Hilfsblatt zur Klausur Mathematische Logik I (WS04/05)

von Ulrich Loup

Hinweis: Dieses Hilfsblatt kann leserlich auf *ein* Blatt gedruckt werden. Ich erhebe keinen Anspruch auf Vollständigkeit oder Richtigkeit meiner Angaben. Kommentare o.ä. an `Ulrich.Loup@rwth-aachen.de`.

1. Aussagenlogosche **Horn-Formeln** sind Formeln in KNF, bei der jede (*Horn*-)Klausel (Disjunktion) höchstens ein positives Literal enthält. Horn-Formeln können auch als Konjunktion von Implikationen geschrieben werden, folgende Fälle treten auf:

   (a) $\neg X_1 \vee \cdots \vee \neg X_k \vee X \equiv X_1 \wedge \cdots \wedge X_k \to X$ für $k = 0$: $1 \to X$

   (b) $\neg X_1 \vee \cdots \vee \neg X_k \equiv X_1 \wedge \cdots \wedge X_k \to 0$

   Die Klauseln in Fall 1 für $k = 0$ bezeichne $\mathcal{C}_1$ und die Implikationen aus Fall 2 $\mathcal{C}_2$. Eine Formel ist folglich erfüllbar, wenn sie keine $\mathcal{C}_1$-Klauseln enthält (durch Belegung aller Variablen mit 0) oder wenn sie keine $\mathcal{C}_2$-Klauseln enthält (durch Belegung aller Variablen mit 1). Ein algorithmischer Erfüllbarkeitstest braucht deshalb nur die Variablen der $\mathcal{C}_1$-/ $\mathcal{C}_2$-Klauseln zu berücksichtigen. Tritt nämlich eine Klausel vom Typ $\mathcal{C}_1$ in einer Formel φ auf, so darf dort keine Klausel der Form $\mathcal{C}_2$ enthalten sein. Ist dies der Fall, ist φ unerfüllbar, ansonsten werden die X mit $1 \to X$ und $X_1 \wedge \cdots \wedge X_k \to X$ auf 1 gesetzt und die anderen Variablen auf 0.

2. Der **Resolutionskalkül** ist nur auf eine Klauselmenge $K := K(\psi)$ anwendbar, die die Klauseln (Menge von Literalen der Disjunktionen) einer KNF-Formel $\psi \in \text{AL}$ enthält. Es gilt $\Box \in \mathit{Res}^*(K) \Leftrightarrow K$ unerfüllbar. $\mathit{Res}^0(K) := K$, $\mathit{Res}^{n+1}(K) := \mathit{Res}(\mathit{Res}^n(K))$ und $\mathit{Res}(K) := K \cup \{$alle Resolventen der Klauseln aus $K\}$. Seien $\varphi, \psi \in \text{AL}$:

   - Geeignet für ψ in DNF: ψ allgemeingültig $\Leftrightarrow \neg\psi$ unerfüllbar. ($\neg\psi$ in KNF, also Resolution anwendbar.)
   - Geeignet für φ in DNF, ψ in KNF: $\psi \models \varphi \Leftrightarrow \psi \wedge \neg\varphi$ unerfüllbar.
   - Für Literale A, B ist $A \to B \equiv \neg A \vee B$ nur *eine* Klausel.
   - Für Horn-Formeln: *Einheitsresolution* analog zum Resolutionskalkül, Klauselmengen dürfen aber nur mit einer Klauselmenge C mit $|C| = 1$ resolviert werden. Die abgeleitete Resolvente heißt *Einheitsresolvente.*
   - Allgemein: Der Resolutionskalkül ist *korrekt*, wenn keine falschen Aussagen abgeleitet werden können. (Gegenbeweis: Zeige, dass aus einer gültigen Klauselmenge $\Box$ ableitbar ist.) Der Kalkül ist *vollständig*, wenn alle wahren Aussagen ableitbar sind.
   - *Tipp:* Bei der Bestimmung von *Res** *alle* möglichen Ableitungen bilden! Immer nur eine Variable in einem Schritt resolvieren sonst Multiresolution, welche nicht korrekt (aber vollständig)!

3. Eine Schlussregel $\frac{\text{Prämissen}}{\text{Konklusion}} = \frac{A_1 \Rightarrow B_1 \quad A_2 \Rightarrow B_2}{A \Rightarrow B}$ in einem **Sequenzenkalkül** ist *korrekt* $\Leftrightarrow$ jede die Konklusion falsifizierende Interpretation falsifiziert auch eine der Prämissen. Wähle Interpretation $\mathfrak{I}$, die Modell des Antezedens (A) ist und nicht Modell des Sukzedens (B) der Konklusion. Beachte, dass $\Gamma, \Delta = \Gamma \cup \Delta$.

   - Zeige für den *Beweis*, dass *eine* der Prämissen mit den Vor. *nicht* gültig ist (evtl. für mehrere Fälle).
   - Der *Gegenbeweis* benutzt $\mathfrak{I}$, um zu zeigen, dass die Prämissen *alle* gültig sind. Konstruiere dann ein Gegenbeispiel (etwa durch Setzen einiger Formeln gleich $\emptyset$).

4. **Strukturen** sind Tupel der Form (U, τ), wobei U Menge (*Universum*) und τ Menge von endlich-stelligen Relationen und Funktionen (*Signatur*) auf U ist. Für τ-Struktur $\mathfrak{A} \in \text{Str}(\tau)$ (Universum wie Struktur: A) ist

   - $\mathfrak{B}$ die *Substruktur* von $\mathfrak{A}$ ($\mathfrak{B} \subseteq \mathfrak{A}$), falls $B \subseteq A$ und B τ-abgeschlossen ist, d.h., alle Relationen gelten auch in B und keine Funktion führt durch Anwenden aus B hinaus. $\mathfrak{A}$ heißt dann *Erweiterung* von $\mathfrak{B}$.
   - für $\sigma \subseteq \tau$ das σ-Redukt $\mathfrak{B} := \mathfrak{A} \restriction \sigma$ die Struktur (A, σ) durch Weglassen von $\tau \setminus \sigma$. $\mathfrak{A}$ heißt τ*-Expansion.*

     Beachte die trivialen Substrukturen $\mathfrak{A} \subseteq \mathfrak{A}$ und die trivialen Redukte von $\mathfrak{A}$ nämlich $(A, \emptyset) = (A)$ und $\mathfrak{A}$. Bei geordneten τ-Strukturen gibt es für $n := |\tau|$ gerade $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ Redukte.
   - $\mathfrak{A} = (A, <)$ mit $\tau = \{<\}$ heißt eine **partielle Ordnung**, falls (1),(2) und damit auch (3) gilt („<" kann jede beliebige Relation sein). $\mathfrak{A}$ heißt *linear*, falls (4) gilt, *dicht*, falls (5) gilt und *diskret*, falls (6) gilt. Eine lineare Ordnung ohne unendliche absteigende Ketten heißt *Wohlordnung* z.B. $(\mathbb{N}, <)$.

     (1) *Irreflexivität*: $\forall x \neg(x < x)$

     (2) *Transitivität*: $\forall x \forall y \forall z((x < y \wedge y < z) \to x < z)$

     (3) *Antisymmetrie*: $\forall x \forall y(a < b \to \neg(b < a))$

     (4) *Vergleichbarkeit*: $\forall x \forall y(x < y \vee x = y \vee y < x)$

     (5) $\forall x \forall y(x < y \to \exists z(x < z \wedge z < y))$

     (6) $\forall x[\forall y((x < y \vee y < x)) \vee \exists y \forall z((y < x \to (z < y \vee x < z)) \vee (x < y \to (z < x \vee y < z)))]$

5. Seien A, B zwei Mengen. A ist mindestens so mächtig wie B ($|A| \geq |B|$), wenn eine Einbettung $B \hookrightarrow A$ existiert. A und B heißen *gleichmächtig* ($|A| = |B|$), falls eine Bijektion $A \leftrightarrow B$ existiert oder die gegenseitigen Einbettungen $A \hookrightarrow B$ und $B \hookrightarrow A$ existieren. A heißt abzählbar, falls es eine surjektive Abbildung $\mathbb{N} \twoheadrightarrow A$ gibt.

   - *Lemma [2.1]:* Ist eine Menge abzählbar, so ist sie entweder endlich oder gleichmächtig zu $\mathbb{N}$.
   - *Satz [2.2]:* Keine Menge A ist gleichmächtig zu ihrer Potenzmenge $Pot(A) = \{B \subseteq A\}$.

6. **Homomorphismen** sind strukturerhaltende Abbildungen $\pi : A \to B$ mit den folgenden Eigenschaften:

   (a) $(a_1, \ldots, a_n) \in R^{\mathfrak{A}} \;\Rightarrow\; (\pi a_1, \ldots, \pi a_n) \in R^{\mathfrak{B}}$ für alle n-stelligen Relationssymbole R und $a_1, \ldots, a_n \in A$.

   (b) $\pi f^{\mathfrak{A}}(a_1, \ldots, a_n) = f^{\mathfrak{B}}(\pi a_1, \ldots, \pi a_n)$ für alle n-stelligen Funktionssymbole f und $a_1, \ldots, a_n \in A$.

   Ist der Homomorphismus *stark*, so gilt bei 1. nicht „$\Rightarrow$“ sondern „$\Leftrightarrow$“. Es heißt $A \hookrightarrow B$ eine *Einbettung* (injektiver Hom.) von $\mathfrak{A}$ in $\mathfrak{B}$, $A \leftrightarrow B$ ein Isomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$, $A \leftrightarrow A$ ein Automorphismus von $\mathfrak{A}$.

7. **Normalformen** sind äquivalente Umformungen prädikatenlogischer Formeln:

   - *NNF* (Negationsnormalform): Negationen stehen nur bei atomaren Formeln (Literale zwischen den Junktoren). Für $\varphi, \psi \in$ FO: $\neg(\varphi \circ \psi) \equiv (\neg\varphi * \neg\psi)$ mit $\circ, * \in \{\wedge, \vee\}$, $\circ \neq *$ und $\neg Qx\varphi \equiv Qx\neg\varphi$ mit $Q \in \{\exists, \forall\}$.
   - *PNF* (Pränex-Normalform): Quantoren nur im *Präfix* der Formel und Formel ist *bereinigt* (Variablen entweder frei oder gebunden und höchstens einmal quantifiziert). *Bereinigen:* von innen nach außen sukzessive jede Variable, die sowohl frei (ungebunden) als auch gebunden ist, in noch nicht verwendeten Variablennamen umbenennen. $\Rightarrow$ Quantoren können unter Beachtung der Reihenfolge ins Präfix geschrieben werden.
   - *SNF* (Skolem-Normalform): PNF ohne $\exists$-Quantoren. *Konstruktion:* jede durch den k-ten $\exists$-Quantor gebundene Variable wird durch ein neues $k-1$-stelliges Funktionssymbol $f_k(x_1, \ldots, x_{k-1})$ mit $x_1, \ldots, x_{k-1}$ den bis dahin quantifizierten Variablen ersetzt und der Quantor wird einfach weggelassen.
   - **Substitutionen:** Ssimultan: $\varphi[x_1/l_1, \ldots, x_k/l_k]$, hintereinander ausgeführt: $\varphi[x_1/l_1] \ldots [x_k/l_k]$. Gebundene Variablen werden nicht ersetzt. Kollisionen mit den Bezeichnern in der Substitutionsregel und gebundenen Variablen werden durch Umbenennen der gebundenen Variablen vermieden.

8. Ein **Spiel** ist *fundiert*, wenn es endlich ist. Es heißt *determiniert*, wenn ein Spieler von jeder Position aus eine GWS (Gewinnstrategie) hat. Ist ein Spiel fundiert, so auch determiniert.

   - MC($\mathfrak{A}, \varphi$) bezeichnet das **Auswertungsspiel** zwischen dem *Falsifizierer F* und der *Verifiziererin V*, welche zeigen möchten, ob $\mathfrak{A} \models \varphi$ (Verifiziererin) oder $\mathfrak{A} \not\models \varphi$ (Falsifizierer). Dazu folgende Vorgehensweise für eine Formel $\varphi \in$ FO:

     (a) Definiere Unterformeln $\alpha_i(x_1, \ldots, x_k)$ von φ, welche über die bis dahin quant. Var. $x_1, \ldots, x_k$ sprechen.

     (b) V zieht bei $\exists$ und $\vee$, F bei $\forall$ und $\wedge$ jeweils durch Belegen einer Variablen.

     (c) Die GWS ist die Menge von Kanten, durch deren Wahl einer der Spieler gewinnen würde (markieren im Spielgraphen).

     (d) Die Gewinnregion ist die Menge von Knoten, von welchen der Spieler eine Gewinnstrategie hat.

     (e) Das Auswertungsspiel ist immer endlich, also stets fundiert und determiniert.

   - Seien $\mathcal{K}, \mathcal{K}'$ Kripkestrukturen. $\mathcal{K}, \mathcal{K}'$ sind ausgehend von (v, w), $v \in V, w \in V'$ durch Formel $\varphi \in$ ML nicht unterscheidbar $\Leftrightarrow \mathcal{K}, v \sim \mathcal{K}', w$ ($(\mathcal{K}, v)$ und $(\mathcal{K}', w)$ sind bisimilar). Spieltheorethisch: $\mathcal{K}, v \sim \mathcal{K}', w$ $\Leftrightarrow$ Spielerin II gewinnt das **Bisimulationsspiel** von (v, w) aus. Ein Polynomzeit-Algorithmus, der zu der Kripkestruktur $\mathcal{K} = (V, (E_a)_{a \in A}, (P_i)_{i \in I})$ alle Paare (v, w) mit $\mathcal{K}, v \sim \mathcal{K}, w$ berechnet lautet wie folgt:

     (a) Setze $\sim_0 := \{(v, w) \mid \forall i v \in P_i \Leftrightarrow w \in P_i\}$, berechne $[v]_0 := \{w \mid v \sim_0 w\}$.

     (b) Für $i = 0$ bis $|V|$:

       i. Setze $\sim_{i+1} := \{(v, w) \mid v \sim_i w$ und für alle $a \in A$ und die $\sim_i$ -Klasse $[v]_i :$ es ex. $z \in [v]_i$ mit $v \xrightarrow{a} z \Leftrightarrow$ es ex. $z' \in [w]_i$ mit $w \xrightarrow{a} z'\}$.

       ii. Falls $\sim_i = \sim_{i+1}$, gebe $\sim_i$ aus, sonst berechne die Klassen $[v]_{i+1}$ für alle $v \in V$. (D.h., ein Knoten w kommt in die Klasse $[v]_{i+1}$, falls er die gleichen Kanten zu der Ursprungsklasse $[v]_i$ hat, wie v, nicht zu anderen Klassen.)

     (Notiere die $[v]_i$ Schrittweise als Mengen und beschrifte sie mit deren Kantenrelationen.)

     Sind zwei verschiedene Kripkestrukturen zu betrachten, so führe den Algorithmus auf jeder dieser Strukturen aus. Seien die $\sim$-Klassen die (in beiden Strukturen gleichwertig sortierten) Mengen $A_1, \ldots, A_k$ in $\mathcal{K}$ und $B_1, \ldots, B_k$ in $\mathcal{K}'$, dann ist $\sim = \{(v, w) \mid v \in A_i, w \in B_i$ für $i = 1, \ldots, k\}$.

Für die Angabe trennender ML-Formeln für alle Knotenpaare (u, v), trage die Knoten gegeneinander tabellarisch auf. Es genügt, die Formeln über der Diagonalen anzugeben. Die minimale Modaltife ist $i = \min\{\mathrm{md}(\varphi) \mid \varphi \text{ trennt Knoten } u, v\}$, wobei u, v in $\sim_i$ in versch. Klassen liegen in $\sim_{i-1}$ aber nicht.

- Seien $\mathfrak{A}, \mathfrak{B}$ relationale τ-Strukturen. $\mathfrak{A}$ und $\mathfrak{B}$ sind durch einen τ-Satz nicht unterscheidbar ($\mathfrak{A} \models \varphi \Leftrightarrow \mathfrak{B} \models \varphi$), wenn $\mathfrak{A} \equiv \mathfrak{B}$ ($\mathfrak{A}$ und $\mathfrak{B}$ *elementar-äquivalent*). $\mathfrak{A}$ und $\mathfrak{B}$ sind *m-äquivalent* ($\mathfrak{A} \equiv_m \mathfrak{B}$), wenn für alle τ-Sätze ψ mit $\mathrm{qr}(\psi) \leq m$ gilt: $\mathfrak{A} \models \psi \Leftrightarrow \mathfrak{B} \models \psi$.

  Analog lautet die spieltheoretische Formulierung über das **Ehrenfeucht-Fraïssï¿½Spiel** (E-F-Spiel): Die *Dublikatorin* versucht den Zug des *Herausforderers*, der ein Element aus einer Struktur gezogen hat, in der anderen Struktur zu kopieren, d.h., sie zieht so, dass ein *lokaler Isomorphismus* zwischen den bisher gewählten Elementen besteht. Es gilt:

  (a) $\mathfrak{A} \equiv \mathfrak{B} \Leftrightarrow$ Dublikatorin gewinnt das E-F-Spiel $G(\mathfrak{A}, \mathfrak{B})$.

  (b) Für $m \in \mathbb{N}$: $\mathfrak{A} \equiv_m \mathfrak{B} \Leftrightarrow$ Dublikatorin gewinnt das m-Züge E-F-Spiel $G_m(\mathfrak{A}, \mathfrak{B})$.

9. Zur Überprüfung der **Gültigkeit einer ML-Formel**, gebe man zum einen die Formel an oder zeige an Hand eines Gegenbeispiels mittels zweier bisimilarer Kripkestrukturen, dass die Formel zwar Modell der einen aber nicht Modell von der anderen Struktur ist.

10. Die Syntax und Semantik der **CTL** (computation tree logic) ist nur eine Erweiterung der Aussagekraft von ML durch Definition neuer *Pfadquantoren*. Es werden wie in ML Aussagen über Transitionssysteme ausgehend von einem Knoten gemacht.

    - $\mathrm{EX}\psi :\equiv \Diamond\psi$, $\mathrm{AX}\psi :\equiv \Box\psi$
    - $\mathrm{E}(\psi \mathrm{U} \varphi)$: „es gibt Pfad, auf dem zuerst ψ und dann φ gilt“, $\mathrm{A}(\psi \mathrm{U} \varphi)$: „auf allen Pfaden gilt ψ, bis φ gilt“
    - $\mathrm{F}\psi :\equiv (1\mathrm{U}\psi)$: „irgendwann gilt ψ auf dem Pfad“, $\mathrm{G}\psi :\equiv \neg\mathrm{F}\neg\psi$: „immer gilt ψ auf dem Pfad“
    - außerdem: $\langle a\rangle\psi \mapsto (\langle a\rangle\psi)^*(x) := \exists y(E_a xy \wedge \psi^*(y))$ und $[a]\psi \mapsto ([a]\psi)^*(x) := \forall y(E_a xy \to \psi^*(y))$

11. Sei $\mathcal{K} = (V^{\mathcal{K}}, (E_a^{\mathcal{K}})_{a\in A}, (P_i^{\mathcal{K}})_{i\in I})$ Kripkestruktur. Die **Abwicklung** von $\mathcal{K}$ von v aus ist die Kripkestruktur $\mathcal{T}_{\mathcal{K},v} = (V^{\mathcal{T}}, (E_a^{\mathcal{T}})_{a\in A}, (P_i^{\mathcal{T}})_{i\in I})$, wobei in jeder Pfad $\bar{v} = v_0 a_0 v_1 \ldots v_{m-1} a_{m-1} v_m$ mit $v_0 = v$, $a_i \in A^{\mathcal{K}}$ und $m \in \mathbb{N}$ ($v_i a_i v_{i+1}$ bezeichne die Kante $v_i \xrightarrow{a_i} v_{i+1}$) in $\mathcal{T}_{\mathcal{K},v}$ auftritt und die Knoten $v_i \in V^{\mathcal{K}}$ und a_i-Kanten mehrmals auftreten können, damit keine Zykel entstehen.

    - *Lemma [4.18]:* Sei $\mathcal{K}$ Kripkestruktur. $\mathcal{K}, v \sim \mathcal{T}_{\mathcal{K},v}, v$.
    - Sei Φ eine Formelmenge einer Logik.

      (a) Φ hat die *Endliche-Modell-Eigenschaft* (EME), wenn jedes erfüllbare $\varphi \in \Phi$ ein endliches Modell hat.

      (b) Falls Φ auf Transitionssystemen definiert ist, hat Φ die *(endliche) Baummodell-Eigenschaft* ((E)BME), wenn jede erfüllbare Formel $\varphi \in \Phi$ ein (endliches) Modell hat, welches ein Baum ist.

      – Erfüllbare $\varphi \in \mathrm{ML}$ haben die EBME, wobei $\mathcal{T}, v \models \varphi$ mit Tiefe $\leq \mathrm{md}(\varphi)$ und Verzweigungsgrad $\leq |\varphi|$.

      – CTL-Formeln besitzen die BME aber nicht die EME.

      – FO besitzt weder die EME, noch die BME (im allgemeinen Fall).

12. Eine **Theorie** ist eine erfüllbare Satzmenge $T \subset \mathrm{FO}(\tau)$, die abgeschlossen unter $\models$ ist, d.h., für alle $\psi \in \mathrm{FO}(\tau)$ muss $T \models \psi \Rightarrow \psi \in T$ gelten. Eine Theorie T heißt *vollständig*, wenn für jeden Satz $\psi \in \mathrm{FO}(\tau)$ entweder $\psi \in T$ oder $\neg\psi \in T$ ist. $\mathrm{Th}(\mathfrak{A})$ bezeichnet die Theorie einer τ-Struktur $\mathfrak{A}$ mit $\mathrm{Th}(\mathfrak{A}) = \{\psi \mid \mathfrak{A} \models \psi\}$. Für eine τ-Modellklasse $\mathcal{K}$ ist $\mathrm{Th}(\mathcal{K}) = \bigcap_{\mathfrak{A}\in\mathcal{K}} \mathrm{Th}(\mathfrak{A})$. $\mathrm{Th}(\mathfrak{A})$ und $\mathrm{Th}(\mathcal{K})$ sind vollständig und abgeschlossen unter $\models$.

    - *Satz [5.12]:* Eine Theorie ist vollständig genau dann, wenn alle ihre Modelle elementar äquivalent sind.
    - Beispiel: Die *Arithmetik* ist die Theorie $\mathrm{Th}(\mathfrak{N})$ der Struktur $\mathfrak{N} = (\mathbb{N}, +, \cdot, 0, 1)$ mit $\{+, \cdot, 0, 1\} =: \tau_{\mathrm{ar}}$.

13. Eine Strukturklasse $\mathcal{C} \subseteq \mathrm{Str}(\tau)$ ist **FO-axiomatisierbar**, wenn ein Axiomensystem $\Phi \subseteq \mathrm{FO}(\tau)$ existiert, so dass $\mathcal{C} = \mathrm{Mod}(\Phi) = \{\text{Strukturen } \mathfrak{A} \mid \mathfrak{A} \models \Phi\}$ *Modellklasse* von Φ. Ist $\Phi = \{\varphi_1, \ldots, \varphi_n\}$ endlich, so axiomatisiert der Satz $\bigwedge_{i\in[1,n]} \varphi_i$ gerade $\mathcal{C}$ dann heißt $\mathcal{C}$ *endlich* (oder *elementar*) *axiomatisierbar.*

    (a) **endliche** Axiomensysteme:

    - Verschiedene Ordnungen lassen sich mit den Sätzen (1) bis (6) unter Punkt 4 endlich axiomatisieren.
    - ungerichtete Graphen (V, E): $\Phi_{\mathrm{Graph}} = \{\forall x \neg Exx,\ \forall x \forall y (Exy \to Eyx)\}$.
    - Gruppen $(G, \circ, e, ^{-1})$: $\Phi_{\mathrm{Gruppe}} = \{\forall x \forall y \forall z (x \circ (y \circ z) = (x \circ y) \circ z),\ \forall x (x \circ e = x),\ \forall x (x \circ x^{-1} = e)\}$.

- Für $n \in \mathbb{N}$ sei $\mathcal{K}_{\geq n}$ die Klasse der Strukturen mit $\geq n$-elementigem Universum. Für $n \geq 2$ ist $\mathcal{K}_{\geq n}$ axiomatisiert durch den Satz $\varphi_{\geq n} = \exists x_1 \dots \exists x_n \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j$.
- Sei $\psi_{\text{Körper}}$ Satz, der die Körperaxiome der Körper $(K, +, \cdot, 0, 1)$ axiomatisiert, $\chi_p = 1 + \dots + 1 (= p \cdot 1)$ für p Primzahl dann axiomatisiert $\Phi_{\text{char}(p)} = \{\psi_{\text{Körper}}\} \cup \{\chi_p\}$ die Körper mit Charakteristik p.

(b) **unendliche** Axiomensysteme:

- Klasse $\mathcal{K}_\infty$ aller unendlicher τ-Strukturen: $\Phi_\infty = \{\varphi_{\geq n} \mid n \in \mathbb{N}\}$ ($\mathcal{K}_{\geq n}$, $\varphi_{\geq n}$ siehe oben).
- $\Phi_{\text{char}(0)} = \{\psi_{\text{Körper}}\} \cup \{\neg\chi_p \mid p \text{ Primzahl}\}$ die Körper mit Charakteristik 0.

(c) Zeige: „τ-Strukturklasse ist **nicht endlich** axiomatisierbar" durch Angabe einer GWS für den Herausforderer im E-F-Spiel oder mittels der folgenden Sätze:

- *Kompaktheitssatz:* Für jede Menge $\Phi \subseteq \text{FO}(\tau)$ und jedes $\psi \in \text{FO}(\tau)$
  i. $\Phi \models \psi \Leftrightarrow$ ex. eine endliche Teilmenge $\Phi_0 \subseteq \Phi$, so dass $\Phi_0 \models \psi$.
  ii. Φ ist erfüllbar $\Leftrightarrow$ jede endliche Teilmenge von Φ ist erfüllbar.
- *Satz [6.14]:* $\Phi_{\text{char}(0)}$ ist nicht endlich axiomatisierbar.
- *Satz [6.15]:* Sei $\Phi \subseteq \text{FO}(\tau)$ Satzmenge mit bel. großen endl. Modellen $\Rightarrow$ Φ hat unendliches Modell.
- Ein *Nichtstandardmodell* der *Arithmetik* $\text{Th}(\mathfrak{N})$ ist eine τ_{ar}-Struktur $\mathfrak{A}$ mit $\mathfrak{A} \equiv \mathfrak{N}$ aber $\mathfrak{A} \not\cong \mathfrak{N}$. *Satz [6.21]:* Es gibt ein abzählbares Nichtstandardmodell der Arithmetik.

(d) Zeige: „τ-Strukturklasse ist **nicht** axiomatisierbar" mittels folgender Sätze:

- Zunächst stehen auch hier die oben genannten Sätze insbes. der Kompaktheitssatz zur Verfügung.
- *Satz [6.12]:* Jede erfüllbare, abzählbare Satzmenge hat ein abzählbares Modell.
- *Satz [6.16]:* Die Klasse aller endlichen τ-Strukturen ist nicht axiomatisierbar.
- *Satz [6.18] (Aufsteigender Löwenheim-Skolem):* Φ besitze ein unendliches Modell. Dann gibt es zu jeder Menge M eine Struktur $\mathfrak{D}$ mit $|D| \geq |M|$, die Modell $\mathfrak{D} \models \Phi$ ist.
- *Lemma [6.19]:* $\{\mathfrak{B} \mid \mathfrak{A} \equiv \mathfrak{B}\}$ ist die kleinste Modellklasse, die $\mathfrak{A}$ enthält.
- (!) *Satz [6.20]:* Sei $\mathfrak{A}$ unendliche Struktur. Dann gibt es Struktur $\mathfrak{B}$ mit $\mathfrak{B} \equiv \mathfrak{A}$ aber $\mathfrak{B} \not\cong \mathfrak{A}$. (!) Insbesondere: Die Isomorphieklasse $\{\mathfrak{B} \mid \mathfrak{A} \cong \mathfrak{B}\}$ von $\mathfrak{A}$ ist *nicht* FO-axiomatisierbar.

14. Eine n-stellige Relation ist in einer festen τ-Struktur **FO-definierbar**, wenn es eine Formel $\psi(x_1, \dots, x_n) \in \text{FO}(\tau)$ gibt mit $\psi^{\mathfrak{A}} := \{(a_1, \dots, a_n) \mid \mathfrak{A} \models \psi(a_1, \dots, a_n)\} \subseteq A^n$. Eine n-stellige Funktion $f : A^n \to A$ ist definierbar, wenn der Graph G_f definierbar ist.

(a) einige **definierbare Relationen**:

- $<$ in $(\mathbb{R}, +, \cdot, 0, 1)$: $\varphi_<(x, y) := \exists z(z \neq 0 \land x + z \cdot z = y)$.
- die Nachfolgerfunktion $z \mapsto z + 1$ in $(\mathbb{Z}, <)$: $\varphi_{\text{suc}}(x, y) := x < y \land \forall z(x < z \land y \neq z \to y < z)$.
- jedes n in $(\mathbb{N}, +, 0, 1)$: $\varphi_n(x) := 1 + \dots + 1 (= n \cdot 1)$ für $n \geq 1$.
- in $(\mathbb{N}, \cdot)$:
  - Nullelement: $\varphi_0(x) := \forall y(x \cdot y = x) =: 0$.
  - Einselement: $\varphi_0(x) := \forall y(x \cdot y = y) =: 1$.
  - Teilbarkeit: $\varphi_0(x, y) := \exists z(x \cdot z = y) =: x \mid y$.
  - Primzahl: $\varphi_{\text{prim}}(x) := \forall z(z \nmid x \lor z = x \lor z = 1)$.
- $\leq$-Relation in $(\mathbb{N}, +)$: $\varphi_\leq(x, y) := \exists z(x + z = y)$.
- $\leq$-Relation in $(\mathbb{R}, +, \cdot)$: $\varphi_\leq(x, y) := \exists z(x + (z \cdot z) = y)$.

(b) Zeige „Relation R ist **nicht FO-definierbar** in $\mathfrak{A} \in \text{Str}(\tau)$" mittels der folgenden Lemmata:

i. *Lemma [5.3]:* Sei $\mathfrak{A}$ eine σ-Struktur und $\mathfrak{B}$ eine σ-Expansion von $\mathfrak{A}$ durch Hinzufügen beliebig vieler, in $\mathfrak{A}$ definierbaren Relationen und Funktionen.
Dann ist jede in $\mathfrak{B}$ definierbare Relation oder Funktion bereits in $\mathfrak{A}$ definiert.
ii. *Lemma [5.5]:* Sei $\mathfrak{A}$ τ-Struktur $\alpha \in \text{Aut}(\mathfrak{A})$ und $\psi \in \text{FO}(\tau)$ dann ist α auch ein Automorphismus der Expansion $(A, \psi^{\mathfrak{A}})$.

Anwendung: Ang. es ex. Formel $\psi \in \text{FO}(\tau)$ mit $\psi^{\mathfrak{A}} = R$. Finde $\alpha \in \text{Aut}(\mathfrak{A})$ mit $\alpha(\bar{x}) \notin R$ aber $\bar{x} \in R$.

15. Die **Entscheidbarkeit** einer Logik ist äquivalent formulierbar als *Erfüllbarkeit*, *Gültigkeit* oder *Beweisbarkeit*.

- ML und CTL sind (sogar effizient) entscheidbar. AL ist zwar entscheidbar, das Problem ist jedoch NP-vollständig.
- Nicht entscheidbar ist hingegen FO.