm{Res}(C_2, C_3) = \emptyset && (\sigma : x \mapsto g(z)) \end{aligned}$$

$\square$

**Aufgabe 2** (186)**.** Gegeben ist die Klauselmenge $M_n = \{\{P(a)\}; \{\neg P(x), P(f(x))\}; \{\neg P(f^{2^n}(a))\}\}$, wobei $f^k(a)$ wie folgt definiert ist: $f^0(a)$ ist $a$ und $f^{k+1}(a)$ ist $f(f^k(a))$. Geben Sie eine Resolutionswiderlegung von $M_n$ mit $\mathcal{O}(n)$ Schritten an. Zeigen Sie, dasss jede AL-Resolutionswiderlegung von $G(M_n)$ mindestens $2^n$ Schritte hat.

*Lösung.* Wir zeigen mittels Induktion

$$\forall k \in \mathbb{N} : \text{mit } 2k \text{ Schritten erreichen wir } \left\{\neg P(x), P\Big(f^{2^k}(x)\Big)\right\}$$

Für $k = 0$ brauchen wir tatsächlich 0 Schritte, da $\{\neg P(x), P(f(x))\} \in M_n$. Nehmen wir für $k \in \mathbb{N}$ nun an, dass in $2k$ Schritten die Menge $\left\{\neg P(x), P\Big(f^{2^k}(x)\Big)\right\}$ erreicht werden kann, so können wir mit $x/f^{2^k}(x)$ die Menge $\left\{\neg P\Big(f^{2^k}(x)\Big), P\Big(f^{2^{k+1}}(x)\Big)\right\}$ erreichen und dann resolvieren um $\left\{\neg P(x), P\Big(f^{2^{k+1}}(x)\Big)\right\}$ zu erhalten. Wenn wir das in $k$ Schritten erreicht haben, müssen wir nur noch zweimal resolvieren, um zuerst $\{P(f^{2^k(a)})\}$ und anschließend $\emptyset$ zu erhalten.

$$G(M_n) = \{\{P(a)\}; \{\neg P(f^{2^n}(a))\}\} \cup \{\{\neg P(x/t), P(f(x/t))\} : t \text{ variablenfreier Term}\}$$

Nun gibt es drei sinnvolle Typen von Resolutionen:

1. $$\begin{aligned} C_{j_1} &= \{P(f^k(a))\} \\ C_{j_2} &= \{\neg P(f^k(a)); P(f^{k+1}(a))\} \\ \mathrm{Res}(C_{j_1}, C_{j_2}) &= \{P(f^{k+1}(a))\} \end{aligned}$$

2. $$\begin{aligned} C_{j_1} &= \{\neg P(f^k(a))\} \\ C_{j_2} &= \{\neg P(f^{k-1}(a)); P(f^k(a))\} \\ \mathrm{Res}(C_{j_1}, C_{j_2}) &= \{\neg P(f^{k-1}(a))\} \end{aligned}$$

3. $$\begin{aligned} C_{j_1} &= \{\neg P(f^{k-1}(a)); P(f^k(a))\} \\ C_{j_2} &= \{\neg P(f^k(a)); P(f^{k+1}(a))\} \\ \mathrm{Res}(C_{j_1}, C_{j_2}) &= \{\neg P(\neg f^{k-1}(a)); P(f^{k+1}(a))\} \end{aligned}$$

Iterierte Anwendung einer beliebigen Kombination dieser Strategien führt mit $\geq 2^n$ Schritten zum Ziel, da in jedem Schritt nur eine $f$-Potenz „gewonnen“ wird. $\square$

# Primitiv rekursive Funktionen

Wir nennen eine Relation $R \subseteq \mathbb{N}^n$ primitiv rekursiv (genauer: „primitiv rekursive Relation“ oder „primitiv rekursiv als Relation“), wenn ihre charakteristische Funktion $\chi_R$ primitiv rekursiv ist.
ACHTUNG: Es gibt Funktionen, die zwar nicht primitiv rekursiv sind, die aber in diesem Sinn eine primitiv rekursive Relation sind.
In jeder der folgenden Aufgaben dürfen Sie die jeweils vorigen Aufgaben verwenden.

**Aufgabe 3** (194 + 195)**.** Zeigen Sie, dass mehrere der folgenden Funktionen primitiv rekursiv sind: (Manche dieser Funktionen sind gelegentlich undefiniert, z.B. an der Stelle 0. Setzen Sie die Funktion so zu einer totalen Funktion fort, dass Sie von der Fortsetzung zeigen können, dass sie primitiv rekursiv ist.)

**Geben Sie explizit die primitiv rekursiven Funktionen $h$ und $g$ an, die Sie im Schema der primitiven Rekursion [1] verwenden.**

1. Addition, Multiplikation, $n!$, modulo-Funktion, $\binom{n}{k}$
2. Die durch
$$f(x) = \begin{cases} g(x) & \text{wenn } x \in A \\ h(x) & \text{sonst} \end{cases}$$
definierte Funktion, wenn $g, h$ primitiv rekursive Funktionen sind und $A$ eine primitiv rekursive Menge.
3. Die charakteristische Funktion jeder endlichen Menge.
4. $(n, k) \mapsto (q, r)$ mit $qk + r = n,\ 0 \leq r < k$.
5. $(n, k) \mapsto \lfloor \frac{n}{k} \rfloor$. (Gaußklammer)
6. $(n, k) \mapsto \max(0, \lfloor \frac{p(n)}{q(k)} \rfloor)$, wobei $p$ und $q$ beliebige Polynome mit ganzzahligen (möglicherweise negativen) Koeffizienten sind.
7. Die Funktion $(n, k) \mapsto k$-te Dezimalstelle von $n$.
8. $n \mapsto \lfloor \sqrt{2} * 10^n \rfloor$.
9. Eine geeignete (von Ihnen zu wählende) injektive (bijektive?) Abbildung $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$.
10. Die Fibonacci-Folge $f(0) = f(1) = 1,\ f(n + 2) = f(n + 1) + f(n)$.
*Hinweis:* Betrachten Sie zunächst die Funktion $n \mapsto 2^{f(n)} \cdot 3^{f(n+1)}$.
11. Ihre Lieblingsfunktion. (Möglichst nichttrivial.)

*Lösung.*

1. Addition $+ = \mathrm{PR}(\pi_1^1, s \circ \pi_3^3)$:
$$\forall x \in \mathbb{N} : +(x, 0) = x + 0 = x = \pi_1^1(x)$$
$$\forall x, y \in \mathbb{N} : +(x, y + 1) = x + (y + 1) = (x + y) + 1 = s \circ \pi_3^3(x, y, +(x, y))$$
Multiplikation $\cdot = \mathrm{PR}(0, +(\pi_1^3, \pi_3^3))$:
$$\forall x \in \mathbb{N} : \cdot(x, 0) = x \cdot 0 = 0$$
$$\forall x, y \in \mathbb{N} : \cdot(x, y + 1) = x(y + 1) = xy + x = +(\pi_1^3, \pi_3^3)(x, y, \cdot(x, y))$$
Vorgänger $v = \mathrm{PR}(0, s \circ \pi_1^2)$:
$$\forall x \in \mathbb{N}^0 : v(, 0) = 0$$
$$\forall x \in \mathbb{N}^0\, \forall y \in \mathbb{N} : v(, y + 1) = y + 1 - 1 = y = s \circ \pi_1^2(, y, v(, y))$$

[1] Gemeint ist eine Definition der Form $f(\vec{x}, 0) = h(\vec{x}),\ f(\vec{x}, y + 1) = g(\vec{x}, f(\vec{x}, y), y)$. Aus notationellen Gründen treten oft die als trivial geltenden Projektionen $\Pi_k^n$ auf.

Subtraktion $- = \mathrm{PR}(\pi_1^1, v \circ \pi_3^3)$:

$$\forall x \in \mathbb{N} : -(x,0) = x - 0 = x = \pi_1^1(x)$$
$$\forall x \in \mathbb{N}\, \forall y \in \mathbb{N} : -(x, y+1) = x - (y+1) = (x-y) - 1 = v \circ \pi_3^3(x, y, -(x,y))$$

Faktorielle $! = \mathrm{PR}(s \circ 0, \cdot(s \circ \pi_1^2, \pi_2^2))$:

$$\forall x \in \mathbb{N}^0 : 0! = 1 = s \circ 0(,)$$
$$\forall x \in \mathbb{N}^0\, \forall y \in \mathbb{N} : (y+1)! = y!(y+1) = \cdot(s \circ \pi_1^2, \pi_2^2)(, y, y!)$$

2.

$$f(x) = \begin{cases} g(x) & \text{wenn } x \in A \\ h(x) & \text{sonst} \end{cases},$$

wobei $f, g, \chi_A$ primitiv rekursive Funktionen sind.

$$\begin{aligned} f(x) &= \chi_A(x)g(x) + (1 - \chi_A(x))h(x) \\ &= +(\cdot(\chi_A, g), \cdot(-(1, \chi_A), h))(x) \end{aligned}$$

3. $\chi_{\{0\}}$

$$\begin{aligned} \chi_{\{0\}}(0) &= 1 = s \circ 0 \\ \forall y \in \mathbb{N} : \chi_{\{0\}}(y+1) &= 0 \end{aligned}$$

$\chi_{\{a\}}$ für $a \in \mathbb{N}$

$$\chi_{\{a\}}(x) = \chi_{\{0\}}(a - x)\chi_{\{0\}}(x - a)$$

$\chi_A$ für eine endliche Menge $A = \{a_1, \ldots, a_l\} \subseteq \mathbb{N}$

$$\chi_A = \chi_{\{a_1\}} + \cdots + \chi_{\{a_l\}}$$

4. Modulo: $\mathrm{mod}(x, y) := y \bmod x$

$$\forall x \in \mathbb{N} : \mathrm{mod}(x, 0) = 0$$
$$\forall x \in \mathbb{N}\, \forall y \in \mathbb{N} : \mathrm{mod}(x, y+1) = \begin{cases} 0 = 0 \circ \pi_1^3(x, y, \mathrm{mod}(x,y)), & y + 1 = x \\ y + 1 = s \circ \pi_2^3(x, y, \mathrm{mod}(x,y)), & \text{sonst} \end{cases}$$

Definiere $A := \{(x, x+1, z) : x, z \in \mathbb{N}\}$

$$\begin{aligned} \forall x \in \mathbb{N}\, \forall z \in \mathbb{N} : \chi_A(x, 0, z) &= 0 \\ \forall x \in \mathbb{N}\, \forall z \in \mathbb{N} :\ \forall y \in \mathbb{N} : \chi_A(x, y+1, z) &= \chi_{\{0\}}(x - y)\chi_{\{0\}}(y - x) \\ &= \cdot(\chi_{\{0\}}(-(\pi_1^4, \pi_2^4)), \chi_{\{0\}}(-(\pi_2^4, \pi_1^4)))(x, y, z, \chi_A(x, y, z)) \end{aligned}$$

5. konstante Funktion als Verknüpfung von konstanter Nullfunktion und Nachfolgerfunktion

$$k = 0 + \sum_{i=1}^{k} 1$$

6. Division mit Rest:

$$\forall y \in \mathbb{N} : \%(0, y) = (0, 0)$$

$$\forall x \in \mathbb{N}\, \forall y \in \mathbb{N} : \%(x+1, y) = \begin{cases} (0,0), & y = 0 \\ (\pi_1^2(\%(x,y)), \pi_2^2(\%(x,y)) + 1), & (\pi_2^2(\%(x,y)) + 1 < y) \wedge y > 0 \\ (\pi_1^2(\%(x,y)) + 1, 0), & \text{sonst} \end{cases}$$

Sowohl $A_1 := \{(x, 0, z) : x \in \mathbb{N}, z \in \mathbb{N}\}$, als auch $A_2 := \{(x, y, z) : z + 1 < y, x, y, z \in \mathbb{N}\}$ sind primitiv rekursiv.

$$\forall x \in \mathbb{N}\, \forall z \in \mathbb{N} : \chi_{A_2}(x, 0, z) = 0$$
$$\forall x \in \mathbb{N}\, \forall z \in \mathbb{N}\, \forall y \in \mathbb{N} : \chi_{A_2}(x, y+1, z) = \chi_{\{0\}}(y - z)(x, y, z)$$

7. Division (Gaußklammer): $\lfloor \frac{n}{k} \rfloor = \pi_1^2 \circ \%(n, k)$

8. Binomialkoeffizient: (Wir setzen $\binom{x}{y} = 0$ für $y > x$)

$$\forall x \in \mathbb{N} : \binom{0}{x} = \chi_{\{0\}}(x)$$

$$\forall x \in \mathbb{N}\, \forall y \in \mathbb{N} : \binom{y+1}{x} = \begin{cases} \chi_{\{0\}}(x - y - 1)\chi_{\{0\}}(y + 1 - x), & y + 1 \leq x \\ \lfloor \frac{(y+1)\binom{y}{x}}{y+1-x} \rfloor, & \text{sonst} \end{cases}$$

9. bijektive Abbildung zwischen $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$: gemäß dem Cantorschen Diagonalverfahren summieren wir die Diagonalen jeweils von links unten nach rechts oben auf

$$f(k, n) := k + \sum_{i=1}^{n+k} i = k + \frac{(n+k)(n+k+1)}{2}$$
$$\begin{pmatrix} 0+0 & 0+1 & 0+3 & 0+6 & \cdots \\ 1+1 & 1+3 & 1+6 & \cdots & \\ 2+3 & 2+6 & \cdots & & \\ 3+6 & \cdots & & & \end{pmatrix}$$

10. Potenzieren einer Zahl $a \in \mathbb{N}$.

$$a^0 = 1, \quad a^{n+1} = a^n a$$

11. $d : (n, k) \to k$-te Dezimalstelle von $n$. Wir schreiben dafür

$$n = \sum_{i=0}^{l} c_i 10^i$$

und erkennen

$$\left\lfloor \frac{n}{10^k} \right\rfloor - 10 \left\lfloor \frac{n}{10^{k+1}} \right\rfloor = \left\lfloor \sum_{i=k}^{l} a_i 10^{i-k} + \underbrace{10^{-k} \sum_{i=0}^{k-1} c_i 10^i}_{<1} \right\rfloor - 10 \left\lfloor \sum_{i=k+1}^{l} a_i 10^{i-(k+1)} + \underbrace{10^{-(k+1)} \sum_{i=0}^{k} c_i 10^i}_{<1} \right\rfloor$$
$$= \sum_{i=k}^{l} a_i 10^{i-k} - \sum_{i=k+1}^{l} a_i 10^{i-k} = a_k$$

12. Wurzel $\lfloor\sqrt{n}\rfloor$

$$\begin{aligned}\left\lfloor\sqrt{0}\right\rfloor &= 0\\ \forall n\in\mathbb{N}: \lfloor\sqrt{n+1}\rfloor &= \left(\lfloor\sqrt{n}\rfloor+1\right)\tilde{\chi}(n)+\lfloor\sqrt{n}\rfloor\,(1-\tilde{\chi}(n))\end{aligned}$$

wobei

$$\tilde{\chi}(n) := \chi_{\{0\}}\Big(\left(\lfloor\sqrt{n}\rfloor+1\right)^2-(n+1)\Big)\chi_{\{0\}}\Big((n+1)-\left(\lfloor\sqrt{n}\rfloor+1\right)^2\Big)$$

13. $n\to\lfloor 10^n\sqrt{2}\rfloor$

$$\begin{aligned}\left\lfloor 10^0\sqrt{2}\right\rfloor &= 1\\ \left\lfloor 10^{n+1}\sqrt{2}\right\rfloor = 10\left\lfloor 10^n\sqrt{2}\right\rfloor &+ d\Big(\left\lfloor\sqrt{2\cdot 10^{2(n+1)}}\right\rfloor,0\Big)\end{aligned}$$

oder aber

$$\left\lfloor 10^n\sqrt{2}\right\rfloor = \sum_{i=0}^{n} d\Big(\left\lfloor\sqrt{2\cdot 10^{2n}}\right\rfloor,i\Big)10^i$$

14. Fibonacci-Folge: Betrachte zuerst die primitiv rekursive Funktion

$$\begin{aligned}g(0) &= (1,1)\\ g(n+1) &= (\pi_1^2\circ g(n)+\pi_2^2\circ g(n),\pi_1^1\circ g(n)).\end{aligned}$$

Jetzt gilt $f(n)=\pi_1^2\circ g(n)$ ist als Verknüpfung primitiv rekursiver Funktionen wieder primitiv rekursiv.

□

**Aufgabe 4** (196)**.** Sei $f:\mathbb{N}\to\mathbb{N}$ primitiv rekursiv. Dann ist auch die durch $(\Sigma f)(n) := \sum_{i<n} f(i)$ definierte Funktion primitiv rekursiv, und überdies (schwach) monoton wachsend.

Sei umgekehrt $g:\mathbb{N}\to\mathbb{N}$ schwach monoton wachsend. Wenn $g$ primitiv rekursiv ist, dann ist auch die durch $(\Delta g)(n) := g(n+1)-g(n)$ definierte Funktion primitiv rekursiv.

*Lösung.*

$$\begin{aligned}(\Sigma f)(0) &= \Sigma_\emptyset = 0.\\ \forall n\in\mathbb{N}: (\Sigma f)(n+1) &= (\Sigma f)(n)+f(n)\end{aligned}$$

und $\Delta g = -(g\circ s, g)$ ist als Verknüpfung von primitiv rekursiven Funktionen wieder primitiv rekursiv.

□

# Nachtrag: Elementare Untermodelle

**Aufgabe 5** (203)**.** Seien $\mathscr{M}_1\leq\mathscr{M}_2$ mit folgender Eigenschaft: Für alle $k$ und endliche Mengen $E\subseteq M_1$ der Größe $k$ und für alle $b\in M_2$ gibt es einen Automorphismus $\pi: M_2\to M_2$, der einerseits alle Elemente von $E$ auf sich selbst abbildet, aber andererseits $\pi(b)\in M_1$ erfüllt.
Zeigen Sie, dass dann $\mathscr{M}_1\preccurlyeq\mathscr{M}_2$ gilt.
*Hinweis:* Induktion nach Aufbau von $\varphi$.

*Lösung.* Wir zeigen zuerst mit Induktion nach dem Formelaufbau

$$\forall\varphi\Big(\varphi \text{ Formel } \Rightarrow \forall b\forall\pi : (b \text{ Belegung mit Werten in } M_2, \pi \text{ Automorphismus } \Rightarrow \widehat{\pi\circ b}(\varphi) = \widehat{b}(\varphi))\Big)$$

Für eine beliebige Variable $x$ und eine beliebige Konstante $c$ gilt

$$\overline{\pi\circ b}(x) = \pi(b(x)) = \pi\big(\overline{b}(x)\big), \quad \overline{\pi\circ b}(c) = c^{\mathscr{M}_2} = \pi\big(c^{\mathscr{M}_2}\big) = \pi\big(\overline{b}(c)\big)$$

und für Terme $t_1,\dots,t_k$ mit $\forall i\in\{1,\dots,k\} : \overline{\pi\circ b}(t_i) = \pi\big(\overline{b}(t_i)\big)$ und ein beliebiges $k$-stelliges Funktionssymbol $f$ gilt

$$\begin{aligned}\overline{\pi\circ b}(f(t_1,\dots,t_k)) &= f^{\mathscr{M}_2}\big(\overline{\pi\circ b}(t_1),\dots,\overline{\pi\circ b}(t_k)\big) = f^{\mathscr{M}_2}\big(\pi\big(\overline{b}(t_1)\big),\dots,\pi\big(\overline{b}(t_k)\big)\big)\\ &= \pi\big(f^{\mathscr{M}_2}\big(\overline{b}(t_1),\dots,\overline{b}(t_k)\big)\big) = \pi\big(\overline{b}(f(t_1,\dots,t_k))\big)\end{aligned}$$

Also gilt für alle Terme $t$ die Gleichheit $\overline{\pi\circ b}(t) = \pi\big(\overline{b}(t)\big)$.
Nun schauen wir uns die Atomformeln an und betrachten dafür Terme $t_1,\dots,t_k$ und ein $k$-stelliges Relationssymbol $R$. Es gilt

$$\begin{aligned}\widehat{\pi\circ b}(R(t_1,\dots,t_k)) = 1 &\Leftrightarrow \big(\overline{\pi\circ b}(t_1),\dots,\overline{\pi\circ b}(t_k)\big) \in R^{\mathscr{M}_2} \Leftrightarrow \big(\pi\big(\overline{b}(t_1)\big),\dots,\pi\big(\overline{b}(t_k)\big)\big) \in R^{\mathscr{M}_2}\\ &\Leftrightarrow \big(\overline{b}(t_1),\dots,\overline{b}(t_k)\big) \in R^{\mathscr{M}_2} \Leftrightarrow \widehat{b}(R(t_1,\dots,t_k)) = 1\end{aligned}$$

Für zwei Formeln $\varphi,\psi$ mit $\widehat{\pi\circ b}(\varphi) = \widehat{b}(\varphi)$ und $\widehat{\pi\circ b}(\psi) = \widehat{b}(\psi)$ gilt exemplarisch für alle Junktoren

$$\widehat{\pi\circ b}(\varphi\wedge\psi) = \widehat{\pi\circ b}(\varphi) \wedge_B \widehat{\pi\circ b}(\psi) = \widehat{b}(\varphi)\wedge_B \widehat{b}(\psi) = \widehat{b}(\varphi\wedge\psi)$$

Zuletzt zeigen wir noch für den Allquantor

$$\begin{aligned}\widehat{\pi\circ b}(\forall\varphi) &= \inf\Big\{\widehat{(\pi\circ b)_{x\to m}}(\varphi) \mid m\in M_2\Big\} = \inf\Big\{\widehat{\pi\circ b_{x\to\pi^{-1}(m)}}(\varphi) \mid m\in M_2\Big\}\\ &= \inf\Big\{\widehat{b_{x\to\pi^{-1}(m)}}(\varphi) \mid m\in M_2\Big\} = \inf\Big\{\widehat{b_{x\to m}}(\varphi) \mid m\in M_2\Big\} = \widehat{b}(\forall\varphi)\end{aligned}$$

Für den Existenzquantor geht es analog.
Nun wollen wir nocheinmal eine Induktion nach dem Formelaufbau durchführen und so für alle Belegungen $b$ mit Werten in $M_1$ zeigen, dass

$$\mathscr{M}_1 \vDash \varphi[b] \iff \mathscr{M}_2 \vDash \varphi[b]$$

gilt.
Notation: Sei $b$ Belegung mit Werten in $M_1\subseteq M_2$:

$$\begin{aligned}\overline{b}_i &:= \overline{b}_{\mathscr{M}_i}, \quad i=1,2\\ \hat{b}_i &:= \hat{b}_{\mathscr{M}_i}, \quad i=1,2.\end{aligned}$$

Zuerst schauen wir uns die Atomformeln an und beschäftigen uns dafür zuerst mit den Termen.

$$\begin{aligned}\overline{b}_1(c) &= c^{\mathscr{M}_1} = c^{\mathscr{M}_2} = \overline{b}_2(c),\\ \overline{b}_1(x) &= b(x) = \overline{b}_2(x),\\ \overline{b}_1(f(t_1,\dots,t_k)) &= f^{\mathscr{M}_1}(\overline{b}_1(t_1),\dots,\overline{b}_1(t_k)) = f^{\mathscr{M}_1}\underbrace{(\overline{b}_2(t_1),\dots,\overline{b}_2(t_k))}_{\in M_1^k} = f^{\mathscr{M}_2}(\overline{b}_2(t_1),\dots,\overline{b}_2(t_k)) = \overline{b}_2(f(t_1,\dots,t_k))\end{aligned}$$

Also wissen wir jetzt $\overline{b}_1 = \overline{b}_2$ und schreiben stets einfach $\overline{b}$. Insbesondere hat $\overline{b}$ nur Werte in $M_1$.

Nun berechnen wir

$$\widehat{b}_1(R(t_1,\dots,t_k)) = 1 \Leftrightarrow (\bar{b}(t_1),\dots,\bar{b}(t_k)) \in R^{\mathscr{M}_1} \Leftrightarrow (\bar{b}(t_1),\dots,\bar{b}(t_k)) \in R^{\mathscr{M}_2} \Leftrightarrow \widehat{b}_2(R(t_1,\dots,t_k)) = 1.$$

Nun ist die gewünschte Aussage für Atomformeln also gezeigt. Für Verträglichkeit mit den Junktoren berechnen wir exemplarisch

$$\widehat{b}_1(\psi_1 \wedge \psi_2) = \widehat{b}_1(\psi_1) \wedge_B \widehat{b}_1(\psi_2) = \widehat{b}_2(\psi_1) \wedge_B \widehat{b}_2(\psi_2) = \widehat{b}_2(\psi_1 \wedge \psi_2).$$

Zu guter Letzt müssen wir uns um die Quantoren kümmern. Wir betrachten eine Formel $\varphi$ für welche alle Belegungen $a$ mit Werten in $M_1$ die Gleichheit $\hat{a}_1(\varphi) = \hat{a}_2(\varphi)$ gilt.

$$E := \{b(y) : y \in \mathrm{Var}(\varphi) \backslash \{x\}\}$$

Für jedes $m \in M_2$ sei nun $\pi_m$ ein Automorphismus, der $E$ festhält und $m$ nach $M_1$ schickt. Es gilt

$$\begin{aligned} \widehat{b}_1(\forall x\, \varphi) &= \inf \left\{ \left(\widehat{b_{x\to m}}\right)_1(\varphi) \mid m \in M_1 \right\} \\ &\geq \inf \left\{ \left(\widehat{b_{x\to m}}\right)_1(\varphi) \mid m \in M_2 \right\} = \widehat{b}_2(\forall x\, \varphi) \end{aligned}$$

Aufgrund $\pi_m(m) \in M_1$, $\pi_m \widehat{\circ (b_{x\to m})} = \widehat{\pi_m \circ (b)}_{x\to\pi_m(m)}$ und $b_{x\to m}(y) = \pi_m \circ b_{x\to\pi_m(m)}(y)$ für alle $y \in \mathrm{Var}(\varphi)$ und $m \in M_2$ gilt sogar

$$\begin{aligned} \widehat{b}_1(\forall x\, \varphi) &= \inf \left\{ \left(\widehat{b_{x\to m}}\right)_1(\varphi) \mid m \in M_1 \right\} = \inf \left\{ \left(\widehat{b_{x\to m}}\right)_2(\varphi) \mid m \in M_1 \right\} \\ &\leq \inf \left\{ \left(\widehat{\pi_m \circ (b)}_{x\to\pi_m(m)}\right)_2(\varphi) \mid m \in M_2 \right\} = \inf \left\{ \left(\pi_m \widehat{\circ (b_{x\to m})}\right)_2(\varphi) \mid m \in M_2 \right\} \\ &= \inf \left\{ \left(\widehat{b_{x\to m}}\right)_2(\varphi) \mid m \in M_2 \right\} = \widehat{b}_2(\forall x\, \varphi) \end{aligned}$$

und damit sind wir fertig! □

**Aufgabe 6** (204)**.** Wir betrachten eine Sprache $\mathscr{L}$, die keine Konstanten und keine Funktionssymbole enthält, und als einziges Relationssymbol die Gleichheit. Seien $M_1 \subseteq M_2$ unendliche Mengen; wir fassen sie als $\mathscr{L}$-Strukturen $\mathscr{M}_1$, bzw. $\mathscr{M}_2$ auf. Verwenden Sie die vorige Aufgabe, um $\mathscr{M}_1 \preccurlyeq \mathscr{M}_2$ zu zeigen.

*Lösung.* Wir müssen hier nur noch für alle endliche Mengen $E \subseteq M_1$ und alle $b \in M_2$ einen Automorphismus $\pi$ finden, der $\pi|_E = \mathrm{id}_E$ und $\pi(b) \in M_1$ erfüllt.
Seien dazu $E \subseteq M_1, b \in M_2$ beliebig.

- Fall 1: $b \in M_1$:
  Wir können $\pi = \mathrm{id}_{M_2}$ wählen.

- Fall 2: $b \notin M_1$:
  Da $E \subset M_1$ eine endliche Menge ist, finden wir ein $m_0 \in M \backslash E$ und wir definieren

  $$\pi(m) = \begin{cases} m_0, & m = b \\ b, & m = m_0 \\ m, & \text{sonst} \end{cases}$$

  Klarerweise gilt $\pi|_E = id_E$ und $\pi$ ist auch bijektiv. Mit Aufgabe 203 erhalten wir damit bereits schon $\mathscr{M}_1 \preccurlyeq \mathscr{M}_2$.

□

# Logik und Grundlagen der Mathematik

*8. Übung am 26.11.2020*

Richard Weiss Florian Schager Fabian Zehetgruber

## Primitiv rekursive Funktionen

Wir nennen eine Relation $R \subseteq \mathbb{N}^n$ primitiv rekursiv (genauer: „primitiv rekursive Relation" oder „primitiv rekursiv als Relation"), wenn ihre charakteristische Funktion $\chi_R$ primitiv rekursiv ist.
ACHTUNG: Es gibt Funktionen, die zwar nicht primitiv rekursiv sind, die aber in diesem Sinn eine primitiv rekursive Relation sind.
In jeder der folgenden Aufgaben dürfen Sie die jeweils vorigen Aufgaben verwenden.

**Aufgabe 1** (200)**.** Es gibt eine nicht berechenbare totale Funktion $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, sodass die durch $f_n(k) := g(n,k)$ und $h_k(n) := g(n,k)$ definierten Funktionen $f_0, f_1, \dots, h_0, h_1, \dots : \mathbb{N} \to \mathbb{N}$ alle berechenbar (sogar primitiv rekursiv) sind.
*Hinweis:* Fassen Sie die Funktion aus der vorigen Aufgabe als Teilmenge von $\mathbb{N} \times \mathbb{N}$ auf.

*Lösung.* Wir setzten voraus, dass wir bereits eine nicht berechenbare Funktion $\beta : \mathbb{N} \to \mathbb{N}$ kennen. Nun betrachten wir

$$\alpha : \mathbb{N} \to \mathbb{N} : n \mapsto \sum_{i=0}^{n} (\beta(i) + 1)$$

Diese Funktion ist strikt monoton wachsend, daher auch injektiv und nicht berechenbar, denn sonst wäre auch $\Delta\alpha(n) = \alpha(n+1) - \alpha(n) = \beta(n+1) + 1$ berechenbar. Nun definieren wir

$$g : \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (n,k) \mapsto \begin{cases} 0 & \text{, falls } \alpha(n) = k \\ 1 & \text{, sonst} \end{cases}$$

Nun erhalten wir für beliebiges $n \in \mathbb{N}$

$$f_n : \mathbb{N} \to \mathbb{N} : k \mapsto g(n,k) = \begin{cases} 0 & \text{, falls } \alpha(n) = k \\ 1 & \text{, sonst} \end{cases}$$

Es gilt $f_n = 1 - \chi_{\{\alpha(n)\}}$ und ist damit berechenbar. Weiters definieren wir für beliebiges $k \in \mathbb{N}$ die Funktion

$$h_k : \mathbb{N} \to \mathbb{N} : n \mapsto g(n,k) = \begin{cases} 0 & \text{, falls } \alpha(n) = k \\ 1 & \text{, sonst} \end{cases}$$

Wegen der Injektivität von $\alpha$ gibt es höchstens ein $l \in \mathbb{N}$ mit $\alpha(l) = k$ und daher ist $h_k$ entweder die konstante Einsfunktion oder an einer Stelle 0 und sonst 1, also berechenbar. Wäre allerdings $g$ berechenbar, so auch

$$\mu g : \mathbb{N} \to \mathbb{N} : n \mapsto \min\{k \in \mathbb{N} \mid g(n,k) = 0\} = \min\{k \in \mathbb{N} \mid f_n(k) = 0\} = \alpha(n)$$

was nicht sein kann. $\square$

## 201/202

**Aufgabe 2** (201)**.** Sei $E \subseteq \mathbb{N}^2$ primitiv rekursiv als Relation, und seien $f, g : \mathbb{N} \to \mathbb{N}$ primitiv rekursiv. Dann ist auch $F := \{(n,k) : (f(n), g(k)) \in E\}$ primitiv rekursiv.

*Lösung.* Es gilt $\chi_F = \chi_E(f \circ \pi_1^2, g \circ \pi_2^2)$.

□

**Aufgabe 3** (202)**.** Sei $P \subseteq \mathbb{N}^k \times \mathbb{N}$ primitiv rekursiv. Dann ist auch die Funktion

$$f(\vec{x}, z) = \min(\{y < z : (\vec{x}, y) \in P\} \cup \{z\})$$

primitiv rekursiv.

*Lösung.*

□

# Programmierung

Sei $p : \mathbb{N}^3 \to \mathbb{N}$ eine injektive primitiv rekursive Funktion, die außerdem $p(a,b,c) > \max(a,b,c)$ für alle $a, b, c$ erfüllt. Wir definieren eine Folge $f_k$ von primitiv rekursiven Funktionen so:
$f_0$ ist die 0-stellige konstante Funktion 0, $f_1$ ist die 1-stellige konstante Funktion 0.
Für $n = p(a,b,c)$: Wenn $a = 0$, dann ist $f_n$ die konstante $b$-stellige Funktion 0. Wenn $a = 1$, dann ist $f_n$ die Nachfolgerfunktion $S : \mathbb{N} \to \mathbb{N}$. Wenn $a = 2$ und $b \geq c \geq 1$, dann ist $f_n = \pi_c^b$. Wenn $a = 3$, und $f_b : \mathbb{N}^k \to \mathbb{N}^l$, $f_c : \mathbb{N}^k \to \mathbb{N}$, dann ist $f_n : \mathbb{N}^k \to \mathbb{N}^l \times \mathbb{N} = \mathbb{N}^{l+1}$ als $f_n(\overline{x}) = (f_b(\overline{x}), f_c(\overline{x}))$. Wenn $a = 4$, $f_b : \mathbb{N}^k \to \mathbb{N}^l$, $f_c : \mathbb{N}^l \to \mathbb{N}^m$, dann ist $f_n := f_c \circ f_b$. Wenn $a = 5$ und $f_b$ $(k+2)$-stellig, $f_c$ $k$-stellig, dann ist $f_n : \mathbb{N}^{k+1} \to \mathbb{N}$ durch $f_n = \mathrm{PR}(f_b, f_c)$ definiert. Sonst sei $f_n$ die konstante einstellige Nullfunktion.

**Aufgabe 4** (205)**.** Zeigen Sie, dass die Menge $\{f_n : n \in \mathbb{N}\}$ genau die Menge aller primitiv rekursiven Funktionen ist, und dass es für jede primitiv rekursive Funktion $f$ unendlich viele $n \in \mathbb{N}$ mit $f = f_n$ gibt. (Und wenn das nicht stimmt, weil in der Definition der $f_n$ eine Klausel fehlt, dann korrigieren Sie die Definition.)

*Lösung.* Wir zeigen zuerst mittels vollständider Induktion, dass jedes $f_n$ primitiv rekursiv ist.
$f_0$ und $f_1$ sind klarerweise primitv rekursiv.
Gelte nun für alle $i \leq n : f_i$ ist primitiv rekursiv:

- Fall $n+1 = p(a,b,c)$, $a \leq 2$: Klar.
- Fall $n+1 = p(a,b,c)$, $a = 3$, $f_b : \mathbb{N}^k \to \mathbb{N}^l$, $f_c : \mathbb{N}^k \to \mathbb{N}$:
  $a, b \leq \max(a,b,c) < p(a,b,c) = n+1$, also sind $f_b, f_c$ nach Induktionsvoraussetzung primitiv rekursiv und somit sind alle $\pi_i^{l+1} \circ f_{n+1}$ primitiv rekursiv.
- Fall $n+1 = p(a,b,c)$, $a = 4$, $f_b : \mathbb{N}^k \to \mathbb{N}^l$, $f_c : \mathbb{N}^l \to \mathbb{N}^m$:
  Wieder sind nach Induktionsvoraussetzung $f_b, f_c$ primitiv rekursiv und daher auch $f_c \circ f_b$.
- Fall $n+1 = p(a,b,c)$, $a = 5$:
  Wieder sind nach Induktionsvoraussetzung $f_b, f_c$ primitiv rekursiv und daher auch $\mathrm{PR}(f_c, f_b)$.
- Sonst: Klar.

Wir zeigen als nächstes mit Induktion nach der Definition von primitv rekursiven Funktionen, dass für jedes primitv rekursives $f$ unendliche viele $n$ mit $f_n = f$ existieren:

- $f = 0 : \mathbb{N}^0 \to \mathbb{N}$:
  Für alle $c \in \mathbb{N}$ gilt: $f_{p(0,0,c)} = f$.

- $f = 0 : \mathbb{N}^1 \to \mathbb{N}$:
  Für alle $c \in \mathbb{N}$ gilt: $f_{p(0,1,c)} = f$.
- $f = S : \mathbb{N} \to \mathbb{N}$:
  Für alle $b, c \in \mathbb{N}$ gilt: $f_{p(1,b,c)} = f$.
- $f = g \circ h,\ h : \mathbb{N}^k \to \mathbb{N}^l,\ g : \mathbb{N}^l \to \mathbb{N}^m$:
  Laut Induktionsvoraussetzung exisitieren Folgen $(i_n)_{n\in\mathbb{N}},\ (j_n)_{n\in\mathbb{N}}$, sodass $g = f_{i_n}, h = f_{j_n}, n \in \mathbb{N}$. Damit folgt $f = f_{p(4,j_n,i_m)}, n, m \in \mathbb{N}$.
- $f = \mathrm{PR(g,h)}$.
  Wieder finden wir Folgen, sodass $g = f_{i_n}, h = f_{j_n}, n \in \mathbb{N}$ und es gilt $f = f_{p(5,i_n,jm)}, n, m \in \mathbb{N}$

$\square$

**Aufgabe 5** (206)**.** Sei $F(n,k) := f_n(k)$, falls $f_n : \mathbb{N} \to \mathbb{N}$, und $F(n,k) = 0$, falls $f_n$ nicht einstellig ist. Skizzieren Sie ein Programm $P$, das $F$ berechnet (also bei Eingabe von $n$ und $k$ den Wert $F(n,k)$ ausgibt).

Verwenden Sie Ihr Programm $P$, um ein neues Programm $Q$ zu definieren, sodass die von $Q$ berechnete Funktion $f_Q$ total ist, aber mit keiner Funktion $f_n$ übereinstimmt. (Oder sogar: $\forall n \forall k > n : f_Q(k) > f_n(k)$ erfüllt.)

*Lösung.*

```
FindeKoeffizienten(n) :
for a = 0, ..., 5 do
  for b = 0, ..., n − 1 do
    for c = 0, ..., n − 1 do
      if p(a, b, c) = n then :
        return(a, b, c)
      end if
    end for
  end for
end for
return(0, 1, 0)
```

Wir führen eine Hilfsvariable $m$ ein, die die Stelligkeit der Funktion bezeichnet, da bei der Entstehung durch primitive Rekursion auch Funktionen von höherer Stelligkeit auftreten werden.

```
P(n, k):
m = dim(k)
(a, b, c) = FindeKoeffizienten(n)
if a = 0 then
  return 0
else if a = 1 ∧ m = 1 then
  return k[1] + 1
else if a = 2 then
  if m = b ≥ c ≥ 1 then
    return k[c]
  else
    return 0
  end if
else if a = 3 then
  return (P(b, k), P(c, k))
else if a = 4 then
  return P(c, F(b, k))
else if a = 5 then
  if k[−1] = 0 then
    return P(c, k[: −1])
  else
    return P(b, [k − 1, P(b, k − 1)])
  end if
else
  return 0
end if
```

```
Q(k):
x = 1
for i = 0, ..., k do
  x = x + P(i, k)
end for
return x
```

Damit gilt $\forall k \in \mathbb{N}\, \forall n \leq k : Q(k) > P(n, k) = f_n(k)$.
Insbesondere existiert zu jedem $n \in \mathbb{N}$ ein $k > n$ mit $Q(k) > f_n(k)$. Daher kann $Q$ kein Element von $\{f_n : n \in \mathbb{N}\}$ sein. $\square$

## Die Ackermannfunktion

Eine totale Funktion $a : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ heißt Ackermannfunktion, wenn sie für alle $x, y \in \mathbb{N}$ die folgenden Bedingungen erfüllt:

$A.1$ $a(0, y) = y + 1$
$A.2$ $a(x + 1, 0) = a(x, 1)$
$A.3$ $a(x + 1, y + 1) = a(x, a(x + 1, y))$.

**Aufgabe 6** (207)**.** Zeigen Sie, dass es

(a) höchstens eine

(b) mindestens eine

Ackermannfunktion gibt. (Sobald wir dies bewiesen haben, geben wir der nun eindeutig bestimmten Ackermannfunktion den Namen $A$.)
Ihr Beweis enthält vermutlich mehrere Hilfssätze, die Sie jeweils mit vollständiger Induktion beweisen. Geben Sie immer explizit an, von welcher Menge $M$ sie die Eigenschaften $0 \in M$ und $x \in M \to x + 1 \in M$ zeigen.

(c) Berechnen (oder beschreiben) Sie $A(4, 2020)$.

(d) Schreiben Sie ein Programm (bzw: Skizzieren Sie einen Algorithmus) ohne rekursive Funktionsaufrufe, welches bei Eingabe $x, y$ den Wert von $A(x, y)$ berechnet. (Sie dürfen davon ausgehen, dass Sie beliebig viel Speicherplatz zur Verfügung haben, etwa in Form von mehrdimensionalen Arrays.)

*Lösung.*

(a) Seien $a_1, a_2$ zwei beliebige Ackermannfunktionen.
Wir wenden vollständige Induktion zuerst auf die Menge

$$M = \{n \in \mathbb{N} : \forall y \in \mathbb{N} : a_1(n, y) = a_2(n, y)\}$$

Es gilt $0 \in M$, da

$$\forall y \in \mathbb{N} : a_1(0, y) = y + 1 = a_2(0, y).$$

Den Induktionsschritt $(n - 1 \to n)$ selbst zeigen mir mit einer weiteren Induktion:

$$M_n = \{y \in \mathbb{N} : a_1(n, y) = a_2(n, y)\}$$

Es gilt $0 \in M_n$, da mit der Induktionsvoraussetzung der äußeren Induktion gilt:

$$a_1(n, 0) = a_1(n - 1, 1) = a_2(n - 1, 1) = a_2(n, 0).$$

Gelte nun $y - 1 \in M_n$:

$$a_1(n, y) = a_1(n - 1, a_1(n, y - 1)) = a_1(n - 1, a_2(n, y - 1)) = a_2(n - 1, a_2(n, y - 1)) = a_2(n, y).$$

Damit gilt $y \in M_n$ und mit der inneren Induktion erhalten wir $M_n = \mathbb{N}$ was uns wiederum $n \in M$ liefert, was schließlich $M = \mathbb{N}$ beweist.

(b) Für die Existenz definieren wir die Bedinungen

$A_n.1$ $a(0, y) = y + 1$
$A_n.2$ $\forall k < n : a(k + 1, 0) = a(k, 1)$
$A_n.3$ $\forall k < n : a(k + 1, y + 1) = a(k, a(k + 1, y))$.

und zeigen mit Induktion

$$M = \{n \in \mathbb{N} : \exists a_n : \{0, \dots, n\} \times \mathbb{N} \to \mathbb{N} \text{ sodass } A_n.1, A_n.2, A_n.3 \text{ gilt}\} \stackrel{!}{=} \mathbb{N}.$$

Es gilt $0 \in M$, da

$$a_0(0, y) := y + 1$$

die Bedingungen $A_0.1, A_0.2, A_0.3$ erfüllt.
Für den Induktionsschritt $n \to n + 1$ definieren wir

$$a_{n+1}(x, y) := \begin{cases} a_n(x, y), & x < k \\ a_n(n, 1), & x = n + 1, y = 0 \\ a_n(n, a_{n+1}(n + 1, y - 1)), & x = n + 1, y \neq 0 \end{cases}$$

Bedingung $A_{n+1}.1$ wird aufgrund der Induktionsvoraussetzung an das $a_n$ erfüllt. Bedingugen $A_{n+1}.2, A_{n+1}.3$ werden aufgrund der Induktionsvoraussetzung jedenfalls von $k < n$ erfüllt und aufgrund der Definition von $a_{n+1}$ auch von $k = n$.
(Formal bräuchte man noch wie im ersten Schritt eine innere Induktion, die zeigt, dass durch die Vorschrift im dritten Fall wirklich eine Funktion wohldefiniert ist, aber man siehts denk ich.)
Schließlich erfüllt die Funktion $A = \bigcup_{n \in \mathbb{N}} a_n$ die originalen Bedingungen $A.1, A.2, A.3$.

(c) Wir induzieren $A(1, n) = n + 2$:

$$\begin{aligned} A(1, 0) &= A(0, 1) = 1 + 1 = 0 + 2 \\ A(1, n) &= A(0, A(1, n - 1)) = A(0, n + 1) = n + 1 + 1 = n + 2. \end{aligned}$$

Wir induzieren $A(2, n) = 2n + 3$:

$$\begin{aligned} A(2, 0) &= A(1, 1) = 1 + 2 = 0 + 3 \\ A(2, n) &= A(1, A(2, n - 1)) = A(1, 2(n - 1) + 3) = A(1, 2n + 1) = 2n + 1 + 2 = 2n + 3. \end{aligned}$$

Für $A(3, n)$ stellen wir eine Rekursiongleichung auf:

$$\begin{aligned} A(3, 0) &= A(2, 1) = 5 \\ A(3, n) &= A(2, A(3, n - 1)) = 2A(3, n - 1) + 3. \end{aligned}$$

Die Lösung davon ist gegeben durch

$$A(3, n) = 5 \prod_{j=1}^{n} 2 + \sum_{i=1}^{n} 3 \prod_{j=i+1}^{n} 2 = 5 \cdot 2^n + 3 \sum_{i=1}^{n} 2^{n-1} = 5 \cdot 2^n + 3(2^n - 1).$$

Schließlich erhalten wir für $A(4, n)$ die Rekursiongleichung

$$\begin{aligned} A(4, 0) &= A(3, 1) = 13 \\ A(4, n) &= A(3, A(4, n - 1)) = 5 \cdot 2^{A(4,n-1)} + 3(2^{A(4,n-1)} - 1). \end{aligned}$$

Ja, und viel Spaß das jetzt noch explizit auszurechnen. Wär da nicht die Summe in der Rekursionsgleichung könnte mans noch mit der Pfeilnotation darstellen.

$$\begin{aligned} a_0 &= b \\ a_n &= c \cdot d \uparrow a_{n-1} \end{aligned}$$

hat als Lösungsdarstellung für $n \geq 2$

$$a_n = c \cdot (d^c \uparrow\uparrow (n - 1)) \uparrow d^b.$$

mit $x \uparrow y := x^y$ und $x \uparrow\uparrow y := \underbrace{x^{x^{\cdots x}}}_{y-\text{mal}}$

(d)

```
A(x, y) :
Wir benötigen ein zweidimensionales erweiterbares Array A
und einen Vektor S der Länge x + 1 mit Anfangswert überall −1
A(0, 0) := 1
S(0) := 0
while S(x) < y
  A(0, S(0) + 1) := S(0) + 2
  S(0) := S(0) + 1
  for i = 1, ..., x do
    if S(i) = −1 do
      if S(i − 1) ≥ 1 do
        A(i, 0) := A(i − 1, 1)
        S(i) := 0
      else
        break
      end if
    else if S(i − 1) ≥ A(i, S(i)) do
      A(i, S(i) + 1) := A(i − 1, A(i, S(i)))
    else
      break
    end if
  end for
end while
return A(x, y)
```

Ein Beispiel, damit man sich das besser vorstellen kann: $A(3,0)$

1 : $A(0,0) = 1, S(0) = 0$
2 : $A(0,1) = 2, S(0) = 1$
3 : $i = 1, S(1) = -1, S(0) = 1 \geq 1 \implies A(1,0) = A(0,1) = 2, S(1) = 0$
4 : $i = 2, S(2) = -1, S(1) = 0 < 1 \implies$ **break**
5 : $A(0,2) = 3, S(0) = 2$
6 : $i = 1, S(1) = 0, S(0) = 2 \geq A(1, S(1)) = A(1,0) = 2 \implies A(1,1) = A(0, A(1,0)) = A(0,2) = 3, S(1) = 1$
7 : $i = 2, S(2) = -1, S(1) = 1 \geq 1 \implies A(2,0) = A(1,1) = 3, S(2) = 0$
8 : $i = 3, S(3) = -1, S(2) = 0 < 1 \implies$ **break**
9 : $A(0,3) = 4, S(0) = 3$
10 : $i = 1, S(1) = 1, S(0) = 3 \geq A(1, S(1)) = A(1,1) = 3 \implies A(1,2) = A(0, A(1,1)) = A(0,3) = 4, S(1) = 2$
11 : $i = 2, S(2) = 0, S(1) = 2 < A(2, S(2)) = A(2,0) = 3 \implies$ **break**
12 : $A(0,4) = 5, S(0) = 4$
13 : $i = 1, S(1) = 2, S(0) = 4 \geq A(1, S(1)) = A(1,2) = 4 \implies A(1,3) = A(0, A(1,2)) = A(0,4) = 5, S(1) = 3$
14 : $i = 2, S(2) = 0, S(1) = 3 \geq A(2, S(2)) = A(2,0) = 3 \implies A(2,1) = A(1, A(2,0)) = A(1,3) = 5, S(2) = 1$
15 : $i = 3, S(3) = -1, S(2) = 1 \geq 1 \implies A(3,0) = A(2,1) = 5, S(3) = 0$
16 : $i = 4, S(4) = -1, S(3) = 0 < 1 \implies$ **break**
17 : $S(x) = S(3) = 0 = y \implies$ **return** $A(3,0) = 5$

□

**Aufgabe 7** (208)**.** Zeigen Sie, dass $A$ in beiden Argumenten streng monoton ist; außerdem, dass $A(x, y+1) \leq A(x+1, y)$ für alle $x, y$ gilt.

*Lösung.*

- Wir zeigen zuerst induktiv Monotonie in $y$:

$$M = \{n \in \mathbb{N} : \forall y_1 > y_2 : a(n, y_1) > a(n, y_2) \wedge a(n,1) > 1\} \stackrel{!}{=} \mathbb{N}. \tag{1}$$

  Es gilt $0 \in M$, da für $y_1 > y_2$

$$\begin{aligned} A(0, y_1) &= y_1 + 1 > y_2 + 1 = A(0, y_2) \\ A(0,1) &= 2 > 1 \end{aligned}$$

  Im Induktionsschritt $(n-1) \to n$ führen wir eine weitere Induktion mit

$$M_n = \{m \in \mathbb{N} : a(n, m+1) > a(n, m)\} \stackrel{!}{=} \mathbb{N}. \tag{2}$$

  Es gilt $0 \in M_n$, da $n - 1 \in M \stackrel{(1)}{\implies} a(n-1, 1) > 1 \stackrel{(1)}{\implies} a(n-1, a(n-1,1)) > a(n-1, 1)$ und daher

$$a(n,1) = a(n-1, a(n,0)) = a(n-1, a(n-1,1)) \stackrel{(1)}{>} a(n-1,1) = a(n,0).$$

  Für den Induktionsschritt $(m-1) \in M_n \to m \in M_n$ rechnen wir

$$a(n, m+1) = a(n-1, a(n,m)) \stackrel{(2),(1)}{>} a(n-1, a(n, m-1)) = a(n,m).$$

  Damit gilt $M_n = \mathbb{N}$ und zusammen mit $a(n,1) > a(n,0) = a(n-1,1) \stackrel{(1)}{>} 1$ folgt daraus $n \in M$ und damit $M = \mathbb{N}$.

- Monotonie in $x$:
  Wir zeigen zuerst induktiv
$$M = \{n \in \mathbb{N} : \forall x > 0 : a(x,n) > n+1\} \stackrel{!}{=} \mathbb{N} \tag{3}$$
  mit Hilfe von
$$M_0 = \{m \in \mathbb{N} : m = 0 \vee a(m,0) > 1\}$$
  Es gilt klarerweise $0 \in M_0$ und
$$a(1,0) = a(0,1) = 2 > 1,$$
$$a(m-1,0) > 1 \implies a(m,0) = a(m-1,1) \stackrel{(1)}{>} a(m-1,0) > 1.$$
  Damit erhalten wir $M_0 = \mathbb{N}$ und $0 \in M$.
  Induktionsschritt $(n-1) \in M \to n \in M$:
$$M_n = \{m \in \mathbb{N} : m = 0 \vee a(m,n) > n+1\} \stackrel{!}{=} \mathbb{N} \tag{4}$$
  Es gilt $1 \in M_n$, da
$$a(1,n) = a(0, a(1,n-1)) \stackrel{(3),(1)}{>} a(0,n) = n+1.$$
  Induktionsschritt: $(m-1) \in M_n \to m \in M_n$:
$$a(m,n) = a(m-1, a(m,n-1)) \stackrel{(3),(1)}{>} a(m-1,n) \stackrel{(4)}{>} n+1.$$
  Also folgt $M_n = \mathbb{N}$, damit $n \in M$ und insgesamt $M = \mathbb{N}$.
  Jetzt können wir die Monotonie in $x$ zeigen:
$$M = \{n \in \mathbb{N} : \forall x_1 > x_2 : a(x_1,n) > a(x_2,n)\} \stackrel{!}{=} \mathbb{N} \tag{5}$$
  Es gilt $0 \in M$, da
$$a(x,0) = a(x-1,1) \stackrel{(1)}{>} a(x-1,0).$$
  Für den Induktionsschritt $(n-1) \to n$ rechnen wir:
$$a(x,n) = a(x-1, a(x,n-1)) \stackrel{(3),(1)}{>} a(x-1,n)$$
- $A(x+1,y) \geq A(x,y+1)$:
$$M = \{n \in \mathbb{N} : \forall x \in \mathbb{N} : A(x+1,n) \geq A(x,n+1)\} \tag{6}$$
  Es gilt $0 \in M$, da
$$\forall x \in \mathbb{N} : A(x+1,0) = A(x,1).$$
  Induktionsschritt: $(n-1) \to n$:
$$A(x+1,n) = A(x, A(x+1,n-1)) \stackrel{(6),(1)}{\geq} A(x, A(x,n)) \stackrel{(5)}{\geq} A(x-1, A(x,n)) = A(x,n+1).$$

$\square$

Für $c \in \mathbb{N}$ schreiben wir $A_c$ für die Funktion $A_c : \mathbb{N} \to \mathbb{N}, A_c(y) = A(c,y)$.
Für jede totale Funktion $f : \mathbb{N}^k \to \mathbb{N}$ schreiben wir $f < A_c$, wenn für alle $\vec{x} \in \mathbb{N}^k$ die Ungleichung $f(\vec{x}) < A_c(\max \vec{x})$ gilt.

## 209/210

**Aufgabe 8** (209)**.** Seien $f_1, \dots, f_k : \mathbb{N}^n \to \mathbb{N}$ und $h : \mathbb{N}^k \to \mathbb{N}$ mit $f_1, \dots, f_k, h < A_c$. Wenn[1] $g := h(f_1, \dots, f_k)$, dann gibt es ein $c'$ mit $g < A_{c'}$.

*Lösung.* Wir definieren $c' := c + 2$ und berechnen für beliebiges $x \in \mathbb{N}^n \setminus \{0\}$

$$\begin{aligned} g(x) = h(f_1(x), \dots, f_k(x)) &< A_c(\max\{f_i(x) \mid i \in \{1, \dots, k\}\}) < A_c(A_c(\max x)) \\ = A(c, A(c, \max x)) &< A(c, A(c+1, \max x)) = A(c+1, \max x + 1) \leq A(c+2, \max x) = A_{c'}(\max x). \end{aligned}$$

□

**Aufgabe 9** (210)**.** Wenn $f$ durch primitive Rekursion aus $h$ und $g$ entsteht, und $h > A_c,\ g < A_c$ gilt, dann gibt es ein $c'$ mit $f < A_{c'}$.

*Lösung.*

□

**Aufgabe 10** (211)**.** Schließen Sie aus den vorigen Aufgaben:

a. Für jede primitiv rekursive Funktion $f$ gibt es ein $c$ mit $f < A_c$.

b. Die Funktion $x \mapsto A(x, x)$ ist nicht primitiv rekursiv (aber berechenbar).

*Lösung.*

a. 1. Für die konstante Nullfunktion $0 : \mathbb{N}^k \to \mathbb{N} : \vec{x} \mapsto 0$ gilt für beliebiges $\vec{x} \in \mathbb{N}^k$ die Ungleichung

$$0(\vec{x}) = 0 < \max \vec{x} + 1 = A(0, \max \vec{x}) = A_0(\max \vec{x})$$

2. Für die Nachfolgerfunktion $S : \mathbb{N} \to \mathbb{N} : x \mapsto x + 1$ gilt für alle $x \in \mathbb{N}$ wegen der in Aufgabe 208 gezeigten strikten Monotonie von $A$ im ersten Argument

$$S(x) = x + 1 = A(0, x) < A(1, x) = A_1(x)$$

3. Für eine Projektion $\Pi^n_k : \mathbb{N}^n \to \mathbb{N} : \vec{x} \mapsto x_k$ gilt für beliebiges $\vec{x} \in \mathbb{N}^n$

$$\Pi^n_k(\vec{x}) = x_k < \max(\vec{x}) + 1 = A(0, \max(\vec{x})) = A_0(\max \vec{x})$$

4. Die Abgeschlossenheit bezüglich der Verknüpfung folgt direkt aus Aufgabe 209

5. Die Abgeschlossenheit bezüglich der primitiven Rekursion folgt direkt aus Aufgabe 210

b. Sei $c \in \mathbb{N}$ beliebig. Wir nennen unsere Abbildung $f : \mathbb{N} \to \mathbb{N} : x \mapsto A(x, x)$. Wegen der in Aufgabe 208 gezeigten strengen Monotonie gilt

$$A_c(c + 1) = A(c, c + 1) < A(c + 1, c + 1) = f(c + 1)$$

nach Punkt (a) kann daher $f$ nicht primitiv rekursiv sein.

□

[1] $g := h(f_1, \dots, f_k)$ ist Abkürzung für $\forall \vec{x} = (x_1, \dots, x_n) : g(\vec{x}) = h(f_1(\vec{x}), \dots, f_k(\vec{x}))$

# Logik und Grundlagen der Mathematik

*10. Übung am 10.12.2020*

Richard Weiss    Florian Schager    Fabian Zehetgruber

## Berechenbare Funktionen und (semi-)entscheidbare Mengen

Die Menge der $\mu$-rekursiven Funktionen ist die kleinste Menge von (möglicherweise partiellen) Funktionen, die alle primitiv rekursiven Funktionen enthält, unter Komposition und primitiver Rekursion abgeschlossen ist, und außerdem Folgendes erfüllt:

Wenn $f : \mathbb{N}^k \times \mathbb{N}$ total und $\mu$-rekursiv ist,
dann ist die partielle Funktion $\vec{x} \mapsto \min\{y : f(\vec{x}, y) = 0\}$ auch $\mu$-rekursiv.

**Aufgabe 1** (213)**.** Es gibt eine berechenbare partielle[1] Funktion $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, sodass die partielle Funktion $g(x) := \min\{y : f(x, y) = 0\}$ nicht berechenbar ist.
*Hinweis:* Verwenden Sie die vorige Aufgabe: Man kann eine Funktion $f$ mit $f(x, 1) = 0$ für alle $x$ finden.

*Lösung.* Sei $A \subseteq \mathbb{N}$ die semi-entscheidbare und nicht entscheidbare Menge aus Aufgabe 212.
Laut Definition ist dann

$$\widetilde{\chi}_A(x) = \begin{cases} 1, & x \in A \\ \text{undefiniert} & x \notin A \end{cases}$$

berechenbar und

$$\chi_A(x) = \begin{cases} 1, & x \in A \\ 0 & x \notin A \end{cases}$$

nicht berechenbar. Definiere also $B := (A \times \{0\}) \cup (\mathbb{N} \times \{1\})$ und

$$f : B \to \mathbb{N}, \quad (x, y) \mapsto \begin{cases} 0, & y = 1 \\ \widetilde{\chi}_A(x) - 1, & y = 0 \end{cases}$$

$$f = \chi_{\{0\}}(y)(\widetilde{\chi}_A(x) - 1) \implies f \text{ berechenbar.}$$

Dann ist

$$g(x) = \min\{y \in \mathbb{N} : f(x, y) = 0\} = \begin{cases} 0, & \widetilde{\chi}_A(x) = 1 \\ 1, & \text{sonst} \end{cases} = 1 - \chi_A(x)$$

nicht berechenbar und $f$ berechenbar. □

[1] „Es gibt eine partielle Funktion $f : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N} \dots$“ heißt: „Es gibt eine Menge $A \subseteq \mathbb{N} \times \mathbb{N}$ und eine Funktion $f : A \to \mathbb{N}$ (also mit Definitionsbereich $A$) ...“ So eine Funktion darf also durchaus auch auf ganz $\mathbb{N} \times \mathbb{N}$ definiert sein.

**Aufgabe 2** (215)**.**
Sei $f : \mathbb{N} \to \mathbb{N}$ eine berechenbare schwach monotone totale Funktion. ($x < y \Rightarrow f(x) \leq f(y)$.) Dann ist die Wertemenge von $f$ entscheidbar.

*Lösung.*

Fall 1: $\exists s \in \mathbb{N} : \forall x \in \mathbb{N} : f(x) < s$. In diesem Fall ist $f(\mathbb{N})$ eine endliche Menge und daher entscheidbar.

Fall 2: $\nexists s \in \mathbb{N} : \forall x \in \mathbb{N} : f(x) < s$. In diesem Fall betrachten wir die berechenbare Funktion

$$g(0, y) := \chi_{\{0\}}(f(y)), \quad g(x+1, y) := g(x) + \chi_{\{0\}}(f(y) - (x+1))\chi_{\{0\}}((x+1) - f(y)).$$

Es gilt $g(x, y) = \chi_{\{0,\dots,x\}}(f(y))$ und aufgrund der Voraussetzung dieses Falles gibt es für jedes $x \in \mathbb{N}$ ein $y_x \in \mathbb{N}$ mit $f(y_x) > x$. Deshalb und wegen der Monotonie gilt

$$\mu g(x) = \min\{y \in \mathbb{N} \mid g(x, y) = 0\} = \max\{z \in \mathbb{N} \mid f(z) \leq x\} + 1.$$

Nun können wir die streng monotone Funktion

$$h(0) := f(0), \quad h(x+1) := f(\mu g(h(x)))$$

definieren für welche $h(\mathbb{N}) = f(\mathbb{N})$ gilt. Die Inklusion „$\subseteq$" ist klar.
Für die umgekehrte Inklusion behaupten wir $h(x) = f_x$, wobei $(f_n)_{n\in\mathbb{N}}$ die aufsteigende, injektive Abzählung von Elementen aus $f(\mathbb{N})$ sei.
Klarerweise gilt $h(0) = f(0) = f_0$ und im Induktionsschritt

$$h(x+1) = f(\mu g(h(x))) = f(\mu g(f_x)) = f(\max\{z \in \mathbb{N} \mid f(z) \leq f_x\} + 1) = f_{x+1}.$$

Es reicht also die Aussage für die streng monotone Funktion $h$ zu zeigen.
Sei $h : \mathbb{N} \to \mathbb{N}$ berechenbar, total und strikt monoton. Dann gilt $h(x) \geq x$ und somit

$$h(x) = z \implies z \leq x.$$

Um zu zeigen, dass $h(\mathbb{N})$ entscheidbar ist, zeigen wir, dass $\chi_{h(\mathbb{N})} \subset \mathbb{N} \times \mathbb{N}$ eine $\Sigma_1$-Menge ist. Berechenbarkeit von $h$ ist äquivalent dazu, dass der Graph von $h$ eine $\Sigma_1$-Menge ist, also gibt es eine $\Sigma_0$-Formel $\varphi$, sodass

$$(x, y) \in h \iff \exists u\, \varphi(x, y, u).$$

Damit erhalten wir

$$\begin{aligned}
(x, y) \in \chi_{h(\mathbb{N})} &\iff [(y = 1 \wedge x \in h(\mathbb{N})) \vee (y = 0 \wedge x \notin f(\mathbb{N}))] \\
&\iff [(y = 1 \wedge \exists z_1 \in \mathbb{N} : x = h(z_1)) \vee (y = 0 \wedge \forall z_2 \in \mathbb{N} : x \neq h(z_2))] \\
&\iff [(y = 1 \wedge \exists z_1 \leq x : x = h(z_1)) \vee (y = 0 \wedge \forall z_2 \leq x : x \neq h(z_2))] \\
&\iff [(y = 1 \wedge \exists z_1 \leq x : \underbrace{x = h(z_1)}_{\Sigma_1-\text{Formel}}) \vee (y = 0 \wedge \forall z_2 \leq x : \underbrace{h(z_2) = y \wedge y \neq x}_{\Sigma_1-\text{Formel}})].
\end{aligned}$$

Also ist $\chi_{h(\mathbb{N})} \subset \mathbb{N} \times \mathbb{N}$ eine $\Sigma_1$-Menge, also $\chi_{h(\mathbb{N})}$ $\mu$-rekursiv, also $h(\mathbb{N})$ entscheidbar.

□

**Aufgabe 3** (216)**.** Für alle $(n_1, \dots, n_k) \in \mathbb{N}^k$ definieren wir $\langle n_1, \dots, n_k \rangle := p_1^{n_1+1} \cdot \dots \cdot p_k^{n_k+1}$, wobei $(p_1, p_2, p_3, \dots) = (2, 3, 5, 7, \dots)$ die Folge der Primzahlen ist. (Runde Klammern für Folgen, spitze Klammern für einzelne Zahlen, die Folgen codieren.)

Für jede Funktion $f : \mathbb{N}^k \times \mathbb{N} \to \mathbb{N}$ definieren wir $\hat{f} : \mathbb{N}^k \times \mathbb{N} \to \mathbb{N}$ so:

$$\hat{f}(\vec{x}, y) = \langle f(\vec{x}, 0), \dots, f(\vec{x}, y-1) \rangle,$$

also insbesondere $\hat{f}(\vec{x}, 0) = \langle\rangle = 1$, und $\hat{f}(\vec{x}, 1) = \langle f(\vec{x}, 0) \rangle = 2^{f(\vec{x},0)+1}$.

Zeigen Sie:

(a) $f$ ist primitiv rekursiv genau dann, wenn $\hat{f}$ primitiv rekursiv ist.

(b) Wenn $f$ total ist, dann ist $f$ genau dann berechenbar, wenn $\hat{f}$ berechenbar ist.

*Lösung.*

(a) "$\Rightarrow$" Es sei also vorausgesetzt, dass $f$ primitiv rekursiv ist. Dann gilt

$$\hat{f}(\vec{x}, 0) = 1, \quad \hat{f}(\vec{x}, y+1) = \hat{f}(\vec{x}, y) p_{y+1}^{f(\vec{x},y)+1}$$

also haben wir eine Darstellung gefunden an welcher wir ekrennen, dass $\hat{f}$ primitiv rekursiv ist.

"$\Leftarrow$" Nun sei umgekehrt vorausgesetzt, dass $\hat{f}$ primitiv rekursiv ist. Für diese Richtung wollen wir die Funktion

$$(\cdot). : \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (x, y) \mapsto \begin{cases} 0 & \text{, falls } x = 0 \vee y = 0 \\ \max\{k \in \mathbb{N} : p_y^k \mid x\} & \text{, sonst} \end{cases}$$

betrachten. $(x)_y$ ist also der Exponent der $y$-ten Primzahl in der Primfaktorzerlegung von $x$. Es gilt

$$f(\vec{x}, y) = \left(\hat{f}(\vec{x}, y+1)\right)_{y+1} - 1.$$

Zu zeigen bleibt, dass alle verwendeten Funktionen primitiv rekursiv ist. Dafür zeigen wir zunächst, dass die Menge aller Primzahlen primitiv rekursiv ist. Wir wissen bereits, dass

$$\div : (n, k) \mapsto (q, r) \quad \text{sodass } qk + r = n, 0 \leq r < k$$

primitiv rekursiv ist und somit auch

$$\text{div} : (n, k) \mapsto \chi_{\{0\}}(\Pi_2^2(\div(n, k))).$$

Es gilt also $\text{div}(n, k) = 1$ genau dann, wenn $k|n$ und 0 sonst. Damit ist auch

$$g : (n, z) \mapsto \sum_{k=1}^{z} \text{div}(n, k)$$

primitiv rekursiv, und wir erhalten mit $\tau(x) = g(x, x)$

$$\chi_{\mathbb{P}}(x) = \chi_{\{2\}}(\tau(x))$$

ist primitiv rekursiv, also sind die Primzahlen als Menge primitiv rekursiv.
Wir wissen aus Aufgabe 202 bereits, dass für ein beliebieges $P \subseteq \mathbb{N}^k \times \mathbb{N}$ das primitiv rekursiv ist die Funktion

$$h_P : \mathbb{N}^k \times \mathbb{N} \to \mathbb{N} : (\vec{x}, z) \mapsto \min\left(\{y < z : (\vec{x}, y) \in P\} \cup \{z\}\right)$$

ebenfalls primitiv rekursiv ist.
Jetzt haben wir alles gesammelt, um zu zeigen, dass die Funktion $p_k$, welche $k$ auf die $k$-te Primzahl abbildet, primitiv rekursiv ist. Die Relation

$$R(m, y) : \chi_{\mathbb{P}}(y) = 1 \wedge m < y$$

ist als Schnitt zweier primitiv rekursiver Relationen wieder primitiv rekursiv. Mit der oberen Schranke $p_{n+1} \leq 2^{2^n}$ (Induktion und die Tatsache $p_{n+1} \leq p_1 \cdots p_n + 1$) erhalten wir für

$$g(m, z) := h_R(m, z)$$

Die primitiv rekursive Funktion

$$p_0 := 1, \quad p_{n+1} := 2\chi_{\{0\}}(n) + (1 - \chi_{\{0\}}(n))g(p_n, 2^{2^n})$$

Nun betrachten wir eine weitere primitiv rekursive Relation, nämlich

$$S := \{(n, k, y) \in \mathbb{N}^3 \mid \operatorname{div}(n, p_k^y) = 0\}$$

Jetzt können wir $(n, k) \mapsto (n)_k$ primitv rekursiv beschreiben durch

$$(n)_k = h_S(n, k, n) - 1.$$

(b) Kann man hier den Beweis aus (a) nicht direkt übernehmen?

□

**Aufgabe 4** (217)**.** Sei $F : \mathbb{N} \to \mathbb{N}$ die Fibonacci-Folge: $F(0) = 0$, $F(1) = 1$, $F(n+2) = F(n+1) + F(n)$ für alle $n \geq 0$. Zeigen Sie, dass $F$ primitiv rekursiv ist, indem Sie zunächst eine primitive Rekursion für $\hat{F}$ angeben.

*Lösung.*

$$\hat{F}(0) = 1, \quad \hat{F}(x+1) = 2\chi_{\{0\}}(x) + 18\chi_{\{1\}}(x) + (1 - \chi_{\{0,1\}}(x))\hat{F}(x)p_{x+1}^{(\hat{F}(x))_x + (\hat{F}(x))_{x-1} - 1}$$

also ist $\hat{F}$ primitiv rekursiv, nach der vorherigen Aufgabe daher auch $F$. □

**Aufgabe 5** (220)**.** Wenn $f : \mathbb{N}^k \to \mathbb{N}$ eine totale Funktion ist, die (als Relation) eine $\Sigma_1$-Menge ist, dann ist $f$ auch $\Delta_1$ (d.h., die Menge $(\mathbb{N}^k \times \mathbb{N}) \setminus f$ ist auch $\Sigma_1$).

*Lösung.*

$$(x_1, \ldots, x_k, y) \in (\mathbb{N}^k \times \mathbb{N}) \setminus f \iff \exists x_1' \cdots \exists x_k' \, \exists y' \, (x_1', \ldots, x_k', y') \in f \wedge x_1 = x_1' \wedge \ldots x_k = x_k' \wedge y \neq y'.$$

□

## Spektren

Für jede geschlossene Formel $\varphi$ (das heißt: $\varphi$ hat keine freien Variable) definieren wir das *Spektrum* $Sp(\varphi)$ als die Menge aller natürlichen Zahlen $n$, sodass es ein endliches Modell von $\varphi$ mit genau $n$ Elementen gibt. (Wir sagen, dass $\mathcal{M}$ ein Modell von $\varphi$ ist, wenn für alle Belegungen $b$ die Gleichung $\hat{b}(\varphi) = 1$ gilt.)

Wir schreiben $\mathscr{S}$ für die Menge aller Spektren (für beliebige prädikatenlogische Sprachen). $\mathscr{S}$ ist eine Untermenge der Potenzmenge von $\mathbb{N} \setminus \{0\}$.

**Aufgabe 6** (71)**.** Zeigen Sie, dass jede endliche Teilmenge von $\{1, 2, \dots\}$ ein Spektrum ist. (Wie definieren Sie „endlich"?) Verwenden Sie vollständige Induktion? Wenn ja, geben Sie explizit die Behauptung $B(n)$ an, von der Sie $B(0)$ und $B(n) \Rightarrow B(n+1)$ zeigen.)

*Lösung.* Wir behaupten

$$M := \{n \in \mathbb{N} \mid \forall A \subseteq \mathbb{N} \setminus \{0\} : (|A| = n \Rightarrow A \in \mathscr{S})\} = \mathbb{N}$$

Für $n = 0$ gilt $A = \emptyset$ und es gilt $Sp(\exists x \exists y (x = y \wedge x \neq y)) = A$.
Nehmen wir nun an $n \in M$ und betrachten wir eine Menge $A \subseteq \mathbb{N} \setminus \{0\}$ mit $|A| = n + 1$. Nun wählen wir ein Element $k \in A$ und definieren $C := A \setminus \{k\}$, damit gilt $|C| = n$. Nach unserer Annahmen folgt, dass es eine geschlossene Formel $\varphi$ gibt mit $C = Sp(\varphi)$. Nun unterscheiden wir zwei Fälle:

Fall 1: $k = 1$, dann ist

$$A = Sp(\varphi \vee (\forall x \forall y : x = y))$$

Fall 2: $k > 1$, dann ist

$$A = Sp(\varphi \vee (\exists^k \wedge \neg \exists^{k+1})),$$

wobei $\exists^k = \exists x_1 \dots \exists x_k (x_1 \neq x_2 \wedge x_1 \neq x_2 \wedge \dots \wedge x_{k-1} \neq x_k)$

□

## 72//73//74

**Aufgabe 7** (72)**.** Zeigen Sie, dass $\mathscr{S}$ unter Durchschnitt abgeschlossen ist. (Anleitung: Sei $A = Sp(\varphi_1)$, $B = Sp(\varphi_2)$. Erklären Sie, warum Sie ohne Beschränkung der Allgemeinheit annehmen dürfen, dass die Sprachen zu $\varphi_1$ und $\varphi_2$ disjunkt sind...)

*Lösung.* Seien $\varphi_1$ und $\varphi_2$ Formeln in den Sprachen $\mathcal{L}_1, \mathcal{L}_2$ respektive. Da $\varphi_1$ und $\varphi_2$ nur endlich viele Funktionssymbole, Relationssymbole, Konstantensymbole und Variable verwenden können wir ohne Beschränkung der Allgemeinheit annehmen, dass die Sprachen zu den beiden Formeln disjunkt sind.
Insbesondere können wir somit $\varphi_1, \varphi_2$ als Formeln in der gemeinsamen Sprache $\mathcal{L}_1 \cup \mathcal{L}_2$ auffassen.
Sei nun $n \in A \cap B$. Wähle ein Modell $\mathfrak{M}_1 = (M_1, I_1)$ mit $|M_1| = n$ und $\mathfrak{M}_1 \vDash \varphi_1$ sowie ein Modell $\mathfrak{M}_2 = (M_2, I_2)$ mit $|M_2| = n$ und $\mathfrak{M}_2 \vDash \varphi_2$. Wir können ohne Beschränkung der Allgemeinheit sagen, dass $M_1 = M_2$ gilt, da es eine Bijektion zwischen den beiden Mengen gibt. Wegen der Disjunktheit der Sprachen können wir nun die Interpretationen „vereinigen":

$$\mathfrak{M} := (M_1, I_1 \cup I_2)$$

wobei es keine Probleme bei den Interpretationen gibt. Wir erhalten nun klarerweise $\mathfrak{M} \vDash \varphi_1 \wedge \varphi_2$.
Betrachten wir umgekehrt $n \in Sp(\varphi_1 \wedge \varphi_2)$ dann gibt es ein Modell $\mathfrak{M}$ mit $|M| = n$ und $\mathfrak{M} \vDash \varphi_1 \wedge \varphi_2$ und damit gilt klarerweise auch $\mathfrak{M} \vDash \varphi_1$ und $\mathfrak{M} \vDash \varphi_2$. □

**Aufgabe 8** (73)**.** Zeigen Sie, dass $\mathscr{S}$ unter Vereinigung abgeschlossen ist.

*Lösung.* Wir wählen zuerst ein $n \in Sp(\varphi_1) \cup Sp(\varphi_2)$. Es gelte ohne Beschränkung der Allgemeinheit $n \in Sp(\varphi_1)$. Nun wissen wir, es gibt ein Modell $\mathfrak{M}$ mit $|M| = n$ mit $\mathfrak{M} \vDash \varphi_1$. Dieses Modell adaptieren indem wir den in $\varphi_2$ vorkommenden Konstanten, Funktions- und Relationssymbolen, welche nicht schon eine Intepretation haben beliebig interpretieren. Das neue Modell nennen wir $\tilde{\mathfrak{M}}$. Klarerweise gilt

$$\tilde{\mathfrak{M}} \vDash \varphi_1 \vee \varphi_2$$

also $n \in Sp(\varphi_1 \vee \varphi_2)$.
Betrachten wir umgekehrt $n \in Sp(\varphi_1 \vee \varphi_2)$. Das bedeutet es gibt ein Modell $\mathfrak{M}$ von $\varphi_1 \vee \varphi_2$ mit $|M| = n$. Mit der Definition der Theorie $\Sigma := \{\exists^n, \neg\exists^{n+1}, \varphi_1 \vee \varphi_2\}$ gilt also $\mathfrak{M} \vDash \Sigma$, also ist $\Sigma$ erfüllbar, nach dem Gödelschen Vollständigkeitssatz also auch konsistent. Wir können diese Theorie vervollständigen zu einer konsistenten Theorie $\bar{\Sigma}$. Benützen wir nun die andere Richtung des Vollständigkeitssatzes so ist $\bar{\Sigma}$ erfüllbar, es gibt also ein Modell $\bar{\mathfrak{M}}$ mit $\bar{\mathfrak{M}} \vDash \Sigma$. Wegen der Vollständigkeit von $\bar{\Sigma}$. Außerdem gilt $\bar{\Sigma} \vdash \varphi_1 \vee \varphi_2$. Mit Aufgabe 113 folgt daraus bereits $\bar{\Sigma} \vdash \varphi_1$ oder $\bar{\Sigma} \vdash \varphi_2$ und mit dem Vollständigkeitssatz sagen wir ohne Beschränkung der Allgeimeinheit $\bar{\Sigma} \vDash \varphi_1$, also $\bar{\mathfrak{M}} \vDash \varphi_1$ und $|\bar{M}| = n$, also $n \in Sp(\varphi_1)$. □

**Aufgabe 9** (74). Zeigen Sie, dass $\mathscr{S}$ unter Komplement abgeschlossen ist.

*Lösung.* Hoffentlich stimmt das...

□

**Aufgabe 10** (75). Zeigen Sie von möglichst vielen der folgenden Mengen, dass Sie Spektren sind: Die Menge der Primzahlen, die Menge aller zusammengesetzen Zahlen (=Nichtprimzahlen $> 1$), die Menge aller Quadratzahlen, die Menge aller Zweierpotenzen, die Menge aller Potenzen von 5, die Menge aller Primzahlpotenzen, die Menge $\{1, 14, 141, 1414, 14142, \dots\} = \left\{\lfloor 10^n\sqrt{2}\rfloor : n = 0, 1, 2, \dots\right\}$.

*Lösung.*

1. Primzahlpotenzen $R$: Sei $\varphi$ eine Formel, für die $\mathrm{Mod}(\varphi)$ die Klasse aller Körper ist. Dann ist das Spektrum von $\varphi$ genau die Menge aller Primzahlpotenzen (Zerfällungskörper des Polynoms $x^{p^n} - x$).

2. Primzahlen $P$: Sei $\varphi$ eine Formel, für die $\mathrm{Mod}(\varphi)$ die Klasse aller Körper ist. Weiters verlangen wir, dass es einen Automorphismus $f$ gibt, der nicht die Identität ist. Damit erhalten wir als Modelle alle Nicht-Primkörper. Vergleich dazu Algebra Skriptum Proposition 6.3.3.2. Als Spektrum erhalten wir damit alle Primzahlpotenzen ohne die Primzahlen selbst, und mit Aufgaben 72,74 erhalten wir damit, dass die Primzahlen selbst ebenso ein Spektrum seien müssen.
$$\varphi = \text{Körperaxiome} \wedge f \text{ Automorphismus} \wedge \exists x f(x) \neq x.$$

3. zusammengesetzte Zahlen $Y$: Nach Aufgabe 71 ist $\{1\} \in \mathscr{S}$ und mit $M := \mathbb{N} \setminus \{0\}$ gilt nach Aufgabe 74 auch $A := M \setminus \{1\} \in \mathscr{S}$ und $B := M \setminus P \in \mathscr{S}$ und schließlich gilt nach Aufgabe 71 die Aussage $Y = A \cap B \in \mathscr{S}$.

4. Zweierpotenzen $Z$: Sei $\psi$ eine Formel, die genau die Booleschen Algebren beschreibt. Dann ist das Spektrum von $\psi$ die Menge aller Zweierpotenzen (Darstellungssatz von Stone).

5. Fünferpotenzen $F$: Sei $\psi$ eine Formel, die genau die Körper der Charakteristik 5 beschreibt.

6. Quadratzahlen $Q$: Wenn $M$ ein Modell dann gibt es eine Teilmenge $A \subseteq M$ und eine Bijektion $f : A \times A \to M$. Wir realisieren das so, dass wir zuerst eine Totalordnung auf unserer Menge verlangen, also
$$\forall x(x \leq x), \quad \forall x \forall y((x \leq y \wedge y \leq x) \to x = y),$$
$$\forall x \forall y \forall z((x \leq y \wedge y \leq z) \to x \leq z), \quad \forall x \forall y(x \leq y \vee y \leq x)$$
und dann wollen wir eine Relation auf einem Quadrat, also
$$\exists a \exists b \forall x \forall y(\exists z R(x, y, z) \leftrightarrow a \leq x \leq b \wedge a \leq y \leq b_{\text{¸}})$$
Nun haben wir einmal den richtigen Definitionsbereich, wir brauchen noch, dass es sich tatsächlich um eine Funktion und eine Bijektion handelt, also
$$\forall x \forall y((\exists u R(x, y, u) \wedge \exists v R(x, y, v)) \to u = v)$$
$$\forall z((\exists x \exists y R(x, y, z) \wedge \exists u \exists v R(u, v, z)) \to u = x \wedge y = v)$$
$$\forall z \exists x \exists y R(x, y, z)$$

□

# Logik und Grundlagen der Mathematik

*11. Übung am 17.12.2020*

Richard Weiss Florian Schager Fabian Zehetgruber

## Berechenbare Funktionen und (semi-)entscheidbare Mengen

Die Menge der $\mu$-rekursiven Funktionen ist die kleinste Menge von (möglicherweise partiellen) Funktionen, die alle primitiv rekursiven Funktionen enthält, unter Komposition und primitiver Rekursion abgeschlossen ist, und außerdem Folgendes erfüllt:

Wenn $f : \mathbb{N}^k \times \mathbb{N}$ total und $\mu$-rekursiv ist,
dann ist die partielle Funktion $\vec{x} \mapsto \min\{y : f(\vec{x}, y) = 0\}$ auch $\mu$-rekursiv.

**Aufgabe 1** (224)**.** Für $i = 0, 1$ sei $P_i$ die Menge aller Programme $p$, die bei Eingabe $p$ halten und $i$ ausgeben. Es gilt offenbar $P_0 \cap P_1 = \emptyset$. Zeigen Sie, dass die Mengen $P_0$ und $P_1$ semi-entscheidbar sind. (indem Sie Programme skizzieren, die die jeweileigen partiellen charakteristischen $\tilde{\chi}_{P_i}$ berechnen), es aber keine entscheidbare Menge $E$ mit $P_0 \subseteq E$, $P_1 \subseteq \mathbb{N} \setminus E$ gibt.

*Lösung.*

**Algorithm 1** charakteristische Funktion von $P_i$ für $i \in \{0, 1\}$

**procedure** $\tilde{\chi}_{P_i}(p)$
    **if** $p(p) = i$ **then**
        **return** 1
    **end if**
**end procedure**

Für den zweiten Teil identifizieren wir die Menge aller Programme mit einer beliebigen Abzählung und nehmen an, es gibt eine entscheidbare Menge $E$ mit $P_0 \subseteq E$ und $P_1 \subseteq \mathbb{N} \setminus E$.
Dann können wir ein Programm $q$ schreiben.

**Algorithm 2** Programm $q$

**procedure** $q(p)$
    **if** $\chi_E(p) = 1$ **then**
        **return** 1
    **else**
        **return** 0
    **end if**
**end procedure**

Nun betrachten wir $q(q)$.

Fall 1: $q(q) = 1$. Dann folgt $q \in E$ also $q \notin P_1$ und daher $q(q) \neq 1$. Ein Widerspruch!

Fall 2: $q(q) = 0$. Dann folgt $q \notin E$ also $q \notin P_0$ und damit $q(q) \neq 0$. Ein Widerspruch!

$\square$

**Aufgabe 2** (225)**.** Eine Menge $A \subseteq \mathbb{N}$ heißt $\Pi_1$-Menge, wenn $\mathbb{N} \setminus A$ eine $\Sigma_1$-Menge ist.
Eine Menge $B \subseteq \mathbb{N}$ heißt $\Delta_1$-Menge, wenn $B$ sowohl $\Sigma_1$- als auch $\Pi_1$-Menge ist.

a. Seien $S_0, S_1 \subseteq \mathbb{N}$ $\Sigma_1$-Mengen mit $S_0 \cup S_1 = \mathbb{N}$. Dann gibt es eine $\Delta_1$-Menge $E$, sodass $S_0 \setminus S_1 \subseteq E \subseteq S_0$ gilt.
   *Hinweis:* Für $n \in S_0 \cap S_1$ vergleiche die jeweils kleinsten Zeugen für $n \in S_0$ und $n \in S_1$.

b. Seien $Q_0, Q_1 \in \mathbb{N}$ $\Pi_1$-Mengen mit $Q_0 \cap Q_1 = \emptyset$. Dann gibt es eine $\Delta_1$-Menge $E$, die $Q_0$ und $Q_1$ trennt, also $Q_0 \subseteq E, Q_1 \subseteq \mathbb{N} \setminus E$.

*Lösung.*

a. Da $S_0, S_1$ $\Sigma_1$-Mengen sind, gibt es $\Sigma_0$-Formeln $\psi_0, \psi_1$, sodass

$$\begin{aligned} x \in S_0 &\iff \exists y\, \psi_0(x, y) \\ x \in S_1 &\iff \exists y\, \psi_1(x, y) \end{aligned}$$

Wir kreieren nun eine neue $\Sigma_1$-Formel $\varphi$:

$$\exists y_0\, (\psi_0(x, y_0) \land \forall y_1 < y_0\, \neg\psi_1(x, y_1))$$

und definieren $E := \{x \in \mathbb{N} : \mathbb{N} \vDash \varphi(x)\}$. Es gilt

$$\begin{aligned} x \in S_0 \setminus S_1 &\iff \exists y_0\, \psi_0(x, y_0) \land \neg\exists y_1\, \psi_1(x, y_1) \iff \exists y_0\, \psi_0(x, y_0) \land \forall y_1\, \neg\psi_1(x, y_1) \\ &\implies (\exists y_0\, \psi_0(x, y_0) \land \forall y_1 < y_0\, \neg\psi_1(x, y_1)) \iff x \in E \\ &\iff \exists y_0\, (\psi_0(x, y_0) \land \forall y_1 < y_0\, \neg\psi_1(x, y_1)) \implies \exists y_0\, \psi_0(x, y_0) \iff x \in S_0. \end{aligned}$$

Es bleibt also noch zu zeigen, dass $\mathbb{N} \setminus E$ ebenso eine $\Sigma_1$-Menge ist: Aus $S_0 \cup S_1 = \mathbb{N}$ folgt

$$\mathbb{N} \vDash \exists y_0\, (\psi_0(x, y_0) \land \forall y_1 < y_0\, \neg\psi_1(x, y_1)) \lor \exists y_1\, (\psi_1(x, y_1) \land \forall y_0 \leq y_1\, \neg\psi_0(x, y_0))$$

und damit

$$x \in \mathbb{N} \setminus E \iff \exists y_1\, (\psi_1(x, y_1) \land \forall y_0 \leq y_1\, \neg\psi_0(x, y_0)).$$

b. Wir führen diesen Teil auf den Teil (a) zurück und betrachten

$$S_0 := \mathbb{N} \setminus Q_0, \quad S_1 := \mathbb{N} \setminus Q_1.$$

Es gilt

$$S_0 \cup S_1 = (\mathbb{N} \setminus Q_0) \cup (\mathbb{N} \setminus Q_1) = \mathbb{N} \setminus (Q_0 \cap Q_1) = \mathbb{N}$$

und $S_0$ und $S_1$ sind $\Sigma_1$-Mengen. Nach Punkt (a) gibt es nun eine $\Delta_1$-Menge $\tilde{E}$ mit

$$Q_1 = (\mathbb{N} \setminus Q_0) \setminus (\mathbb{N} \setminus Q_1) = S_0 \setminus S_1 \subseteq \tilde{E} \subseteq S_0 = \mathbb{N} \setminus Q_0.$$

Wir definieren eine neue Menge $E := \mathbb{N} \setminus \tilde{E}$. Für diese gilt nun

$$Q_0 = \mathbb{N} \setminus (\mathbb{N} \setminus Q_0) \subseteq \mathbb{N} \setminus \tilde{E} = E$$

und

$$Q_1 \subseteq \tilde{E} = \mathbb{N} \setminus (\mathbb{N} \setminus \tilde{E}) = \mathbb{N} \setminus E$$

$\square$

# Berechenbare Funktionen auf Strings

Im Folgenden sei $S$ die Menge aller Strings über einem festen Alphabet $A$. Für $x \in S$ sei $|x|$ die Länge von $x$.
Um zu zeigen, dass eine Menge $A$ von Strings entscheidbar oder semi-entscheidbar ist, geben Sie (informell) einen Algorithmus an, der $\chi_A$ bzw. $\tilde{\chi}_A$ berechnet.

## 230/231

Für jede Menge $\Sigma$ von geschlossenen Formeln sei $cl(\Sigma)$ die Menge aller aus $\Sigma$ ableitbaren geschlossenen Formeln.

**Aufgabe 3** (230)**.** Wenn $\Sigma$ semi-entscheidbar ist, dann auch $cl(\Sigma)$.

*Lösung.* Unter Verwendung von Aufgabe 229: Sei $P$ ein Programm, welches die charakteristische Funktion die Menge der logischen Axiome berechnet, und $Q$ ein Programm, das $\tilde{\chi}_\Sigma$ berechnet.

**Algorithm 3** Programm, welches $\tilde{\chi}_{cl(\Sigma)}$ berechnet

**procedure** $\tilde{\chi}_{cl(\Sigma)}$ $(\sigma)$
  **if** $P(\sigma) = 1$ **then**
    **return** 1
  **end if**
**end procedure**

$\square$

**Aufgabe 4** (231)**.** Sei $\Sigma$ semi-entscheidbar. Dann gibt es eine entscheidbare Menge $\Sigma'$ mit $cl(\Sigma') = cl(\Sigma)$.
*Hinweis:* $\varphi \wedge \varphi$

# Unentscheidbare Mengen; universelle Mengen

**Aufgabe 5** (236)**.**

(a) Sei $A \subseteq \mathbb{N}^2$ eine $\Sigma_1$-Menge. Dann sind die Mengen $B := \{y \in \mathbb{N} : (5, y) \in A\}$ und $C := \{x \in \mathbb{N} : (x, x) \in A\}$ auch $\Sigma_1$-Mengen.

(b) Es gibt eine $\Sigma_1$-Menge $U \subseteq \mathbb{N}$, die keine $\Pi_1$-Menge ist. (Das heißt: $\mathbb{N} \setminus U$ ist keine $\Sigma_1$-Menge.) Hinweis: Verwenden Sie (a) sowie die beiden vorigen Aufgaben.

*Lösung.*

(a) Wir können $B$ und $C$ als Projektionen von Schnitten von $\Sigma_1$-Mengen darstellen:

$$B' := \{(x, y) \in \mathbb{N}^2 : x = 5\}$$
$$B = \{y \in \mathbb{N} : (x, y) \in A \cap B'\}$$
$$C' := \{(x, y) \in \mathbb{N}^2 : x = y\}$$
$$C = \{x \in \mathbb{N} : (x, y) \in A \cap C'\}$$

(b) Aus der vorigen Aufgabe holen wir uns eine $\Sigma_1$-Menge $A \subseteq \mathbb{N} \times \mathbb{N}$ mit der Eigenschaft, dass es für jede $\Sigma_1$-Menge $B \subseteq \mathbb{N}$ ein $k \in \mathbb{N}$ mit $B = \{y \in \mathbb{N} \mid (k, y) \in A\}$ gibt. Wegen der vorvorigen Aufgabe können wir weiters eine Bijektion $p_2 : \mathbb{N}^2 \to \mathbb{N}$ finden, sodass für alle $C \subseteq \mathbb{N}^2$ gilt, dass $C$ genau dann eine $\Sigma_1$-Menge ist, wenn $p_2[C]$ eine $\Sigma_1$-Menge ist.

Wir definieren $U := p_2[A]$, damit ist $U$ eine $\Sigma_1$-Menge. Nun nehmen wir an $\mathbb{N} \setminus U$ ist ebenfalls eine $\Sigma_1$-Menge. Damit ist auch

$$p_2^{-1}[\mathbb{N} \setminus U] = p_2^{-1}[\mathbb{N}] \setminus p_2^{-1}[U] = \mathbb{N}^2 \setminus A$$

eine $\Sigma_1$-Menge. Mit Punkt (a) folgt, dass auch $B := \{x \in \mathbb{N} \mid (x, x) \in \mathbb{N}^2 \setminus A\}$ eine $\Sigma_1$-Menge ist. Wir unterscheiden für beliebiges $k \in \mathbb{N}$ nun zwei Fälle.

Fall 1: $k \in B$. Dann ist $(k, k) \in \mathbb{N}^2 \setminus A$ und daher $k \notin \{x \in \mathbb{N} \mid (k, x) \in A\}$. Und damit $B \neq \{x \in \mathbb{N} \mid (k, x) \in A\}$.

Fall 2: $k \notin B$. Dann ist $(k, k) \notin \mathbb{N}^2 \setminus A$ und daher $(k, k) \in A$. Damit ist $k \in \{x \in \mathbb{N} \mid (k, x) \in A\}$ und damit $B \neq \{x \in \mathbb{N} \mid (k, x) \in A\}$

In jedem Fall gilt also

$$B \neq \{x \in \mathbb{N} \mid (k, x) \in A\}$$

und da das für alle $k \in \mathbb{N}$ gilt ist das ein Widerspruch zur Eigenschaft von $A$.

□

# Wohlordnungen

Eine strikte lineare Ordnung $(A, <)$ (mit der zugehörigen reflexiven Ordnung $\leq$) heißt Wohlordnung, wenn jede nichtleere Teilmenge von $A$ ein kleinstes Element hat: $\forall B \subseteq A : (B \neq \emptyset \Rightarrow \exists b \in B \, \forall x \in B : b \leq x)$

**Aufgabe 6** (237)**.** Wenn $(A, <)$ eine Wohlordnung ist, in der jede nichtleere Teilmenge ein größtes Element hat, dann ist $A$ endlich.

*Lösung.* Nehmen wir an $A$ ist nicht endlich. Wir definieren $A_0 := A$ und für jedes $n \in \mathbb{N}$ die Menge $A_{n+1} := A_n \setminus \{\min A_n\}$. Wir nehmen an, dass $A$ eine unendliche Menge ist und definieren die Funktion

$$f : \mathbb{N} \to A : n \mapsto \min A_n$$

Nun bezeichnen wir mit $c \in A$ das größte Element von $f[\mathbb{N}] \subseteq A$. Sei $k \in \mathbb{N}$ ein Element mit $f(k) = c$. Es gilt

$$c = f(k) = \min A_k < \min A_{k+1} = f(k+1).$$

Ein Widerspruch dazu, dass $c$ das größte Element in $f[\mathbb{N}]$ ist.

□

**Aufgabe 7** (239)**.** Seien $(A, <)$ und $(B, <)$ Wohlordnungen. Finden Sie eine Wohlordnung auf $A \times B$. (Hinweis: lexikographische Ordnung: $(x, y) < (x', y') \Leftrightarrow (x < x' \vee (x = x' \wedge y < y'))$.)

*Lösung.* Wir rechnen nach.

1. Irreflexivität: $\forall z \in A \times B : z \not< z$. Sei also $(x, y) \in A \times B$ beliebig. Es gilt $x = x$ und $y = y$ also folgt $(x, y) \not< (x, y)$.

2. Transitivität: $\forall u, v, w \in A \times B : ((u < v \wedge v < w) \Rightarrow u < w)$. Seien also $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in A \times B$ mit $(x_1, y_1) < (x_2, y_2)$ und $(x_2, y_2) < (x_3, y_3)$.

Fall 1: $x_1 < x_2 \vee x_2 < x_3$. Dann gilt auch $x_1 < x_3$ und daher $(x_1, y_1) < (x_3, y_3)$.

Fall 2: $x_1 = x_2 \wedge x_2 = x_3$. Dann folgt $x_1 = x_3$ und $y_1 < y_2 < y_3$. und damit $(x_1, y_1) < (x_3, y_3)$.

3. Trichotomie: $\forall u, v \in A \times B : (u < v \vee u = v \vee u > v)$. Seien $(x_1, y_1), (x_2, y_2) \in A \times B$ mit $(x_1, y_1) \neq (x_2, y_2)$ und $(x_1, y_1) \not> (x_2, y_2)$. Wir unterscheiden zwei Fälle.

Fall 1: $x_1 = x_2$. Dann folgt bereits $y_1 < y_2$ und daher $(x_1, y_1) < (x_2, y_2)$.
Fall 2: $x_1 < x_2$. Dann folgt unmittelbar $(x_1, y_1) < (x_2, y_2)$.

4. Wohlordnung: $\forall C \subseteq A \times B : (C \neq \emptyset \Rightarrow \exists c \in C \,\forall x \in C : x = c \vee c < x)$. Sei also $C \subseteq A \times B$ mit $C \neq \emptyset$. Wir betrachten zuerst die Menge

$$C_1 := \{a \in A \mid \exists b \in B : (a, b) \in C\}$$

Da $C_1 \neq \emptyset$ gibt es ein $u \in C_1$, sodass für alle $x \in C_1 : u = x \vee u < x$. Als nächstes betrachten wir noch die Menge

$$C_2 := \{b \in B \mid (u, b) \in C\}$$

Auch $C_2 \neq \emptyset$ und daher finden wir ein $v \in C_2$, sodass für alle $y \in C_2 : v = y \vee v < y$.

Nun betrachten wir $(x, y) \in C$ beliebig. Es gilt $x \in C_1$ und daher können wir zwei Fälle unterscheiden.

Fall 1: $x = u$. Dann folgt $y \in C_2$ und es gibt zwei Fälle.
Fall 1.1 $y = v$. Dann ist also $(x, y) = (u, v)$.
Fall 1.2 $v < y$. Dann ist $(u, v) < (x, y)$.
Fall 2: $u < x$. Dann folgt sofort $(u, v) < (x, y)$.

Wir sehen, dass wir mit $(u, v)$ das kleinste Element von $C$ gefunden haben, also ist $(A \times B, <)$ eine Wohlordnung.

□

**Aufgabe 8** (240)**.** Definieren Sie die lexikographische Ordnung auf $\{0,1\}^{\mathbb{N}}$. Gibt es ein kleinstes Element? Zeigen Sie, dass diese Ordnung eine lineare Ordnung aber keine Wohlordnung ist.

*Lösung.* Wir definieren die lexikographische Ordnung

$$(x_n)_{n\in\mathbb{N}} <_{\text{lex}} (y_n)_{n\in\mathbb{N}} :\Longleftrightarrow \exists n_0 \in \mathbb{N} : x_{n_0} < y_{n_0} \wedge \forall n < n_0 : x_n = y_n$$

und rechnen nachk, dass es sich um eine lineare Ordnung, aber keine Wohlordnung handelt.

1. Irreflexivität: $\forall z \in \{0,1\}^{\mathbb{N}} : z \not<_{\text{lex}} z$. Für $(x_n)_{n\in\mathbb{N}} \in \{0,1\}^{\mathbb{N}}$ gilt klarerweise für alle $k \in \mathbb{N}$, dass $x_k = x_k$ und daher ist $(x_n)_{n\in\mathbb{N}} \not<_{\text{lex}} (x_n)_{n\in\mathbb{N}}$.

2. Transitivität: $\forall u, v, w \in \{0,1\}^{\mathbb{N}} : ((u < v \wedge v < w) \Rightarrow u < w)$. Seien $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}}, (z_n)_{n\in\mathbb{N}} \in \{0,1\}^{\mathbb{N}}$ mit $(x_n)_{n\in\mathbb{N}} <_{\text{lex}} (y_n)_{n\in\mathbb{N}}$ und dem Zeugen $k \in \mathbb{N}$ sowie $(y_n)_{n\in\mathbb{N}} <_{\text{lex}} (z_n)_{n\in\mathbb{N}}$ mit dem Zeugen $l$. Wir definieren $m := \min\{k, l\}$. Es gilt

$$\forall i < m : x_i = y_i = z_i \quad \text{und} \quad x_m < z_m$$

und damit $(x_n)_{n\in\mathbb{N}} <_{\text{lex}} (z_n)_{n\in\mathbb{N}}$.

3. Trichotomie: $\forall u, v \in \{0,1\}^{\mathbb{N}} : (u < v \vee u = v \vee u > v)$. Seien also $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}} \in \{0,1\}^{\mathbb{N}}$ mit $(x_n)_{n\in\mathbb{N}} \not<_{\text{lex}} (y_n)_{n\in\mathbb{N}}$ und $(x_n)_{n\in\mathbb{N}} \neq (y_n)_{n\in\mathbb{N}}$. Weil die beiden Folgen nicht gleich sind können wir

$$k := \min\{i \in \mathbb{N} \mid x_i \neq y_i\}$$

definieren. Es gilt also

$$\forall i < k : x_i = y_i \quad \text{und} \quad x_k \neq y_k$$

und wegen $x_k \not< y_k$ gilt $x_k > y_k$ und daher $(x_n)_{n\in\mathbb{N}} >_{\text{lex}} (y_n)_{n\in\mathbb{N}}$.

4. keine Wohlordnung: $\exists C \subseteq \{0,1\}^{\mathbb{N}} : (C \neq \emptyset \wedge \forall z \in C \exists x \in C : x <_{\text{lex}} z)$. Das kleinste Element der Menge $\{0,1\}^{\mathbb{N}}$ ist $x^* := (0,0,\dots)$. Das heißt wir müssen uns eine andere Menge suchen. Die Teilmenge $C := \{0,1\}^{\mathbb{N}} \setminus \{x^*\}$ hat kein kleinstes Element. Angenommen sie hätte ein kleinstes Element $x'$, dann folgt aus $x' \neq x^*$

$$\exists n_0 \in \mathbb{N} : x'_{n_0} = 1$$

und wir finden mit $(x''_n)_{n\in\mathbb{N}} = (\delta_{n_0+1,n})_{n\in\mathbb{N}}$ ein echt kleineres Element. Ein Widerspruch.

□

# Bijektionen

Beachten Sie, dass wir $f(x)$ für den Funktionswert von $f$ an der Stelle $x$ schreiben. Für $U \subseteq \text{dom}(f)$ nennen wir die Menge $\{f(u) : u \in U\}$ nicht $f(U)$ sondern $f[U]$.

**Aufgabe 9** (243)**.** Seien $f : A \to B$ und $g : B \to A$ injektiv. Der Einfachheit halber seien $A$ und $B$ disjunkt. Zeigen Sie, dass es eine Bijektion $h : A \to B$ gibt, indem Sie den folgenden Beweis vervollständigen:
Wir definieren $A_0 := A, B_0 := B, A_{n+1} := g[B_n], B_{n+1} := f[A_n]$.
Sei $X_1 := \bigcup_{k\in\mathbb{N}} A_{2k} \setminus A_{2k+1}, X_2 := \bigcup_{k\in\mathbb{N}} A_{2k+1} \setminus A_{2k+2}, X_3 := \bigcap_{k\in\mathbb{N}} A_k$
und $Y_1 := \bigcup_{k\in\mathbb{N}} B_{2k} \setminus B_{2k+1}, Y_2 := \bigcup_{k\in\mathbb{N}} B_{2k+1} \setminus B_{2k+2}, Y_3 := \bigcap_{k\in\mathbb{N}} B_k$.

a. Zeigen Sie, dass $\{X_1, X_2, X_3\}$ eine Partition von $A$ ist.

b. Definieren Sie $h : A \to B$ mit einer Fallunterscheidung: Für $x \in X_1$ verwenden Sie $f$, um $h(x)$ zu definieren, für $x \in X_2$ hingegen $g$. Und für $x \in X_3$?

c. Zeigen Sie, dass die so definierte Funktion wohldefiniert ist, und überdies eine Bijektion.

*Lösung.*

a. Wir zeigen zuerst mit Induktion $\forall k \in \mathbb{N} : A_{k+2} \subseteq A_k$.

$$\begin{aligned} k = 0 : &\quad A_2 = g[B_1] = g[f[A_0]] = g[f[A]] \subseteq g[B] \subseteq A = A_0 \\ (k-1) \rightsquigarrow k : &\quad A_{k+2} = g[f[A_k]] \subseteq g[f[A_{k-2}]] = A_k. \end{aligned}$$

Als nächstes zeigen wir, dass $X_1, X_2, X_3$ paarweise disjunkt sind: Sei $x \in X_1 \cap X_2$:
Dann existieren $k_1, k_2$, sodass $x \in A_{2k_1} \setminus A_{2k_1+1}$, sowie $x \in A_{2k_2+1} \setminus A_{2k_2+2}$.
Fall 1: $k_1 \leq k_2$: Dann ist $x \in A_{2k_2+1} \subseteq A_{2k_1+1}$. Widerspruch!
Fall 2: $k_1 > k_2$: Dann ist $x \in A_{2k_1} \subseteq A_{2k_2+2}$. Widerspruch!
Die Disjunktheit von $X_3$ mit $X_1$ und $X_2$ ist offensichtlich.
Ganz analog sieht man auch, dass $\{Y_1, Y_2, Y_3\}$ eine Partition von $B$ sein muss.

Schließlich zeigen wir noch $X_1 \cup X_2 \cup X_3 = A$.
Dazu sei $x \in A \setminus X_3$ und $k_0 \geq 1$ das kleinste $k \in \mathbb{N}$ sodass $x \notin A_k$. Dann gilt $x \in A_{k-1} \setminus A_k \subset X_1 \cup X_2$.
Die andere Inklusion folgt aus $A_k \subseteq A, k \in \mathbb{N}$.

b. Für Fall $x \in X_3$ können wir uns aussuchen, ob wir $f$ oder $g^{-1}$ zur Definition hernehmen, wir entscheiden uns mal für $f$.

$$h(x) = \begin{cases} f(x) & x \in X_1 \\ g^{-1}(x) & x \in X_2 \\ f(x) & x \in X_3 \end{cases}$$

c. Die Wohldefiniertheit ist nur für $x \in X_2$ auf den ersten Blick fraglich, da aber $X_2 \subset A_1 = g[B]$ gilt, folgt sie sofort aus der Injektivität von $g$.
Weiters gilt aufgrund der Injektivität von $f$

$$
\begin{aligned}
f(X_1) &= f\left[\bigcup_{k\in\mathbb{N}} A_{2k} \setminus A_{2k+1}\right] = \bigcup_{k\in\mathbb{N}} f\left[A_{2k} \setminus A_{2k+1}\right] = \bigcup_{k\in\mathbb{N}} f\left[A_{2k}\right] \setminus f[A_{2k+1}] = \bigcup_{k\in\mathbb{N}} B_{2k+1} \setminus B_{2k+2} = Y_2,\\
g(Y_1) &= g\left[\bigcup_{k\in\mathbb{N}} B_{2k} \setminus B_{2k+1}\right] = \bigcup_{k\in\mathbb{N}} g\left[B_{2k} \setminus B_{2k+1}\right] = \bigcup_{k\in\mathbb{N}} g\left[B_{2k}\right] \setminus g[B_{2k+1}] = \bigcup_{k\in\mathbb{N}} A_{2k+1} \setminus A_{2k+2} = X_2,\\
f(X_3) &= f\left[\bigcap_{k\in\mathbb{N}} A_k\right] = \bigcap_{k\in\mathbb{N}} f\left[A_k\right] = \bigcap_{k\in\mathbb{N}} B_{k+1} = Y_3,\\
g(Y_3) &= g\left[\bigcap_{k\in\mathbb{N}} B_k\right] = \bigcap_{k\in\mathbb{N}} g\left[A_k\right] = \bigcap_{k\in\mathbb{N}} A_{k+1} = X_3.
\end{aligned}
$$

Also sehen wir, dass $f : X_1 \to Y_2$ und $g : X_2 \to Y_1$ Bijektionen sind, sowie $f : X_3 \to Y_3$ und $g : Y_3 \to X_3$, also können wir $h$ für $x \in X_3$ tatsächlich auf beide Arten definieren und erhalten in jedem Fall eine Bijektion von $A$ nach $B$.

$\square$