Einführung in die Logik

Aufgabenblatt 5, 2023-06-19

Präsenzaufgabe 1

Beweisen Sie den Satz auf Folie 221.

Lösungsvorschlag:

In jedem der Fälle Modus Ponens, Modus tollens und Kontraposition wählen wir eine $\mathcal{S}$-Struktur $\mathcal{M} = \langle D, I \rangle$ und eine Belegung $\sigma \in D^{\mathcal{V}}$ der Variablen, so dass alle Formeln in Γ erfüllt werden.

- **Modus Ponens**: Wir gehen davon aus, dass das Paar $\langle \mathcal{M}, \sigma \rangle$ auch B sowie $B \to A$ erfüllt, d.h.,
$$\mathcal{M}[\![B]\!](\sigma) = \mathcal{M}[\![B \to A]\!](\sigma) = 1$$
Aber letzteres ist gleichbedeutend mit
$$\mathcal{M}[\![B]\!](\sigma) \leqslant \mathcal{M}[\![A]\!](\sigma) \tag{$*$}$$
und folglich muß auch gelten
$$\mathcal{M}[\![A]\!](\sigma) = 1$$
- **Modus Tollens**: Wir gehen davon aus, dass das Paar $\langle \mathcal{M}, \sigma \rangle$ auch $B \to A$ sowie $\neg A$ erfüllt, d.h.,
$$\mathcal{M}[\![B \to A]\!](\sigma) = 1 - \mathcal{M}[\![A]\!](\sigma) = 1$$
Wegen $(*)$ gilt auch
$$\mathcal{M}[\![\neg A]\!](\sigma) = 1 - \mathcal{M}[\![A]\!](\sigma) \leqslant 1 - \mathcal{M}[\![B]\!](\sigma) = \mathcal{M}[\![\neg B]\!](\sigma)$$
woraus schließlich folgt
$$\mathcal{M}[\![\neg B]\!](\sigma) = 1$$
- **Modus Bogus**: Hier genügt ein Gegenbeispiel. Betrachte die Signatur $\mathcal{S}_{\text{arith}}$ der Arithmetik sowie die Formeln A und B, die aussagen, dass x durch 2 bzw. durch 4 teilbar ist, also
$$A(x) = \exists y.\, x \doteq y + y \quad \text{und} \quad B(x) = \exists y.\, x \doteq y + y + y + y$$
Offenbar ist jede durch 4 teilbare Zahl auch durch 2 teilbar, also
$$\models B(x) \to A(x) \quad \text{und somit} \quad \Gamma \models B(x) \to A(x) \quad \text{für jede Prämissenmenge} \quad \Gamma$$
Nun bestehe Γ aus der einzigen Prämisse, dass x^2 gerade ist:
$$G(x) = \exists z.\, x * x \doteq z + z$$
Es gilt also
$$\{G(x)\} \models B(x) \to A(x) \quad \text{sowie} \quad \{G(x)\} \models A(x)$$
aber unter der Voraussetzung, dass x^2 gerade ist, können wir i.A. *nicht* folgern, dass x durch 4 teilbar ist, d.h.,
$$\{G(x)\} \not\models B(x)$$
Betrachte etwa eine Belegung σ mit $\sigma(x) = 2$.

- **Kontraposition**: Aufgrund des semantischen Deduktionstheorems der Prädikatenlogik (Folie 220) können wir die Aussage umformlieren zu

$$\Gamma \models B \to \neg A \quad \text{gdw.} \quad \Gamma \models A \to \neg B$$

Analog wie oben ergibt sich nun

$$\begin{aligned} \mathcal{M}[\![B \to \neg A]\!](\sigma) = 1 \quad &\text{gdw.} \quad \mathcal{M}[\![B]\!](\sigma) \leqslant 1 - [\![A]\!](\sigma) \\ &\text{gdw.} \quad \mathcal{M}[\![A]\!](\sigma) \leqslant 1 - [\![B]\!](\sigma) \quad \text{gdw.} \quad \mathcal{M}[\![A \to \neg B]\!](\sigma) = 1 \end{aligned}$$

Präsenzaufgabe 2

Begründen Sie ihre Antworten ausführlich:

(a) Die Signatur S möge mindestens ein einstelliges Prädikatensymbol P enthalten. Wir betrachten einen Term t, in dem die Variable x nicht vorkommt. Ist die Formel

$$P(t) \leftrightarrow \forall x : (x \doteq t \to P(x))$$

allgemeingültig?

(b) Bleibt die Antwort dieselbe, wenn x im Term t vorkommt?

Lösungsvorschlag:

(a) Die Behauptung ist korrekt: Betrachte eine S-Struktur $\mathcal{M} = \langle D, I \rangle$ und eine Belegung $\sigma \in D^{\mathcal{V}}$. Dann gilt

$$\mathcal{M}[\![P(t)]\!](\sigma) = 1 \quad \text{gdw.} \quad \mathcal{M}[\![t]\!](\sigma) \in P^{\mathcal{M}} \subseteq D \quad \text{gdw.} \quad P^{\mathcal{M}}(\mathcal{M}[\![t]\!](\sigma)) = 1$$

insbesondere also $\mathcal{M}[\![P(t)]\!](\sigma) = P^{\mathcal{M}}\big(\mathcal{M}[\![t]\!](\sigma)\big)$, sowie

$$\begin{aligned}
&\mathcal{M}[\![\forall x \, (x \doteq t \to P(x))]\!](\sigma) && (1)\\
&= \inf\{\, \mathcal{M}[\![x \doteq t \to P(x)]\!](\sigma\{x/d\}) \;:\; d \in D \,\} && (2)\\
&= \inf\{\, \mathcal{M}[\![\neg(x \doteq t) \vee P(x)]\!](\sigma\{x/d\}) \;:\; d \in D \,\} && (3)\\
&= \inf\{\, \sup\{\mathcal{M}[\![\neg(x \doteq t)]\!](\sigma\{x/d\}), \mathcal{M}[\![P(x)]\!](\sigma\{x/d\})\} \;:\; d \in D \,\} && (4)\\
&= \inf\{\, \sup\{1 - \mathcal{M}[\![x \doteq t]\!](\sigma\{x/d\}), \mathcal{M}[\![P(x)]\!](\sigma\{x/d\})\} \;:\; d \in D \,\} && (5)\\
&= \inf\{\, \sup\{1 - (\mathcal{M}[\![x]\!](\sigma\{x/d\}) = \mathcal{M}[\![t]\!](\sigma\{x/d\})), P^{\mathcal{M}}(\mathcal{M}[\![x]\!](\sigma\{x/d\}))\} \;:\; d \in D \,\} && (6)\\
&= \inf\{\, \sup\{1 - (d = \mathcal{M}[\![t\{x/d\}]\!](\sigma)), P^{\mathcal{M}}(d)\} \;:\; d \in D \,\} && (7)\\
&= \inf\{\, \sup\{1 - (d = \mathcal{M}[\![t]\!](\sigma)), P^{\mathcal{M}}(d)\} \;:\; d \in D \,\} && (8)\\
&= \inf\{\, \sup\{d \neq \mathcal{M}[\![t]\!](\sigma), P^{\mathcal{M}}(d)\} \;:\; d \in D \,\} && (9)\\
&= \inf\{\, \sup\{d \neq \mathcal{M}[\![t]\!](\sigma), P^{\mathcal{M}}((\mathcal{M}[\![t]\!](\sigma))\} \;:\; d \in D \,\} && (10)\\
&= \sup\{\, \inf\{\, d \neq \mathcal{M}[\![t]\!](\sigma) \;:\; d \in D \,\}, \inf\{\, P^{\mathcal{M}}\big(\mathcal{M}[\![t]\!](\sigma)\big) \;:\; d \in D \,\} \,\} && (11)\\
&= \sup\{\, 0, P^{\mathcal{M}}\big(\mathcal{M}[\![t]\!](\sigma)\big) \,\} && (12)\\
&= \mathcal{M}[\![P(t)]\!](\sigma) && (13)
\end{aligned}$$

Dabei wurde in Zeile (7) das Substitutionslemma angewendet. Zeile (8) folgt, weil x nicht in t vorkommt, die Substitution $\{x/d\}$ also wirkungslos bleibt. In Zeile (10) kommt zum Tragen, dass das binäre Supremum den Wert 0 höchstens für $d = \mathcal{M}[\![t]\!](\sigma)$ annehmen kann, während Zeile (11) das Distributivgesetz für Suprema und Infima in $\mathbb{B}$ verwendet, vergl. Hinweis zu Aufgabe 5, Blatt 4.

(b) Wenn x in t vorkommt, enthält $P(t)$ die freie Variable x, die rechte Seite der Äquivalenz aber nicht. Wir wollen versuchen, in einer Struktur $\mathcal{M} = \langle D, I \rangle$ die Voraussetzung der Implikation $x \doteq t \to P(x)$ immer falsch und somit die rechte Seite der Äquivalenz immer wahr zu machen, während der Wert von $\mathcal{M}[\![P(t)]\!]$ von σ abhängen kann, also nicht immer wahr zu sein braucht. Insbesondere ist $P^{\mathcal{M}}$ dann eine echte Teilmenge von D.

Beispiel: für den Datenbereich $D = \mathbb{N}$, das Prädikat $P(x)$ "x ist gerade" und den Term $t := x + 1$ passiert genau das: $P(t)$ ist nur für ungerade Zahlen $\sigma(x)$ erfüllt, aber die Implikation auf der rechten Seite ist aufgrund der immer falschen Voraussetzung für jedes $a \in \mathbb{N}$ erfüllt, also ist die rechte Seite immer wahr.

Die linke Seite wird aber für solche Belegungen σ falsch, die x eine gerade Zahl zuordnen.

Hausaufgabe 3 [16 PUNKTE]

Rechenregeln für Quantoren (Folie 224):

1. [10 PUNKTE] Beweisen Sie jeweils die rechte Aussage von (1), (2) und (3).
2. [6 PUNKTE] Beweisen Sie (4) und geben Sie im Fall $x \in \boldsymbol{FV}(A)$ ein Gegenbeispiel an. **Hinweis**: Sie dürfen verwenden, dass die Supremum- und Infimum-Operationen in $\mathbb{B}$ für beliebig indexierte Familen $\langle b_i : i \in I \rangle \in \mathbb{B}^I$ ein Distributiv-Gesetz analog zu dem auf Folie 71 erfüllen: d.h.,

$$a \wedge \sup_{i \in I} b_i = \sup_{i \in I} (a \wedge b_i) \qquad \text{sowie} \qquad a \vee \inf_{i \in I} b_i = \inf_{i \in I} (a \vee b_i)$$

Lösungsvorschlag:

Wir wählen jeweils eine $\mathcal{S}$-Struktur $\mathcal{M} = \langle D, I \rangle$ und eine Belegung $\sigma \in D^{\mathcal{V}}$ der Variablen.

1. [3 PUNKTE] Behauptung: $\neg \exists x\, A \mathrel{\vDash\!\!\!\Dashv} \forall x\, \neg A$

$$\begin{aligned}
\hat{\sigma}(\neg \exists x.\, A) &= 1 - \hat{\sigma}(\exists x.\, A) \\
&= 1 - \sup\{\, \widehat{\sigma\{x/d\}}(A) \;:\; d \in D \,\} \\
&= \inf\{\, 1 - \widehat{\sigma\{x/d\}}(A) \;:\; d \in D \,\} \\
&= \inf\{\, \widehat{\sigma\{x/d\}}(\neg A) \;:\; d \in D \,\} \\
&= \hat{\sigma}(\forall x.\, \neg A)
\end{aligned}$$

[4 PUNKTE] Behauptung: $\exists x.\, A \vee \exists x.\, B \mathrel{\vDash\!\!\!\Dashv} \exists x.\, (A \vee B)$

$$\begin{aligned}
\hat{\sigma}(\exists x.\, A \vee \exists x.\, B) &= \sup\big\{\, \hat{\sigma}(\exists x.\, A), \hat{\sigma}(\exists x.\, B) \,\big\} \\
&= \sup\big\{\, \sup\{\, \widehat{\sigma\{x/d\}}(A) \;:\; d \in D \,\}, \sup\{\, \widehat{\sigma\{x/e\}}(B) \;:\; e \in D \,\} \,\big\} \\
&= \sup\big\{\, \sup\{\, \widehat{\sigma\{x/d\}}(A), \widehat{\sigma\{x/e\}}(B) \,\} \;:\; d, e \in D \,\big\} \\
&\geqslant \sup\big\{\, \sup\{\, \widehat{\sigma\{x/f\}}(A), \widehat{\sigma\{x/f\}}(B) \,\} \;:\; f \in D \,\big\} \\
&= \sup\big\{\, \widehat{\sigma\{x/f\}}(A \vee B) \;:\; f \in D \,\big\} \\
&= \hat{\sigma}(\exists x.\, A \vee B)
\end{aligned}$$

Warum dürfen wir in Schritt 4 die Relation $\geqslant$ durch $=$ ersetzen? Die einzige Möglichkeit, dass $\sup\big\{\, \sup\{\, \widehat{\sigma\{x/f\}}(A), \widehat{\sigma\{x/f\}}(B) \,\} \;:\; f \in D \,\big\}$ den Wert 0 annimmt, besteht darin, dass für jedes $f \in D$ sowohl $\widehat{\sigma\{x/f\}}(A) = 0$ als auch $\widehat{\sigma\{x/f\}}(B) = 0$ gilt. Aber dann haben wir für alle $\langle d, e \rangle \in D^2$ auch $\sup\{\, \widehat{\sigma\{x/d\}}(A), \widehat{\sigma\{x/e\}}(B) \,\} = 0$.

[3 PUNKTE] Behauptung: $\exists x\, \exists y.\, A \mathrel{|}\!\!\!=\!\!\!\mathrel{|} \exists y\, \exists x.\, A$ mit $x \neq y$

$$\begin{aligned}
\hat{\sigma}(\exists x\, \exists y.\, A) &= \sup\left\{ \widehat{\sigma\{x/d\}}(\exists y.\, A) \;:\; d \in D \right\} \\
&= \sup\left\{ \sup\{ \widehat{\sigma\{x/d\}\{y/e\}}(A) \;:\; e \in D \} \;:\; d \in D \right\} \\
&= \sup\left\{ \widehat{\sigma\{x/d\}\{y/e\}}(A) \;:\; \langle d, e\rangle \in D \times D \right\} \\
&= \sup\left\{ \widehat{\sigma\{y/e\}\{x/d\}}(A) \;:\; \langle e, d\rangle \in D \times D \right\} \\
&= \sup\left\{ \sup\{ \widehat{\sigma\{y/e\}\{x/d\}}(A) \;:\; d \in D \} \;:\; e \in D \right\} \\
&= \sup\left\{ \widehat{\sigma\{y/e\}}(\exists x.\, A) \;:\; e \in D \right\} \\
&= \hat{\sigma}(\exists y\, \exists x.\, A)
\end{aligned}$$

2. Behauptung: $A \star \mathcal{Q}x\, B \mathrel{|}\!\!\!=\!\!\!\mathrel{|} \mathcal{Q}x\, (A \star B)$

   Der Junktor $\rightarrow$ kann analog zu $\vee$ abgehandelt werden.

   Zu überprüfen bleiben vier Fälle, von denen jeweils zwei dual zueinander sind. Aufgrund der Voraussetzung $x \notin \boldsymbol{FV}(A)$ gilt $\hat{\sigma}(A) = \widehat{\sigma\{x/d\}}(A)$ für jedes $d \in D$.

   (a) [3 PUNKTE]

$$\begin{aligned}
\hat{\sigma}(A \wedge \forall x.\, B) &= \inf\left\{ \hat{\sigma}(A), \inf\{ \widehat{\sigma\{x/d\}}(B) \;:\; d \in D \}\right\} \\
&= \inf\left\{ \inf\{\hat{\sigma}(A), \widehat{\sigma\{x/d\}}(B)\} \;:\; d \in D \right\} \\
&= \inf\left\{ \inf\{\widehat{\sigma\{x/d\}}(A), \widehat{\sigma\{x/d\}}(B)\} \;:\; d \in D \right\} \\
&= \inf\left\{ \widehat{\sigma\{x/d\}}(A \wedge B)\} \;:\; d \in D \right\} \\
&= \hat{\sigma}\big(\forall x.\, (A \wedge B)\big)
\end{aligned}$$

   Analog folgt

$$\hat{\sigma}(A \vee \exists x.\, B) = \hat{\sigma}\big(\exists x.\, (A \vee B)\big)$$

   (b) [3 PUNKTE]

$$\begin{aligned}
\hat{\sigma}(A \wedge \exists x.\, B) &= \inf\left\{ \hat{\sigma}(A), \sup\{ \widehat{\sigma\{x/d\}}(B) \;:\; d \in D \}\right\} \\
&= \sup\left\{ \inf\{\hat{\sigma}(A), \widehat{\sigma\{x/d\}}(B)\} \;:\; d \in D \right\} \\
&= \sup\left\{ \inf\{\widehat{\sigma\{x/d\}}(A), \widehat{\sigma\{x/d\}}(B)\} \;:\; d \in D \right\} \\
&= \sup\left\{ \widehat{\sigma\{x/d\}}(A \wedge B)\} \;:\; d \in D \right\} \\
&= \hat{\sigma}\big(\exists x.\, (A \wedge B)\big)
\end{aligned}$$

   Analog folgt

$$\hat{\sigma}(A \vee \forall x.\, B) = \hat{\sigma}\big(\forall x.\, (A \vee B)\big)$$

Hausaufgabe 4 [21 PUNKTE]

[21 PUNKTE] Beweisen Sie das Substitutionslemma ohne Verwendung von Semantik-Klammern $[\![\cdot]\!]$, aber stattdessen mit $\check{\sigma}$, $\overline{\sigma}$ und $\hat{\sigma}$. Genauer: für eine $\mathcal{S}$-Struktur $\mathcal{M} = \langle D, I\rangle$ gilt

$$\check{\sigma}(u\{x/t\}) = \check{\sigma}\{x/\check{\sigma}(t)\}(u) \quad \text{sowie} \quad \hat{\sigma}(A\{x/t\}) = \hat{\sigma}\{x/\check{\sigma}(t)\}(A)$$

wobei u ein Term und A eine Formel ist.

Lösungsvorschlag:

Beweis für Terme: Wir schreiben $\boldsymbol{u}$ für $\langle u_0, \ldots, u_{n-1}\rangle \in \boldsymbol{Term}(\boldsymbol{Fun}, \mathcal{V})^n$.

- [2 PUNKTE] ξ ist eine von x verschiedene Variable u:

$$\check{\sigma}(u\{x/t\}) = \check{\sigma}(u) = \widetilde{\sigma\{x/t\}}(u)$$

- [2 PUNKTE] $\xi = x$:

$$\check{\sigma}(x\{x/t\}) = \overline{\sigma}(t) = \widetilde{\sigma\{x/t\}}(x)$$

- [2 PUNKTE] $\xi = f(\boldsymbol{u})$:

$$\check{\sigma}(f(\boldsymbol{u})\{x/t\}) = f^{\mathcal{M}}\big\langle\check{\sigma}(\boldsymbol{u}\{x/t\})\big\rangle = f^{\mathcal{M}}\big\langle\widetilde{\sigma\{x/\check{\sigma}(t)\}}(\boldsymbol{u})\big\rangle = \widetilde{\sigma\{x/\check{\sigma}(t)\}}(f(\boldsymbol{u}))$$

Beweis für atomare Formeln:

- [3 PUNKTE] ξ ist eine Gleichung $u_0 \doteq u_1$:

$$\begin{aligned} & \overline{\sigma}\big((u_0 \doteq u_1)\{x/t\}\big) = 1 \\ \text{gdw.}\quad & \check{\sigma}(u_0\{x/t\}) = \check{\sigma}(u_1\{x/t\}) \\ \text{gdw.}\quad & \widetilde{\sigma\{x/\check{\sigma}(t)\}}(u_0) = \widetilde{\sigma\{x/\check{\sigma}(t)\}}(u_1) \\ \text{gdw.}\quad & \overline{\sigma\{x/\check{\sigma}(t)\}}(u_0 \doteq u_1) = 1 \end{aligned}$$

- [3 PUNKTE] ξ ist eine Prädikatenauswertung $P(\boldsymbol{u})$:

$$\begin{aligned} & \overline{\sigma}\big(P(\boldsymbol{u})\{x/t\}\big) = 1 \\ \text{gdw.}\quad & \langle\check{\sigma}(\boldsymbol{u}\{x/t\})\rangle \in P^{\mathcal{M}} \\ \text{gdw.}\quad & \langle\widetilde{\sigma\{x/\check{\sigma}(t)\}}(\boldsymbol{u})\rangle \in P^{\mathcal{M}} \\ \text{gdw.}\quad & \overline{\sigma\{x/\check{\sigma}(t)\}}(P(\boldsymbol{u})) = 1 \end{aligned}$$

Beweis für aussagenlogisch zusammengesetzte Formeln:

- [2 PUNKTE] A ist eine Negation $\neg B$:

$$\begin{aligned} \hat{\sigma}(\neg B\{x/t\}) &= 1 - \hat{\sigma}(B\{x/t\}) \\ &= 1 - \widehat{\sigma\{x/\check{\sigma}(t)\}}(B) = \widehat{\sigma\{x/\check{\sigma}(t)\}}(\neg B) \end{aligned}$$

- [2 PUNKTE] ξ ist eine Konjunktion $B \wedge C$:

$$\begin{aligned} \hat{\sigma}((B \wedge C)\{x/t\}) &= \inf\{\hat{\sigma}(B\{x/t\}), \hat{\sigma}(C\{x/t\})\} \\ &= \inf\{\widehat{\sigma\{x/\check{\sigma}(t)\}}(B), \widehat{\sigma\{x/\check{\sigma}(t)\}}(C)\} = \widehat{\sigma\{x/\check{\sigma}(t)\}}(B \wedge C) \end{aligned}$$

- ξ ist eine Disjunktion $B \vee C$: analog, mit $\sup$ anstelle von $\inf$.
- ξ ist eine Implikation $B \to C$: umschreiben zu $\neg B \vee C$.

Beweis für quantifizierte Formeln:

- [5 PUNKTE] A ist eine $\forall$-quantifizierte Formel $\forall y\, B$:

$$
\begin{aligned}
& \hat{\sigma}(\forall y.\, B\{x/t\}) \qquad \text{(Achtung: } y \text{ könnte in } t \text{ auftreten!)} \\
&= \hat{\sigma}(\forall z.\, B\{y/z\}\{x/t\}) \text{ mit } z \notin V(B) \cup \{x\} \cup V(t) \\
&= \inf\Big\{\, \widehat{\sigma\{z/d\}}(B\{y/z\}\{x/t\}) \;:\; d \in D \Big\} \\
&= \inf\Big\{\, \widehat{\sigma\{z/d\}\{x/\widehat{\sigma\{z/d\}}(t)\}}(B\{y/z\}) \;:\; d \in D \Big\} \\
&= \inf\Big\{\, \widehat{\sigma\{z/d\}\{x/\check{\sigma}(t)\}}(B\{y/z\}) \;:\; d \in D \Big\} \text{ da } z \notin V(t) \\
&= \inf\Big\{\, \widehat{\sigma\{x/\check{\sigma}(t)\}\{z/d\}}(B\{y/z\}) \;:\; d \in D \Big\} \text{ da } z \neq x \\
&= \widehat{\sigma\{x/\check{\sigma}(t)\}}(\forall z.\ B\{y/z\}) \\
&= \widehat{\sigma\{x/\check{\sigma}(t)\}}(\forall y.\ B)
\end{aligned}
$$

Hausaufgabe 5 [16 PUNKTE]

Wir betrachten die Signatur Σ der Arithmetik mit zwei Konstanten 0 und 1, zwei zweistelligen Funktionensymbolen $+$ und $\cdot$ einem zweistelligen Prädikatensymbol $<$. Viele Aussagen über natürliche Zahlen (also die Σ- Struktur mit Trägermenge $\mathbb{N}$ und der üblichen Interpretation der Symbole in Σ) lassen sich als prädikatenlogische Formeln über Σ ausdrücken.

Beispiel: Der Aussage „ x ist eine gerade Zahl“ entspricht die Formel $\exists y : (x = y + y)$ mit einer freien Variable x.

Transformieren Sie die folgenden Aussagen in prädikatenlogische Formeln über Σ:

(a) [5 PUNKTE] „ x und Y sind Primzahlzwillinge.“

(b) [5 PUNKTE] „Es gibt unendlich viele pythagoräische Tripel“

(c) [3 PUNKTE] „Jede gerade Zahl $\geqslant 4$ läßt sich als Summe zweier Primzahlen darstellen.“

(d) [3 PUNKTE] „Alle Zahlen mit geradem Quadrat sind gerade.“

Lösungsvorschlag:

Wir machen uns das Leben leichter, indem wir geeignete Abkürzungen einführen. Man beachte, dass die dabei gebundenen Variablen in der Abkürzung nicht vorkommen. D.h., wir verwenden die Tatsache, dass gebundene Variablen immer geeignet umbenannt werden können.

(a) Primzahlen lassen sich charakterisieren mit

$$P(x) := \neg(x \doteq 1) \wedge \forall y.\, \big(\exists z.\, y \cdot z \doteq x \rightarrow (y \doteq 1) \vee (y \doteq x)\big)$$

Die gewünschte Aussage ist dann

$$P(x) \wedge P(y) \wedge (x + 1 + 1 \doteq y \vee y + 1 + 1 \doteq x)$$

(b) Ein pythagoräisches Tripel $\langle a, b, c\rangle \in \mathbb{N}^3$ erfüllt definitionsgemäß $a^2 + b^2 = c^2$, z.B. $\langle 3, 4, 5\rangle$ oder $\langle 5, 12, 13\rangle$. Um unendlich viele davon zu garantieren, kann man z.B. verlangen, dass zu jedem $n \in \mathbb{N}$ solch ein Tripel mit $n < a + b + c$ existiert:

$$\forall w\, \exists x\, \exists y\, \exists z.\, (w < x + y + z \wedge x * x + y * y = z * z)$$

(c) $\forall x.\ (1 + 1 + 1 < x \wedge \exists y : y + y \doteq x \rightarrow \exists u.\, \exists v.\, P(u) \wedge P(v)\ x \doteq u + v)$

(d) Charakterisierung der geraden Zahlen: $G(x) := \exists y.\, x \doteq y + y$. Das liefert:

$$\forall x.\, (G(x * x) \to G(x))$$

Hausaufgabe 6 [12 PUNKTE]

Berechnen Sie eine erfüllbarkeitsäquivalente Formel in Skolem-Normalform zu

$$\big(\forall x\, \exists y.\, P(x, f(y))\big) \wedge \Big(\neg \exists y\, \forall x\, \exists z.\, \big(Q(g(z), f(x)) \vee P(y, z)\big)\Big)$$

Lösungsvorschlag:

Zunächst ist die Formel zu bereinigen. Dazu benennen wir die Variablen x und y im ersten Teil in u bzw. v um:

$$\big(\forall u\, \exists v.\, P(u, f(v))\big) \wedge \Big(\neg \exists y\, \forall x\, \exists z.\, \big(Q(g(z), f(x)) \vee P(y, z)\big)\Big)$$

Anwendung der verallgemeinerten De Morgan'schen Regeln liefert

$$\big(\forall u\, \exists v.\, P(u, f(v))\big) \wedge \Big(\forall y\, \exists x\, \forall z.\, \big(\neg Q(g(z), f(x)) \wedge \neg P(y, z)\big)\Big)$$

woaraus wir gemäß Rechenregel (2) eine PNF gewinnen:

$$\forall u\, \exists v\, \forall y\, \exists x\, \forall z.\, \big(P(u, f(v)) \wedge \neg Q(g(z), f(x)) \wedge \neg P(y, z)\big)$$

Zwecks Skolemisierung führen wir für v die frische Funktion $g_{/1}$ und für x die frische Funktion $h_{/2}$ ein:

$$\forall u\, \forall y\, \forall z.\, \big(P(u, f(g(u))) \wedge \neg Q(g(z), f(h(u, y))) \wedge \neg P(y, z)\big)$$