

# ENDLICHE MODELLETHEORIE

STEFAN GESCHKE

## 1. ERSTSTUFIGE LOGIK UND ENDLICHE STRUKTUREN

**1.1. Strukturen.** Ein **Vokabular**  $\tau$  ist eine endliche Menge bestehend aus Relationssymbolen  $P, Q, R, \dots$ , Funktionssymbolen  $f, g, h, \dots$  und Konstantensymbolen  $c, d, \dots$ . Jedes Relations- und Funktionssymbol trägt eine natürliche Zahl  $\geq 1$ , seine **Stelligkeit**.

Fixiere ein Vokabular  $\tau$ . Eine **Struktur**  $\mathcal{A}$  für  $\tau$  (eine  $\tau$ -**Struktur**) ist eine Menge  $A$  zusammen mit

- (S1) Relationen  $R^{\mathcal{A}} \subseteq A^n$  für jedes  $n$ -stellige Relationssymbol  $R \in \tau$ ,
- (S2) Funktionen  $f^{\mathcal{A}} : A^m \rightarrow A$  für jedes  $m$ -stellige Funktionssymbol  $f \in \tau$  und
- (S3) Konstanten  $c^{\mathcal{A}} \in A$  für jedes Konstantensymbol  $c \in \tau$ .

Oft identifiziert man eine Struktur  $\mathcal{A}$  mit ihrer unterliegenden Menge  $A$ , schreibt also  $A$  anstatt  $\mathcal{A}$ . Das ist übliche Praxis in der Algebra, wo man etwa von einer Gruppe  $G$  spricht, wenn eigentlich eine Struktur  $(G, \cdot)$  (oder auch  $(G, \cdot, 1, {}^{-1})$ ) gemeint ist, aber weniger üblich in der Graphentheorie, wo man gerne einem Graphen  $G = (V, E)$  betrachtet.

Außerdem werden wir manchmal die Interpretation  $R^{\mathcal{A}}$ ,  $f^{\mathcal{A}}$  oder  $c^{\mathcal{A}}$  eines Symbols  $R$ ,  $f$  oder  $c$  ebenfalls mit  $R$ ,  $f$  oder  $c$  bezeichnen.

Eine  $\tau$ -Struktur  $\mathcal{B}$  heißt **Unterstruktur** von  $\mathcal{A}$ , falls

- (U1) die  $\mathcal{B}$  unterliegende Menge  $B$  eine Teilmenge von  $A$  ist,
- (U2) jede Relation  $R^{\mathcal{B}}$  Einschränkung von  $R^{\mathcal{A}}$  auf  $B$  ist,
- (U3) jede Funktion  $f^{\mathcal{B}}$  die Einschränkung von  $f^{\mathcal{A}}$  auf  $B$  ist und
- (U4) jede Konstante  $c^{\mathcal{B}}$  mit  $c^{\mathcal{A}}$  übereinstimmt.

Beachte, dass (U2) impliziert, dass  $B$  unter allen Funktionen  $f^{\mathcal{A}}$  abgeschlossen ist. Analog folgt aus (U3), dass alle Konstanten  $c^{\mathcal{A}}$  Elemente von  $B$  sind.

Zwei  $\tau$ -Strukturen  $\mathcal{A}$  und  $\mathcal{B}$  sind **isomorph**, wenn eine Bijektion  $i : A \rightarrow B$  existiert, so dass

- (I1) für jedes  $n$ -stellige Relationssymbol  $R \in \tau$  und alle  $a_1, \dots, a_n \in A$

$$(a_1, \dots, a_n) \in R^{\mathcal{A}} \Leftrightarrow (i(a_1), \dots, i(a_n)) \in R^{\mathcal{B}}$$

gilt,

- (I2) für jedes  $n$ -stellige Funktionssymbol  $f \in \tau$  und alle  $a_1, \dots, a_n \in A$

$$i(f^{\mathcal{A}}(a_1, \dots, a_n)) = f^{\mathcal{B}}(i(a_1), \dots, i(a_n))$$

gilt und

- (I3) für jedes Konstantensymbol  $c \in \tau$

$$i(c^{\mathcal{A}}) = c^{\mathcal{B}}$$

gilt.

**1.2. Formeln.** Eine **erststufige Formel** über  $\tau$  ist eine Zeichenkette über dem Alphabet

$$\{\exists, \vee, \neg, =, (, )\} \cup \tau \cup \text{Var},$$

wobei  $\text{Var}$  die unendliche Menge der Variablen ist. Wir setzen implizit voraus, dass die Mengen  $\{\exists, \vee, \neg, =, (, )\}$ ,  $\tau$  und  $\text{Var}$  paarweise disjunkt sind. Variablen werden typischer Weise mit  $x, y, z, \dots$  bezeichnet. Bevor wir genauer definieren, was Formeln sind, definieren wir **Terme**.

Ein Term über  $\tau$  ist eine Zeichenkette, die sich durch endlich viele Anwendungen folgender Regeln gewinnen lässt:

- (T1) Alle Konstantensymbole in  $\tau$  und alle Variablen sind Terme.
- (T2) Sind  $t_1, \dots, t_n$  Terme und ist  $f \in \tau$  ein  $n$ -stelliges Funktionssymbol, so ist  $f(t_1, \dots, t_n)$  ein Term.

Eine erststufige Formel über  $\tau$  ist eine Zeichenkette, die sich durch endlich viele Anwendungen folgender Regeln gewinnen lässt:

- (F1) Sind  $t_1$  und  $t_2$  Terme über  $\tau$ , so ist  $(t_1 = t_2)$  eine Formel.
- (F2) Ist  $R \in \tau$  ein  $n$ -stelliges Relationssymbol und sind  $t_1, \dots, t_n$  Terme über  $\tau$ , so ist  $R(t_1, \dots, t_n)$  eine Formel.
- (F3) Ist  $\varphi$  eine Formel, so auch  $\neg\varphi$ .
- (F4) Sind  $\varphi$  und  $\psi$  Formeln, so ist auch  $(\varphi \vee \psi)$  eine Formel.
- (F5) Ist  $\varphi$  eine Formel und  $x$  eine Variable, so ist  $\exists x\varphi$  eine Formel.

Sind  $\varphi$  und  $\psi$  Formeln, so benutzen wir  $(\varphi \wedge \psi)$ ,  $(\varphi \rightarrow \psi)$ ,  $(\varphi \leftrightarrow \psi)$  bzw.  $\forall x\varphi$  als Abkürzungen für  $\neg(\neg\varphi \vee \neg\psi)$ ,  $(\neg\varphi \vee \psi)$ ,  $\neg(\neg(\neg\varphi \vee \psi) \vee \neg(\varphi \vee \neg\psi))$  bzw.  $\neg\exists x\neg\varphi$ . Außerdem werden Klammern weggelassen, solange das die Lesbarkeit nicht stört.

Eine Variable  $x$  kommt in einer Formel  $\varphi$  **frei** vor, wenn  $x$  in  $\varphi$  außerhalb des Einflussbereiches eines Quantors  $\exists x$  oder  $\forall x$  vorkommt. Eine Formel ohne freie Variablen ist eine **Aussage**.

Wir benutzen die Notation  $\varphi(x_1, \dots, x_n)$  um anzudeuten, dass  $x_1, \dots, x_n$  paarweise verschiedene Variablen sind und alle freien Variablen von  $\varphi$  unter den Variablen  $x_1, \dots, x_n$  sind. Analog schreiben wir für einen Term  $t(x_1, \dots, x_n)$  um anzudeuten, dass die  $x_i$  paarweise verschieden sind und alle in  $t$  vorkommenden Variablen unter den  $x_i$  sind.

**1.3. Semantik.** Fixiere eine  $\tau$ -Struktur  $\mathcal{A} = (A, \dots)$ . Für einen  $\tau$ -Term  $t(x_1, \dots, x_n)$  und  $a_1, \dots, a_n \in A$  definiert man  $t(a_1, \dots, a_n)$  (oder genauer,  $t^{\mathcal{A}}(a_1, \dots, a_n)$ ) wie folgt:

- (TA1)  $x_i(a_1, \dots, a_n) := a_i$
- (TA2) Ist  $c \in \tau$  ein Konstantensymbol, so sei  $c(a_1, \dots, a_n) := c^{\mathcal{A}}$ .
- (TA3) Ist  $f \in \tau$  ein  $m$ -stelliges Funktionssymbol und sind  $t_1(x_1, \dots, x_n), \dots, t_m(x_1, \dots, x_n)$  Terme, so sei

$$f(t_1, \dots, t_m)(a_1, \dots, a_n) := f^{\mathcal{A}}(t_1(a_1, \dots, a_n), \dots, t_m(a_1, \dots, a_n)).$$

Schließlich definieren wir für jede Formel  $\varphi(x_1, \dots, x_n)$  und alle  $a_1, \dots, a_n \in A$  die **Gültigkeit** von  $\varphi(a_1, \dots, a_n)$  in  $\mathcal{A}$ :

- (FG1) Für Terme  $t_1(x_1, \dots, x_n)$  und  $t_2(x_1, \dots, x_n)$  gilt  $(t_1 = t_2)(a_1, \dots, a_n)$  genau dann in  $\mathcal{A}$ , wenn  $t_1(a_1, \dots, a_n) = t_2(a_1, \dots, a_n)$  ist.
- (FG2) Für Terme  $t_1(x_1, \dots, x_n), \dots, t_m(x_1, \dots, x_n)$  und ein  $m$ -stelliges Relationssymbol  $R$  gilt  $R(t_1, \dots, t_m)(a_1, \dots, a_n)$  genau dann in  $\mathcal{A}$ , wenn

$$(t_1(a_1, \dots, a_n), \dots, t_m(a_1, \dots, a_n)) \in R^{\mathcal{A}}$$

ist.

- (FG3) Für Formeln  $\varphi(x_1, \dots, x_n)$  und  $\psi(x_1, \dots, x_n)$  gilt  $(\varphi \vee \psi)(a_1, \dots, a_n)$  genau dann in  $\mathcal{A}$ , wenn  $\varphi(a_1, \dots, a_n)$  oder  $\psi(a_1, \dots, a_n)$  in  $\mathcal{A}$  gilt.

(FG4) Für eine Formel  $\varphi(x_1, \dots, x_n)$  gilt  $\neg\varphi(a_1, \dots, a_n)$  genau dann in  $\mathcal{A}$ , wenn  $\varphi(a_1, \dots, a_n)$  nicht in  $\mathcal{A}$  gilt.

(FG5) Für eine Formel  $\varphi(x, x_1, \dots, x_n)$  gilt  $\exists x\varphi(a_1, \dots, a_n)$  genau dann in  $\mathcal{A}$ , wenn es ein  $a \in A$  gibt, so dass  $\varphi(a, a_1, \dots, a_n)$  in  $\mathcal{A}$  gilt.

Wenn  $\varphi(a_1, \dots, a_n)$  in  $\mathcal{A}$  gilt, so schreiben wir  $\mathcal{A} \models \varphi(a_1, \dots, a_n)$ .

Die Gültigkeitsrelation lässt sich auch für unendliche Formelmengen leicht definieren. Sei  $a : \text{Var} \rightarrow A$  eine beliebige Abbildung, eine **Belegung** der Variablen mit Elementen von  $A$ . Weiter sei  $\Phi$  eine Menge von Formeln über  $\tau$ . Dann gilt  $\Phi$  genau dann in  $\mathcal{A}$  unter der Belegung  $a$ , wenn für jede Formel  $\varphi(x_1, \dots, x_n) \in \Phi$  gilt:

$$\mathcal{A} \models \varphi(a(x_1), \dots, a(x_n))$$

In diesem Falle schreibt man  $\mathcal{A} \models \Phi[a]$ . Gilt  $\Phi$  in  $\mathcal{A}$  unter jeder Belegung, so schreibt man  $\mathcal{A} \models \Phi$ .

Man beachte, dass die Gültigkeit einer Menge von Aussagen in  $\mathcal{A}$  unabhängig von der Belegung ist. Ist  $i : A \rightarrow B$  ein Isomorphismus zwischen den  $\tau$ -Strukturen  $\mathcal{A}$  und  $\mathcal{B}$ , so induziert jede Belegung  $a : \text{Var} \rightarrow A$  eine Belegung  $b := i \circ a : \text{Var} \rightarrow B$ , so dass für jede Menge  $\Phi$  von Formeln gilt:

$$\mathcal{A} \models \Phi[a] \Leftrightarrow \mathcal{B} \models \Phi[b]$$

Insbesondere erfüllen isomorphe Strukturen dieselben Aussagen.

Das Symbol  $\models$  wird auch für die **semantische Konsequenzrelation** benutzt. Seien  $\Phi$  und  $\Psi$  Mengen von Formeln über  $\tau$ . Dann **folgt**  $\Psi$  aus  $\Phi$ , wenn für alle  $\tau$ -Strukturen  $\mathcal{A}$  und alle Belegungen  $b$  gilt:

$$\mathcal{A} \models \Phi[b] \Rightarrow \mathcal{A} \models \Psi[b]$$

In diesem Falle schreibt man  $\Phi \models \Psi$ .

Auf beiden Seiten von  $\models$  dürfen auch einzelne Formeln stehen. Die Bedeutung ist die naheliegende.

**1.4. Klassische Sätze der erststufigen Logik und endliche Strukturen.** Wir fixieren wieder ein (endliches) Vokabular  $\tau$ . Im Folgenden sind alle Formeln Formeln über  $\tau$  und alle Strukturen  $\tau$ -Strukturen. Eine der wesentlichen Stärken der erststufigen Logik ist, dass sich die Relation  $\models$  zwischen Formelmengen auch rein syntaktisch definieren lässt. Genauer, mit Hilfe eines geeigneten Kalküls führt man eine (formale) Ableitbarkeitsrelation  $\vdash$  zwischen Formelmengen ein. Eine Formel  $\psi$  ist aus einer Formelmenge  $\Phi$  ableitbar, wenn  $\psi$  aus  $\Phi$  durch Anwendung gewisser syntaktischer Regeln hervorgeht (durch “Symbolgeschiebe”).

Den Zusammenhang zwischen  $\models$  und  $\vdash$  stellt der **Vollständigkeitsatz** her:

**Satz 1.1.** *Für Formelmengen  $\Phi$  und  $\Psi$  gilt  $\Phi \models \Psi$  genau dann, wenn  $\Phi \vdash \Psi$  gilt.*

Man kann den Vollständigkeitsatz auch etwas anders formulieren. Eine Struktur  $A$  zusammen mit einer Belegung  $a$  der Variablen mit Elementen von  $A$  ist **Modell** einer Formelmenge  $\Phi$ , wenn  $A \models \Phi[a]$  gilt. Eine Struktur  $A$  ist Modell von  $\Phi$ , wenn  $A$  zusammen mit jeder Belegung der Variablen mit Elementen von  $A$  Modell von  $\Phi$  ist.  $\Phi$  ist **erfüllbar**, wenn  $\Phi$  ein Modell hat. Eine Formelmenge  $\Phi$  ist **widerspruchsfrei**, wenn sich aus  $\Phi$  nicht jede Formel (insbesondere kein Widerspruch) ableiten lässt.

**Satz 1.2.** *Eine Formelmenge  $\Phi$  ist genau dann widerspruchsfrei, wenn  $\Phi$  erfüllbar ist.*

Beweist man den Vollständigkeitsatz in dieser Form, so erhält man üblicher Weise automatisch den **Satz von Löwenheim-Skolem**:

**Satz 1.3.** *Ist  $\Phi$  erfüllbar, so hat  $\Phi$  ein abzählbares Modell.*

Man beachte dabei, dass auch endliche Strukturen abzählbar sind.

Formales Ableiten kann man leicht einem Computer beibringen. Insbesondere gibt es einen Algorithmus, der allen wahren Aussagen (über einem festen Vokabular) aufzählt. Dabei ist eine Aussagen **wahr**, wenn sie aus der leeren Menge folgt.

**Satz 1.4.** *Die Menge der wahren Aussagen ist rekursiv aufzählbar.*

Da die Ableitung einer Formel  $\psi$  aus einer Formelmenge  $\Phi$  endliche Länge hat und damit nur endlich viele Formeln aus  $\Phi$  benutzt, folgt aus dem Vollständigkeitsatz der **Kompaktheitssatz**:

**Satz 1.5.** *Sei  $\Phi$  eine Formelmenge,  $\psi$  eine Formel. Gilt  $\Phi \models \psi$ , so hat  $\Phi$  eine endliche Teilmenge  $\Phi_0$ , so dass bereits  $\Phi_0 \models \psi$  gilt.*

*Insbesondere ist eine Formelmenge  $\Phi$  genau dann erfüllbar, wenn jede endliche Teilmenge von  $\Phi$  erfüllbar ist.*

Was passiert, wenn man sich in der Definition von  $\models$  auf endliche Strukturen beschränkt? Für zwei Formelmengen  $\Phi$  und  $\Psi$  sei  $\Phi \models_{\text{endlich}} \Psi$  genau dann, wenn für jede endliche Struktur  $A$  und jede Belegung  $a$  der Variablen mit Elementen von  $A$  gilt:

$$A \models \Phi[a] \Rightarrow A \models \Psi[a]$$

Wie üblich dürfen auch einzelne Formeln auf beiden Seiten von  $\models_{\text{endlich}}$  stehen.

Die Relation  $\models_{\text{endlich}}$  verhält sich deutlich schlechter als  $\models$ . Zum Beispiel lässt sich kein Kalkül angeben, mit dem man  $\models_{\text{endlich}}$  auf syntaktische Weise beschreiben kann. Das folgt aus

**Satz 1.6** (Trahtenbrot). *Falls  $\tau$  mindestens ein zweistelliges Relationssymbol enthält, so ist die Menge der Aussagen über  $\tau$ , die für alle endlichen  $\tau$ -Strukturen gelten, nicht rekursiv aufzählbar.*

Wir werden den Satz von Trahtenbrot später beweisen.

Auch der Kompaktheitssatz (Satz 1.5) scheitert im endlichen. Betrachte nämlich für jedes  $n > 0$  die Aussage

$$\varphi_{\geq n} := \exists x_0 \dots \exists x_n \text{ " } x_1, \dots, x_n \text{ sind paarweise verschieden"}$$

Dann hat jede endliche Teilmenge der Menge  $\Phi := \{\phi_n : n > 0\}$  ein endliches Modell, die gesamte Menge  $\Phi$  jedoch nicht.

**1.5. Modellklassen.** Wir fixieren wieder ein Vokabular  $\tau$ . Für eine Menge von Sätzen  $\Phi$  über  $\tau$  sei

$$\text{Mod}(\Phi) := \{A : A \text{ ist endliche } \tau\text{-Struktur mit } A \models \Phi\}$$

die **Modellklasse** von  $\Phi$ .

Man beachte, dass Modellklassen unter Isomorphie abgeschlossen sind. Im Folgenden werden wir stillschweigend voraussetzen, dass alle betrachteten Klassen von Strukturen unter Isomorphie abgeschlossen sind, d.h., für jede Klasse  $K$  von Strukturen, alle  $A \in K$  und alle Strukturen  $B$  mit  $A \cong B$  nehmen wir  $B \in K$  an.

Für jede endliche  $\tau$ -Struktur  $A$  ist die Klasse der zu  $A$  isomorphen  $\tau$ -Strukturen Modellklasse einer einzelnen Formel  $\varphi_A$  über  $\tau$ . Außerdem kann man leicht für jede natürliche Zahl  $n$  eine Formel  $\varphi_{=n}$  hinschreiben, deren Modellklasse die die Klasse der  $\tau$ -Strukturen mit genau  $n$  Elementen ist.

**Satz 1.7.** *Jede Klasse  $K$  von endlichen  $\tau$ -Strukturen ist Modellklasse einer Menge  $\Phi$  von Aussagen über  $\tau$ .*

*Beweis.* Wir haben vorausgesetzt, dass  $K$  unter Isomorphie abgeschlossen ist. Man beachte, dass es für jedes  $n$  bis auf Isomorphie nur endlich viele  $\tau$ -Strukturen der Mächtigkeit  $n$  gibt. Damit existiert eine Formel  $\psi_n$ , die besagt, dass eine  $\tau$ -Struktur  $A$  eine der endlich vielen (bis auf Isomorphie) Strukturen in  $K$  mit Mächtigkeit  $n$  ist, falls  $A$  selbst  $n$  Elemente hat.  $K$  ist die Modellklasse von  $\Phi := \{\psi_n : n \in \mathbb{N}\}$ .  $\square$

## 2. EHRENFUCHT-FRAISSE-SPIELE

Die wichtigste Methode, um zu zeigen, dass sich gewisse Klassen endlicher Strukturen nicht einfach beschreiben lassen, sind die sogenannten Ehrenfeucht-Fraisse-Spiele.

Wir beschränken uns auf Vokabulare ohne Funktionssymbole. Man beachte, dass sich jede  $n$ -stellige Funktion als  $n + 1$ -stellige Relation auffassen lässt. Allerdings macht es einen Unterschied, ob man eine Funktion als Funktion realisiert oder als Relation, wenn man Substrukturen betrachtet. Substrukturen sind unter den Funktionen auf der Struktur abgeschlossen, nicht jedoch unter Funktionen, die wir als Relationen realisiert haben.

**2.1. Elementare Klassen.** Wir nennen eine Klasse  $K$  von endlichen Strukturen **erststufig axiomatisierbar** oder **elementar**, wenn  $K$  die Modellklasse einer einzelnen erststufigen Aussage  $\varphi$  ist.

Um für eine gegebene Klasse  $K$  endlicher Strukturen zu zeigen, dass  $K$  nicht elementar ist, muss man für jede Aussage  $\varphi$  über dem entsprechenden Vokabular zeigen, dass  $K \neq \text{Mod}(\varphi)$  ist. Dazu ist es nützlich, den **Quantorenrang** einer Formel einzuführen.

Formeln, die keine Quantoren enthalten, haben den Quantorenrang 0. Der Quantorenrang von  $\varphi \vee \psi$  ist das Maximum der Quantorenräge von  $\varphi$  und  $\psi$ . Der Quantorenrang von  $\neg\varphi$  ist einfach der Quantorenrang von  $\varphi$ . Der Quantorenrang von  $\exists x\varphi$  ist um eins größer als der Quantorenrang von  $\varphi$ .

Zwei Strukturen  $A$  und  $B$  sind  **$m$ -äquivalent**, falls  $A$  und  $B$  dieselben erststufigen Aussagen vom Quantorenrang  $\leq m$  erfüllen. In diesem Falle schreiben wir  $A \equiv_m B$ .

Das Standardverfahren, die Nichtelementarität einer gegebenen Klasse endlicher Strukturen zu zeigen, liefert

**Lemma 2.1.** *Sei  $K$  eine Klasse endlicher Strukturen. Angenommen, für jedes  $m \in \mathbb{N}$  existieren endliche Strukturen  $A$  und  $B$  mit  $A \in K$ ,  $B \notin K$  und  $A \equiv_m B$ . Dann ist  $K$  nicht erststufig axiomatisierbar.*

*Beweis.* Sei  $\varphi$  eine erststufige Aussage und  $m$  der Quantorenrang von  $\varphi$ . Angenommen,  $K = \text{Mod}(\varphi)$ . Sei  $A \in K$  und  $B \notin K$  mit  $A \equiv_m B$ . Wegen  $A \models \varphi$  gilt auch  $B \models \varphi$ . Also ist  $B \in \text{Mod}(\varphi)$ . Wegen  $B \notin K$  ist  $K \neq \text{Mod}(\varphi)$ , ein Widerspruch.  $\square$

Wie wir später sehen werden, gilt auch die Umkehrung dieses Lemmas.

**2.2. Der Satz von Ehrenfeucht.** Intuitiv sind zwei Strukturen  $A$  und  $B$   $m$ -äquivalent, wenn sie "lokal" gleich aussehen, wobei die genaue Bedeutung von "lokal" von  $m$  abhängt.

*Partielle Isomorphismen.* Sei  $p$  eine Abbildung von einer Teilmenge von  $A$  in eine Teilmenge von  $B$ . Wir schreiben  $\text{dom}(p)$  für den Definitionsbereich von  $p$  und  $\text{ran}(p)$  für das Bild von  $p$ . Die Abbildung  $p$  ist ein **partieller Isomorphismus**, falls gilt:

(PI1)  $p$  ist injektiv.

(PI2) Für alle Konstantensymbole  $c$  ist  $c^A \in \text{dom}(p)$  und  $p(c^A) = c^B$ .

(PI3) Für jedes  $n$ -stellige Relationssymbol  $R$  und alle  $a_1, \dots, a_n \in \text{dom}(p)$  gilt

$$(a_1, \dots, a_n) \in R^A \Leftrightarrow (p(a_1), \dots, p(a_n)) \in R^B.$$

Für  $\bar{a} = (a_1, \dots, a_n) \in A^n$  und  $\bar{b} = (b_1, \dots, b_n) \in B^n$  schreiben wir  $\bar{a} \mapsto \bar{b}$  für die Abbildung mit Definitionsbereich  $\{a_1, \dots, a_n\}$ , die jedes  $a_i$  auf  $b_i$  abbildet. Dabei setzen wir natürlich implizit voraus, dass die  $a_i$  paarweise verschieden sind bzw., falls  $a_i = a_j$  gilt, dass auch  $b_i = b_j$  ist, damit die Abbildung wohldefiniert ist.

Man beachte, dass eine Abbildung  $p$  mit  $\text{dom}(p) \subseteq A$  und  $\text{ran}(p) \subseteq B$  genau dann ein partieller Isomorphismus ist, wenn  $\text{dom}(p)$  alle Konstanten von  $A$  enthält und für alle quantorenfreien Formeln  $\varphi(x_1, \dots, x_n)$  und alle  $a_1, \dots, a_n \in \text{dom}(p)$  gilt:

$$A \models \varphi(a_1, \dots, a_n) \Leftrightarrow B \models \varphi(p(a_1), \dots, p(a_n))$$

Im Allgemeinen lässt sich nichts darüber sagen, ob partielle Isomorphismen Formeln mit Quantoren erhalten. Wie wir bald sehen werden, hat  $m$ -Äquivalenz etwas mit der Fortsetzbarkeit partieller Isomorphismen zu tun.

*Ehrenfeucht-Spiele.* Seien nun  $\bar{a}$  und  $\bar{b}$  Folgen der Länge  $n$  in  $A$  bzw.  $B$ . Das **Ehrenfeucht-Spiel**  $\mathcal{G}_m(A, \bar{a}, B, \bar{b})$  ist folgendes Spiel über  $m$  Runden zwischen **Samson (spoiler)** und **Delilah (duplicator)**:

In der  $i$ -ten Runde wählt Samson eine der beiden Strukturen  $A$  oder  $B$  und ein Element dieser Struktur. Delilah antwortet mit einem Element der anderen Struktur. Das in dieser Runde gewählte Element von  $A$  sei  $e_i$ , das von  $B$  sei  $f_i$ .

Insgesamt werden also zwei Folgen  $\bar{e} \in A^m$  und  $\bar{f} \in B^m$  gewählt. Delilah **gewinnt**  $\mathcal{G}_m(A, \bar{a}, B, \bar{b})$ , falls die Abbildung  $\bar{a}\bar{e} \mapsto \bar{b}\bar{f}$  ein partieller Isomorphismus ist.

Sind  $\bar{a}$  und  $\bar{b}$  Folgen der Länge 0, so schreiben wir für  $\mathcal{G}_m(A, \bar{a}, B, \bar{b})$  einfach  $\mathcal{G}_m(A, B)$ .

$\mathcal{G}_m(A, \bar{a}, B, \bar{b})$  ist ein **endliches** Spiel mit **perfekter Information**. Das Spiel (game) ist endlich, weil jede Partie (play) eine endliche Anzahl von Zügen (bzw. Runden) dauert, und es ist ein Spiel mit perfekter Information, weil der Spieler, der gerade am Zug ist, genau weiß welche Züge der Gegner bisher gemacht hat. (Das bekannte Spiel mit Stein, Schere und Papier ist ein Spiel ohne perfekte Information, weil man den aktuellen Zug des Gegners nicht kennt.)

Eine **Gewinnstrategie** für einen der beiden Spieler ist eine Abbildung, die zum bisherigen Spielverlauf (d.h., zur Folge der bisher gespielten Züge) einen Zug vorschlägt, so dass der Spieler das Spiel immer gewinnt, wenn er entsprechend der Strategie spielt. Wenn einer der beiden Spieler ein Gewinnstrategie hat, sagen wir kurz **er gewinnt** das Spiel (weil er jede Partie gewinnen könnte, wenn er wollte).

Wir betrachten nur Spiele zwischen zwei Spielern, bei denen immer einer der beiden Spieler gewinnt (und bei denen die Regeln sich nicht mit der Zeit verändern). Wir nehmen an, dass die Spiele in Runden ablaufen, in denen immer zuerst der erste Spieler und dann der zweite Spieler je einmal ziehen. Das Spiel endet immer mit einem Zug des zweiten Spielers (auch wenn das Spiel eventuell schon vorher entschieden ist).

**Satz 2.2.** *Sein  $\mathcal{G}$  ein endliches Spiel mit perfekter Information. Dann hat einer der beiden Spieler eine Gewinnstrategie.*

*Beweis.* Angenommen der zweite Spieler (II) hat keine Gewinnstrategie. Wir geben eine Gewinnstrategie für den ersten Spieler (I) an.

Es gibt einen ersten Zug für I mit folgender Eigenschaft: Wenn I den Zug spielt, so hat II keine Gewinnstrategie für den Rest des Spieles. Denn sonst hätte II eine Gewinnstrategie für das gesamte Spiel. II antwortet mit irgendeinem Zug. Immernoch hat II keine Gewinnstrategie für das verbleibende Spiel, da II sonst bereits direkt nach dem ersten Zug von I eine Gewinnstrategie für das verbleibende Spiel gehabt hätte.

Angenommen, es wurden bereits  $n$  Runden gespielt, I ist am Zug und II hat keine Gewinnstrategie für den Rest des Spieles. Dann gibt es einen Zug für I, so dass II immernoch keine Gewinnstrategie für das verbleibende Spiel hat. Wie oben bleibt die Nichtexistenz einer Gewinnstrategie für II erhalten, wenn II irgendeinen Zug macht.

Nach endlich vielen Runden ist das Spiel beendet. Wegen der Wahl der Züge von I hatte II in seinem letzten Zug keine Gewinnstrategie. Insbesondere kann II nicht gewonnen haben. Also hat I gewonnen und die angegebene Strategie für I ist in der Tat eine Gewinnstrategie.  $\square$

**Lemma 2.3.** a) Ist  $A \cong B$ , so gewinnt Delilah  $\mathcal{G}_m(A, B)$  für alle  $m \in \mathcal{N}$ .

b) Falls Delilah  $\mathcal{G}_{m+1}(A, B)$  gewinnt und  $|A|=m$  ist, so gilt  $A \cong B$ .

*Beweis.* a) Sei  $i : A \rightarrow B$  ein Isomorphismus. Dann gewinnt Delilah, indem sie in jedem Zug das der Wahl Samsons via  $i$  entsprechende Element der jeweils anderen Struktur wählt.

b) Wir lassen Samson und Delilah gegeneinander spielen. Delilah folgt dabei ihrer Gewinnstrategie. Nach der  $m$ -ten Runde wurden Folgen  $\bar{e} \in A^m$  und  $\bar{f} \in B^m$  gewählt. Angenommen, Samson hat so gewählt, dass die  $a_i$  und die  $b_i$  jeweils paarweise verschieden sind. Dann ist  $A = \{a_1, \dots, a_m\}$ .

Die Abbildung  $i : \bar{a} \mapsto \bar{b}$  ist ein partieller Isomorphismus, da Delilah das Spiel gewinnt. Die Abbildung  $i$  ist ein Isomorphismus, falls  $B = \{b_1, \dots, b_m\}$  gilt. Angenommen,  $B$  enthält noch ein Element  $b_{m+1}$ , das nicht in  $\{b_1, \dots, b_m\}$  liegt. Dann kann Samson im letzten Zug  $b_{m+1}$  wählen und gewinnt. Ein Widerspruch. Also sind  $A$  und  $B$  isomorph  $\square$



Als nächstes definieren wir für alle Strukturen  $A$ , für alle  $m \in \mathbb{N}$  und alle  $a_1, \dots, a_n \in A$  eine Formel  $\varphi_{A,\bar{a}}^m(x_1, \dots, x_n)$ , so dass für alle Strukturen  $B$  und alle  $b_1, \dots, b_n \in B$  gilt:

$$B \models \varphi_{A,\bar{a}}^m(\bar{b}) \text{ genau dann, wenn Delilah } \mathcal{G}_m(A, \bar{a}, B, \bar{b}) \text{ gewinnt}$$

Ist  $n = 0$ , so schreiben wir  $\varphi_A^m$  anstelle von  $\varphi_{A,\bar{a}}^m(x_1, \dots, x_n)$ . Ergibt sich  $A$  aus dem Zusammenhang, so schreiben wir  $\varphi_{\bar{a}}^m(x_1, \dots, x_n)$  anstelle von  $\varphi_{A,\bar{a}}^m(x_1, \dots, x_n)$ .

Die Definition von  $\varphi_{A,\bar{a}}^m(x_1, \dots, x_n)$  erfolgt gleichzeitig für alle  $n \in \mathbb{N}$  und alle  $\bar{a} \in A^n$  durch Induktion über  $m$ . Eine Formel heißt **atomar**, wenn sie keine Quantoren und keine Booleschen Verknüpfungen enthält. Wir schreiben  $\bar{x}$  für  $x_1, \dots, x_n$ . Es sei

$$\varphi_{A,\bar{a}}^0(\bar{x}) := \bigwedge \{ \varphi(\bar{x}) : \varphi \text{ ist atomare oder negierte atomare Formel mit } A \models \varphi(\bar{a}) \}.$$

Für  $m > 0$  sei

$$\varphi_{A,\bar{a}}^m(\bar{x}) := \bigwedge_{a \in A} \exists x_{n+1} \varphi_{\bar{a}a}^{m-1}(\bar{x}, x_{n+1}) \wedge \forall x_{n+1} \bigvee_{a \in A} \varphi_{\bar{a}a}^{m-1}(\bar{x}, x_{n+1}).$$

Man beachte, dass die großen Konjunktionen und Disjunktionen jeweils über endliche Mengen gebildet werden: Man sieht leicht durch Induktion über  $m$ , dass für alle  $n \in \mathbb{N}$  die Menge  $\{ \varphi_{A,\bar{a}}^m(\bar{x}) : A \text{ ist eine Struktur und } \bar{a} \in A^n \}$  endlich ist. Der Induktionsanfang ist dabei die Tatsache, dass die Menge  $\{ \varphi(x_1, \dots, x_n) : \varphi \text{ ist atomare oder negierte atomare Formel} \}$  endlich ist, solange das Vokabular endlich ist. Letzteres setzen wir jedoch immer implizit voraus.

Die Formel  $\varphi_{A,\bar{a}}^m(\bar{x})$  ist der  $m$ -**Isomorphietyp** (oder die  $m$ -**Hintikka-Formel**) von  $\bar{a}$  in  $A$ . Wir sammeln ein paar einfache Eigenschaften der  $\varphi_{A,\bar{a}}^m(\bar{x})$ .

**Lemma 2.4.** *a) Der Quantorenrang von  $\varphi_{A,\bar{a}}^m(\bar{x})$  ist genau  $m$ .*

*b)  $A \models \varphi_{A,\bar{a}}^m(\bar{a})$*

*c) Für alle  $B$  und alle  $\bar{b} \in B^n$  gilt:*

*$B$  erfüllt  $\varphi_{A,\bar{a}}^0(\bar{b})$  genau dann, wenn  $\bar{a} \mapsto \bar{b}$  ein partieller Isomorphismus ist.*

Wir sind nun in der Lage, den Satz von Ehrenfeucht zu beweisen.

**Satz 2.5** (Ehrenfeucht). *Seien  $A$  und  $B$  Strukturen,  $m, n \in \mathbb{N}$ ,  $\bar{a} \in A^n$  und  $\bar{b} \in B^n$ . Dann sind die folgenden Aussagen äquivalent:*

(1) *Delilah gewinnt  $\mathcal{G}_m(A, \bar{a}, B, \bar{b})$ .*

(2)  *$B \models \varphi_{A,\bar{a}}^m(\bar{b})$*

(3) *Für alle Formeln  $\varphi(\bar{x})$  mit Quantorenrang  $\leq m$  gilt*

$$(*) \quad A \models \varphi(\bar{a}) \Leftrightarrow B \models \varphi(\bar{b}).$$

*Beweis.* Aus (3) folgt (2), da  $\varphi_{A,\bar{a}}^m(\bar{x})$  eine Formel vom Quantorenrang  $m$  ist und  $A \models \varphi_{A,\bar{a}}^m(\bar{a})$  gilt.

Wir beweisen die Äquivalenz von (1) und (2) durch Induktion über  $m$ . Für  $m = 0$  gilt

$$\begin{aligned} \text{Delilah gewinnt } \mathcal{G}_0(A, \bar{a}, B, \bar{b}) &\Leftrightarrow \bar{a} \mapsto \bar{b} \text{ ist ein partieller Isomorphismus} \\ &\Leftrightarrow B \models \varphi_{A,\bar{a}}^0(\bar{b}) \end{aligned}$$

nach Lemma 2.4 c).

Für  $m > 0$  gilt Folgendes: Delilah gewinnt  $\mathcal{G}_m(A, \bar{a}, B, \bar{b})$  genau dann, wenn für alle  $a \in A$  ein  $b \in B$  existiert, so dass Delilah  $\mathcal{G}_{m-1}(A, \bar{a}a, B, \bar{b}b)$  gewinnt, und für alle  $b \in B$  ein  $a \in A$  existiert, so dass Delilah  $\mathcal{G}_{m-1}(A, \bar{a}a, B, \bar{b}b)$  gewinnt. Nach Induktionsannahme ist Letzteres ist genau dann der Fall, wenn für alle  $a \in A$  ein

$b \in B$  mit  $B \models \varphi_{\bar{a}\bar{a}}^{m-1}(\bar{b}, b)$  existiert und für alle  $b \in B$  ein  $a \in A$  mit  $B \models \varphi_{\bar{a}\bar{a}}^{m-1}(\bar{b}, b)$  existiert. Das ist aber äquivalent zu

$$B \models \bigwedge_{a \in A} \exists x_{n+1} \varphi_{\bar{a}\bar{a}}^{m-1}(\bar{b}, x_{n+1}) \wedge \forall x_{n+1} \bigvee_{a \in A} \varphi_{\bar{a}\bar{a}}^{m-1}(\bar{b}, x_{n+1}),$$

also zu  $B \models \varphi_{\bar{a}}^m(\bar{b})$ .

Die Implikation (1) $\Rightarrow$ (2) zeigen wir auch durch Induktion über  $m$ . Der Fall  $m = 0$  geht wie oben. Sei  $m > 0$ . Angenommen, Delilah gewinnt  $\mathcal{G}_m(A, \bar{a}, B, \bar{b})$ . Insbesondere ist  $\bar{a} \mapsto \bar{b}$  ein partieller Isomorphismus. Damit gilt (\*) für alle quantorenfreien Formeln. Man beachte, dass die Menge der Formeln, für die (\*) gilt, unter Booleschen Verknüpfungen abgeschlossen ist.

Sei  $\varphi(\bar{x})$  die Formel  $\exists y \psi(\bar{x}, y)$ , wobei  $\psi$  vom Quantorenrang  $< m$  ist und  $y$  verschieden von den  $x_i$ . Wir müssen zeigen, dass (\*) für  $\varphi$  gilt.

Angenommen,  $A \models \varphi(\bar{a})$ . Dann existiert  $a \in A$  mit  $A \models \psi(\bar{a}, a)$ . Nach (1) gewinnt Delilah  $\mathcal{G}_m(A, \bar{a}, B, \bar{b})$ . Also existiert  $b \in B$ , so dass Delilah  $\mathcal{G}_{m-1}(A, \bar{a}a, B, \bar{b}b)$  gewinnt. Nach Induktionsannahme ( $\psi$  hat höchstens den Quantorenrang  $m-1$ ) gilt  $B \models \psi(\bar{b}, b)$ , also  $B \models \varphi(\bar{b})$ . Analog sieht man  $B \models \varphi(\bar{b}) \Rightarrow A \models \varphi(\bar{a})$ .  $\square$

Für  $n = 0$  ergibt sich

**Korollar 2.6.** *Für alle Strukturen  $A$  und  $B$  und alle  $m \in \mathbb{N}$  sind äquivalent:*

- (1) *Delilah gewinnt  $\mathcal{G}_m(A, B)$ .*
- (2)  $B \models \varphi_A^m$
- (3)  $A \equiv_m B$

Mit Lemma 2.3 c) erhalten wir

**Korollar 2.7.** *Sei  $A$  eine Struktur mit  $|A| \leq m$ . Dann gilt für alle  $B$*

$$B \models \varphi_A^{m+1} \Leftrightarrow A \cong B.$$

Mit Hilfe der Hintikka-Formeln können wir eine Art Normalform für Formeln vom Quantorenrang  $m$  angeben.

**Satz 2.8.** *Sei  $\varphi(x_1, \dots, x_n)$  eine Formel mit Quantorenrang  $\leq m$ . Dann gilt*

$$\models \varphi \leftrightarrow \bigvee \{ \varphi_{A, \bar{a}}^m(\bar{x}) : A \text{ ist eine Struktur, } \bar{a} \in A^n \text{ und } A \models \varphi(\bar{a}) \}.$$

*Man beachte, dass die Disjunktion über eine endliche Menge gebildet wird.*

*Beweis.* Angenommen,  $B \models \varphi(\bar{b})$ . Dann taucht die Formel  $\varphi_{B, \bar{b}}^m$  in der Disjunktion auf der rechten Seite der Äquivalenz auf. Die Disjunktion wird also von  $\bar{b}$  erfüllt. Für die andere Richtung gelte

$$B \models \bigvee \{ \varphi_{A, \bar{a}}^m(\bar{b}) : A \text{ ist eine Struktur, } \bar{a} \in A^n \text{ und } A \models \varphi(\bar{a}) \}.$$

Dann gibt es  $A$  und  $\bar{a}$  mit  $A \models \varphi(\bar{a})$ , so dass  $B \models \varphi_{A, \bar{a}}^m(\bar{b})$  gilt. Es ist also die Aussage (2) in Satz 2.5 erfüllt. Damit ist auch die Aussage (3) in Satz 2.5 erfüllt, und wegen  $A \models \varphi(\bar{a})$  gilt  $B \models \varphi(\bar{b})$ .  $\square$

Wir können nun die Umkehrung von Lemma 2.1 beweisen.

**Satz 2.9.** *Eine Klasse  $K$  von endlichen Strukturen ist genau dann erststufig axiomatisierbar, wenn es ein  $m \in \mathbb{N}$  gibt, so dass  $K$  unter  $m$ -Äquivalenz abgeschlossen ist, d.h., so dass für alle  $A \in K$  und alle Strukturen  $B$  gilt:*

$$A \equiv_m B \Rightarrow B \in K$$

*Beweis.* Ist  $K$  erststufig axiomatisierbar, so existiert ein  $m \in \mathbb{N}$ , so dass  $K$  unter  $m$ -Äquivalenz abgeschlossen ist. Das besagt Lemma 2.1.

Angenommen,  $K$  ist unter  $m$ -Äquivalenz abgeschlossen für ein gewisses  $m \in \mathbb{N}$ . Wir zeigen, dass  $K$  die Modellklasse der Aussage

$$\psi := \bigvee \{\varphi_A^m : A \in K\}$$

ist. (Man beachte wieder, dass die Disjunktion über eine endliche Menge von Aussagen gebildet wird.)

Da jede Struktur  $A$  die Aussage  $\varphi_A^m$  erfüllt, ist jedes Element von  $K$  Modell von  $\psi$ .

Sei nun  $B$  eine Struktur mit  $B \models \psi$ . Dann existiert eine Struktur  $A \in K$  mit  $B \models \varphi_A^m$ . Nach Korollar 2.6 ist  $A \equiv_m B$ . Da  $K$  unter  $m$ -Äquivalenz abgeschlossen ist, ist  $B \in K$ . Das zeigt  $K = \text{Mod}(\psi)$ .  $\square$

**2.3. Der Satz von Fraïssé.** Wir geben noch eine Variante von Satz 2.5 an, in der  $m$ -Äquivalenz etwas algebraischer als mit Ehrenfeucht-Spielen charakterisiert wird.

**Definition 2.10.** Zwei Strukturen  $A$  und  $B$  heißen  $m$ -isomorph (kurz  $A \cong_m B$ ), falls es eine Folge  $(I_j)_{j \leq m}$  gibt, für die gilt:

- (MI1) Jedes  $I_j$  ist eine nichtleere Menge partieller Isomorphismen von  $A$  nach  $B$ .
- (MI2) (**Forth-Eigenschaft**) Für alle  $j < m$ ,  $p \in I_{j+1}$  und  $a \in A$  existiert  $q \in I_j$  mit  $p \subseteq q$  und  $a \in \text{dom}(q)$ .
- (MI3) (**Back-Eigenschaft**) Für alle  $j < m$ ,  $p \in I_{j+1}$  und  $b \in B$  existiert  $q \in I_j$  mit  $p \subseteq q$  und  $b \in \text{ran}(q)$ .

Ist  $(I_j)_{j \leq m}$  eine Folge, die (MI1)–(MI3) erfüllt, so sagen wir, dass  $A$  und  $B$   $m$ -isomorph sind **via**  $(I_j)_{j \leq m}$ .

Für Strukturen  $A$  und  $B$  sowie  $m \in \mathbb{N}$  sei

$$W_m(A, B) := \{\bar{a} \mapsto \bar{b} : \text{Es gibt } s \in \mathbb{N} \text{ mit } \bar{a} \in A^s, \bar{b} \in B^s \text{ und Delilah gewinnt } \mathcal{G}^m(A, \bar{a}, B, \bar{b})\}$$

die Menge der **Gewinnpositionen** für Delilah.

**Satz 2.11.** *Seien  $A$  und  $B$  Strukturen,  $m, s \in \mathbb{N}$ ,  $\bar{a} \in A^s$  und  $\bar{b} \in B^s$ . Dann sind äquivalent:*

- (1) *Delilah gewinnt  $\mathcal{G}_m(A, \bar{a}, B, \bar{b})$ .*
- (2)  *$\bar{a} \mapsto \bar{b} \in W_m(A, B)$  und  $A \cong_m B$  via  $(W_j(A, B))_{j \leq m}$ .*
- (3) *Es gibt  $(I_j)_{j \leq m}$  mit  $(\bar{a} \mapsto \bar{b}) \in I_m$ , so dass  $A$  und  $B$  via  $(I_j)_{j \leq m}$   $m$ -isomorph sind.*
- (4)  *$B \models \varphi_{\bar{a}}^m(\bar{b})$*
- (5)  *$\bar{a}$  erfüllt in  $A$  dieselben Formeln vom Quantorenrang  $\leq m$  wie  $\bar{b}$  in  $B$ .*

*Beweis.* (1) $\Rightarrow$ (2): Angenommen, Delilah gewinnt  $\mathcal{G}_m(A, \bar{a}, B, \bar{b})$ . Nach Definition von  $W_m(A, B)$  gilt dann  $\bar{a} \mapsto \bar{b} \in W_m(A, B)$ . Außerdem ist kein  $W_j(A, B)$  leer. Wir zeigen die forth-Eigenschaft von  $(W_j(A, B))_{j \leq m}$ . Der Beweis der back-Eigenschaft ist symmetrisch.

Seien  $j < m$ ,  $(\bar{e} \mapsto \bar{f}) \in W_{j+1}(A, B)$  und  $a \in A$ . Dann gewinnt Delilah  $\mathcal{G}_{j+1}(A, \bar{e}, B, \bar{f})$ . Wenn Samson im ersten Zug dieses Spiels  $a$  zieht, so gibt es  $b \in B$ , so dass Delilah das Spiel  $\mathcal{G}_j(A, \bar{e}a, B, \bar{f}b)$  gewinnt. Insbesondere ist, wie für die forth-Eigenschaft gewünscht,  $(\bar{e}a \mapsto \bar{f}b) \in W_j(A, B)$ .

(2) $\Rightarrow$ (3) ist trivial. Die restlichen Implikationen bis auf (3) $\Rightarrow$ (1) folgen aus Satz 2.5. Für (3) $\Rightarrow$ (2) sei  $A \cong_m B$  via  $(I_j)_{j \leq m}$  mit  $(\bar{a} \mapsto \bar{b}) \in I_m$ . Wir geben eine Gewinnstrategie für Delilah in dem Spiel  $\mathcal{G}_m(A, \bar{a}, B, \bar{b})$  an.

Im  $i$ -ten Zug sollte Delilah  $e_i \in A$  beziehungsweise  $f_i \in B$  so wählen, dass für  $p_i : \bar{a}e_1 \dots e_i \mapsto \bar{b}f_1 \dots f_i$  ein  $q \in I_{m-i}$  mit  $p_i \subseteq q$  existiert. Das geht wegen der back-and-forth-Eigenschaften von  $(I_j)_{j \leq m}$ . Insgesamt spielen die beiden Spieler dann  $p_m$ , und es gibt  $q \in I_0$  mit  $p_m \subseteq q$ . Da  $q$  ein partieller Isomorphismus ist, ist auch  $p_m$  ein partieller Isomorphismus. Also gewinnt Delilah.  $\square$

Setzt man  $s = 0$  ergibt sich aus Satz 2.11 sofort

**Korollar 2.12.** *Für zwei Strukturen  $A$  und  $B$  sowie  $m \in \mathbb{N}$  sind folgende Aussagen äquivalent:*

- (1) *Delilah gewinnt  $\mathcal{G}_m(A, B)$ .*
- (2)  *$A \cong_m B$  via  $(W_j(A, B))_{j \leq m}$ .*
- (3)  *$A \cong_m B$*
- (4)  *$B \models \varphi_A^m$*
- (5)  *$A \equiv_m B$*

Die Äquivalenz von (3) und (5) in diesem Korollar ist als der Satz von Fraïssé bekannt. Deshalb nennt man die Ehrenfeucht-Spiele auch Ehrenfeucht-Fraïssé-Spiele.

Wir geben eine einfache Anwendung der Sätze von Ehrenfeucht und Fraïssé an.

**Satz 2.13.** *Sei  $\tau$  ein endliches Vokabular ohne Funktionssymbole. Dann ist die Klasse  $K$  der endlichen  $\tau$ -Strukturen mit gerader Mächtigkeit nicht erststufig axiomatisierbar.*

*Beweis.* Nach Lemma 2.1 genügt es, für jedes  $m \in \mathbb{N}$  Strukturen  $A$  und  $B$  anzugeben mit  $A \in K$ ,  $B \notin K$  und  $A \equiv_m B$ .

Sei also  $m \in \mathbb{N}$ . Sei  $A$  eine  $\tau$ -Struktur mit folgenden Eigenschaften:

- (A1)  $|A|$  ist gerade und  $\geq m$ .
- (A2) Alle Konstantensymbole haben dieselbe Interpretation  $c \in A$ .
- (A3) Alle Relationssymbole haben die leere Interpretation.

Wegen (A1) ist  $A \in K$ .

Sei  $B$  eine  $\tau$ -Struktur mit folgenden Eigenschaften:

- (B1)  $|B|$  ist ungerade und  $\geq m$ .
- (B2) Alle Konstantensymbole haben dieselbe Interpretation  $d \in B$ .
- (B3) Alle Relationssymbole haben die leere Interpretation.

Wegen (B1) ist  $B \notin K$ .

Wir zeigen  $A \equiv_m B$ . Nach Korollar 2.6 genügt es zu zeigen, dass Delilah  $\mathcal{G}_m(A, B)$  gewinnt. Wegen der Wahl von  $A$  und  $B$  ist jede partielle Bijektion zwischen  $A$  und  $B$ , die entweder  $c$  auf  $d$  abbildet oder (auf  $c$  nicht definiert ist und  $d$  nicht trifft), ein partieller Isomorphismus.

Wir geben eine Gewinnstrategie für Delilah an. Nach dem  $i$ -ten Zug seien die Folgen  $(a_1, \dots, a_i) \in A^i$  und  $(b_1, \dots, b_i) \in B^i$  gespielt. Angenommen, Samson zieht  $a \in A$ . Ist  $a$  eines der bereits gespielten  $a_1, \dots, a_i$ , zum Beispiel  $a_j$ , so antwortet Delilah mit  $b_j$ . Ist  $a = c$ , so antwortet Delilah mit  $d \in B$ . Ist  $a$  nicht unter den  $a_1, \dots, a_i$ , so antwortet Delilah mit einem beliebigen  $b \in B \setminus \{b_1, \dots, b_i\}$ . Das geht wegen  $|B| \geq m$ .

Wählt Samson ein  $b \in B$ , so spielt Delilah entsprechend. Es ist klar, dass Delilah das Spiel gewinnt.  $\square$

Man beachte, dass dieser Beweis auch für Graphen durchgeht. Ist  $\tau$  das Vokabular der Graphentheorie, so sind die oben konstruierten Strukturen in der Tat Graphen. Man kann aber zeigen, dass es über einem geeigneten Vokabular (ein zweistelliges Relationssymbol genügt) erststufig axiomatisierbare Klassen endlicher Strukturen gibt, die zwar beliebig große Strukturen enthalten, aber nur solche von gerader Mächtigkeit.

**2.4. Der Satz von Hanf.** Sei  $A$  eine  $\tau$ -Struktur, wobei  $\tau$  wieder ein endliches Vokabular ohne Funktionssymbole ist. Wir definieren eine zweistellige Relation  $E^A$  wie folgt:

Für  $a, b \in A$  mit  $a \neq b$  sei  $(a, b) \in E^A$  genau dann, wenn es ein  $n$ -stelliges Relationssymbol  $R \in \tau$  gibt sowie  $\bar{c} \in A^n$ , so dass  $a$  und  $b$  Komponenten des Tupels  $\bar{c}$  sind.

Die Struktur  $G(A) := (A, E^A)$  nennt man den **Gaifman-Graphen** von  $A$ . Wenn  $A$  selbst ein Graph ist, so gilt  $G(A) = A$ . Für  $a, b \in A$  sei  $d(a, b)$  der **Abstand** von  $a$  und  $b$  in  $G(A)$ , also die minimale Länge eines Weges von  $a$  nach  $b$  in  $G(A)$ , falls so ein Weg existiert, und  $\infty$ , falls in  $G(A)$  kein Weg von  $a$  nach  $b$  existiert. Wie man leicht nachrechnet, ist  $d$  eine Metrik auf  $A$ , falls  $G(A)$  zusammen hängend ist.

Für  $r \in \mathbb{N}$  und  $a \in A$  sei

$$N^A(r, a) := \{b \in A : d(a, b) \leq r\}$$

die  **$r$ -Umgebung** von  $a$ . Ergibt sich  $A$  aus dem Zusammenhang, so schreiben wir auch einfach  $N(r, a)$  anstelle von  $N^A(r, a)$ . Für  $\bar{a} = (a_1, \dots, a_n) \in A^n$  sei  $N(r, \bar{a}) := N(r, a_1) \cup \dots \cup N(r, a_n)$ . Für  $n = 0$  erhalten wir damit  $N(r, \bar{a}) = \emptyset$ .

Mit  $(N(r, a), a)$  bezeichnen wir die Unterstruktur von  $A$  mit der Trägermenge  $N(r, a)$  mit der zusätzlichen Konstante  $a$ . Analog bezeichnet  $N((r, \bar{a}), \bar{a})$  die Unterstruktur von  $A$  mit der Trägermenge  $N(r, \bar{a})$  mit den zusätzlichen Konstanten  $a_1, \dots, a_n$ . Der  **$r$ -Typ** von  $a \in A$  sei der Isomphietyp von  $(N(r, a), a)$ . Für eine weitere  $\tau$ -Struktur  $B$  haben also  $a \in A$  und  $b \in B$  den gleichen  $r$ -Typ, wenn es einen Isomorphismus zwischen der Unterstruktur von  $A$  mit der Trägermenge  $N^A(r, a)$  und der Unterstruktur von  $B$  mit der Trägermenge  $N^B(r, b)$  gibt, der  $a$  auf  $b$  abbildet.

**Satz 2.14 (Hanf).** *Seien  $A$  und  $B$   $\tau$ -Strukturen und  $m \in \mathbb{N}$ . Sei  $e \in \mathbb{N}$  so, dass die  $4^m$ -Umgebungen in  $A$  und  $B$  höchstens  $e$  Elemente haben. Angenommen, für jeden  $4^m$ -Typ  $T$  gilt*

- (i)  *$A$  und  $B$  haben die gleiche Anzahl von Elementen vom  $4^m$ -Typ  $T$  oder*
- (ii)  *$A$  und  $B$  haben beide mehr als  $m \cdot e$  Elemente vom  $4^m$ -Typ  $T$ .*

*Dann gilt  $A \equiv_m B$ .*

*Beweis.* Wir benutzen Korollar 2.12 und zeigen, dass  $A$  zu  $B$   $m$ -isomorph ist via  $(I_j)_{j \leq m}$ , wobei

$$I_j := \{\bar{a} \mapsto \bar{b} : \text{Es gibt } k \leq m - j \text{ mit } \bar{a} \in A^k \text{ und } \bar{b} \in B^k \\ \text{und } (N^A(4^j, \bar{a}), \bar{a}) \cong (N^B(4^j, \bar{b}), \bar{b})\}$$

sei. (Kühn akzeptieren wir in dieser Definition  $\emptyset \cong \emptyset$ , obwohl wir sonst Strukturen als nicht leer voraussetzen.) Beachte, dass die Elemente von  $I_j$  tatsächlich partielle Isomorphismen zwischen  $A$  und  $B$  sind.

Aus der Definition der  $I_j$  ergibt sich, dass alle  $I_j$  die leere Funktion enthalten. Insbesondere sind die  $I_j$  nicht leer. (MI1) in Definition 2.10 ist also erfüllt. Wir

zeigen die forth-Eigenschaft (MI2) von  $(I_j)_{j \leq m}$ . Der Beweis der back-Eigenschaft (MI3) ist symmetrisch.

Sei  $j < m$ . Zunächst stellen wir fest, dass für jeden  $4^j$ -Typ  $T$  mindestens eine der folgenden Aussagen gilt:

- (i)<sub>j</sub>  $A$  und  $B$  haben die gleiche Anzahl von Elementen vom  $4^j$ -Typ  $T$  oder
- (ii)<sub>j</sub>  $A$  und  $B$  haben beide mehr als  $m \cdot e$  Elemente vom  $4^j$ -Typ  $T$ .

Sei nämlich  $T$  ein  $4^j$ -Typ und  $T'$  ein  $4^m$ -Typ. Wir sagen, dass  $T'$  den Typ  $T$  **erweitert**, falls es eine Struktur gibt, die ein Element enthält, welches den  $4^j$ -Typ  $T$  und den  $4^m$ -Typ  $T'$  hat.

Angenommen,  $T$  wird von einem  $4^m$ -Typ  $T'$  erweitert, für den (ii) gilt. Jedes Element vom  $4^m$ -Typ  $T'$  hat den  $4^j$ -Typ  $T$ . Damit gilt für  $T$  die Aussage (ii)<sub>j</sub>.

Angenommen, für jeden  $4^m$ -Typ  $T'$ , der  $T$  erweitert, gilt (i). Treten in einer der beiden Strukturen  $A$  und  $B$  mehr als  $m \cdot e$  verschiedene  $4^m$ -Typen auf, die  $T$  erweitern, so gilt für  $T$  die Aussage (ii)<sub>j</sub>. Treten in  $A$  und  $B$  nur endlich viele  $4^m$ -Typen auf, die  $T$  erweitern, so gilt für  $T$  die Aussage (i)<sub>j</sub>, da jedes Element nur einen  $4^m$ -Typ hat.

Sei nun  $(\bar{a} \mapsto \bar{b}) \in I_{j+1}$  und  $a \in A$ . Wir suchen  $b \in B$  mit  $(\bar{a}a \mapsto \bar{b}b) \in I_j$ . Nach Definition von  $I_{j+1}$  existiert ein Isomorphismus

$$\pi : (N^A(4^{j+1}, \bar{a}), \bar{a}) \rightarrow (N^B(4^{j+1}, \bar{b}), \bar{b}).$$

Wir unterscheiden zwei Fälle:

**Fall 1.**  $a \in N^A(3 \cdot 4^j, \bar{a})$ . In diesem Fall ist  $N^A(4^j, \bar{a}a) \subseteq N^A(4^{j+1}, \bar{a})$ . Setze  $b := \pi(a)$ . Dann ist  $\pi \upharpoonright N^A(4^j, \bar{a}a)$  ein Isomorphismus zwischen  $(N^A(4^j, \bar{a}a), \bar{a}a)$  und  $(N^B(4^j, \bar{b}b), \bar{b}b)$ . Insbesondere gilt  $(\bar{a}a \mapsto \bar{b}b) \in I_j$ .

**Fall 2.**  $a \notin N^A(3 \cdot 4^j, \bar{a})$ . In diesem Fall hat jedes Element von  $N^A(4^j, a)$  zu jedem Element von  $N^A(4^j, \bar{a})$  einen Abstand  $> 1$ . Insbesondere gibt es in  $G(A)$  keine Kante, die zwischen  $N^A(4^j, a)$  und  $N^A(4^j, \bar{a})$  verläuft. Es gibt also auf  $A$  keine Relation, die ein Tupel enthält, das gleichzeitig Komponenten in  $N^A(4^j, a)$  und in  $N^A(4^j, \bar{a})$  hat.

Sei  $T$  der  $4^j$ -Typ von  $a$  in  $A$ . Sei  $k \leq m - j$  so, dass  $\bar{a} \in A^k$  und  $\bar{b} \in B^k$  gelten. Da  $\pi \upharpoonright N^A(3 \cdot 4^j, \bar{a})$  ein Isomorphismus zwischen  $(N^A(3 \cdot 4^j, \bar{a}), \bar{a})$  und  $(N^B(3 \cdot 4^j, \bar{b}), \bar{b})$  ist, enthalten  $N^A(3 \cdot 4^j, \bar{a})$  und  $N^B(3 \cdot 4^j, \bar{b})$  gleich viele Elemente vom  $4^j$ -Typ  $T$ .

Das sind, nach unserer Annahme über die Größe von Umgebungen, jeweils nicht mehr als  $k \cdot e$ . Sowohl (i)<sub>j</sub> als auch (ii)<sub>j</sub> implizieren, dass es ein  $b \in B \setminus N^B(3 \cdot 4^j, \bar{b})$  gibt, welches den  $4^j$ -Typ  $T$  hat. Wie oben gibt es auf  $B$  keine Relation, die ein Tupel enthält, welches gleichzeitig Komponenten in  $N^B(4^j, b)$  und in  $N^B(4^j, \bar{b})$  hat.

Wähle einen Isomorphismus

$$\pi' : (N^A(4^j, a), a) \rightarrow (N^B(4^j, b), b).$$

Dann ist  $\pi \cup \pi' \upharpoonright N^A(4^j, \bar{a}a)$  ein Isomorphismus zwischen  $(N^A(4^j, \bar{a}a), \bar{a}a)$  und  $(N^B(4^j, \bar{b}b), \bar{b}b)$ . Damit gilt  $(\bar{a}a \mapsto \bar{b}b) \in I_j$ .  $\square$

Als Anwendung des Satzes von Hanf zeigen wir, dass sich weder Kreisfreiheit noch Zusammenhang von Graphen erststufig axiomatisieren lassen.

**Satz 2.15.** a) Die Klasse der endlichen, kreisfreien Graphen ist nicht erststufig axiomatisierbar.

b) Die Klasse der endlichen, zusammenhängenden Graphen ist nicht erststufig axiomatisierbar.

*Beweis.* a) Sei  $m \in \mathbb{N}$ . Wir suchen zwei endliche Graphen  $A$  und  $B$ , so dass  $A$  kreisfrei ist,  $B$  einen Kreis hat und  $A \equiv_m B$  gilt.

Setze  $e := 2 \cdot 4^m + 1$ . Sei  $A$  eine Kette mit  $m \cdot e + 2 \cdot 4^m + 1$  Elementen. Sei  $B$  eine Kette mit  $m \cdot e + 2 \cdot 4^m + 1$  Elementen zusammen mit einem (zur Kette disjunkten)

Kreis der Länge  $e + 1$ . Offenbar ist  $A$  kreisfrei, aber  $B$  nicht. Wir zeigen  $A \equiv_m B$  und benutzen dazu Satz 2.14.

Wie man leicht nachrechnet, haben die  $4^m$ -Umgebungen in  $A$  und  $B$  höchstens  $e$  Elemente. Wir zeigen, dass für jeden  $4^m$ -Typ (i) oder (ii) in Satz 2.14 gilt.

Ist  $T$  ein  $4^m$ -Typ der Mächtigkeit  $< e$ , so haben nur Elemente der Kette von  $B$  den  $4^m$ -Typ  $T$ , nämlich höchstens solche, deren Abstand zu einem der Endpunkte  $< 4^m$  ist. Da die Kette von  $B$  zu  $A$  isomorph ist, haben  $A$  und  $B$  gleich viele Elemente vom  $4^m$ -Typ  $T$ .

In  $A$  und  $B$  tritt nur ein  $4^m$ -Typ mit Mächtigkeit  $\geq e$  auf, nämlich eine Kette der Länge  $e$  zusammen mit ihrem Mittelpunkt als Konstante. In  $A$  haben genau diejenigen Elemente diesen  $4^m$ -Typ, deren Abstand zu den Endpunkten mindestens  $4^m$  beträgt. In  $B$  haben genau diejenigen Elemente diesen  $4^m$ -Typ, die entweder auf dem Kreis liegen oder auf der Kette von  $B$ , wobei ihr Abstand zu den Endpunkten der Kette von  $B$  mindestens  $4^m$  ist. In jedem Falle gibt es mehr als  $e \cdot m$  solcher Punkte.

Damit sind die Voraussetzungen von Satz 2.14 erfüllt, und es gilt  $A \equiv_m B$ .

b) Der Beweis von b) geht genauso, wie der von a). Wir müssen nur feststellen, dass der Graph  $A$  aus dem Beweis von a) zusammenhängend ist,  $B$  jedoch nicht.  $\square$

## 3. 0-1-GESETZE

Nach den Ehrenfeucht-Fraïssé-Spielen gibt es eine weitere wichtige Methode, um zu zeigen, dass gewisse Klassen endlicher Strukturen nicht erststufig axiomatisierbar sind. Das sind die sogenannten 0-1-Gesetze.

Für eine gegebene Klasse  $K$  endlicher Strukturen kann man sich fragen, ob eher viele oder wenige Strukturen über dem entsprechenden Vokabular in der Klasse  $K$  liegen. Genauso kann man sich für eine Teilklasse  $L$  von  $K$  fragen, ob eher viele Strukturen aus  $K$  in  $L$  liegen oder nicht.

Natürlich gibt es unendlich viele Strukturen des gleichen Isomorphietyps. Es gibt zwei Möglichkeiten, dieses Problem zu umgehen. Entweder man identifiziert je zwei isomorphe Strukturen und zählt nur Isomorphietypen anstelle von einzelnen Strukturen. Das ist sinnvoll, bringt aber gewisse technische Probleme mit sich. Eine andere Möglichkeit ist es, nur Strukturen auf einer festen Trägermenge zu betrachten, zum Beispiel auf Mengen der Form  $\{1, \dots, n\}$ .

Wir fixieren ein endliches Vokabular  $\tau$ .

**Definition 3.1.** Sei  $n \in \mathbb{N}$ . Für eine Klasse  $K$  endlicher  $\tau$ -Strukturen sei  $L_n(K)$  die Anzahl der Strukturen in  $K$  auf der Trägermenge  $\{1, \dots, n\}$ .  $L_n(\tau)$  sei die Anzahl aller  $\tau$ -Strukturen auf der Trägermenge  $\{1, \dots, n\}$ . Weiter sei

$$l_n(K) := \frac{L_n(K)}{L_n(\tau)}.$$

Für eine Formel  $\varphi$  über dem Vokabular  $\tau$  sei  $L_n(\varphi) := L_n(\text{Mod}(\varphi))$  und  $l_n(\varphi) := l_n(\text{Mod}(\varphi))$ . Falls der Grenzwert existiert, so sei

$$l(K) := \lim_{n \rightarrow \infty} l_n(K).$$

Entsprechend sei  $l(\varphi) = l(\text{Mod}(\varphi))$ , falls  $l(\text{Mod}(\varphi))$  definiert ist.

Ist  $H$  eine weitere Klasse von  $\tau$ -Strukturen, so sei

$$l_n(K|H) := \frac{L_n(K \cap H)}{L_n(H)}.$$

Falls der Grenzwert existiert, so sei

$$l(K|H) := \lim_{n \rightarrow \infty} l_n(K|H).$$

Schreibweisen wie  $l(\varphi|H)$  etc. sind selbsterklärend.

Die Zahl  $l(K)$ , so sie denn existiert, ist die **asymptotische Wahrscheinlichkeit** von  $K$ . Die Zahl  $l(K|H)$  ist die **asymptotische Wahrscheinlichkeit** von  $K$  **bezüglich**  $H$ .

Ein Satz  $\varphi$  gilt für **fast alle** endlichen Strukturen, wenn  $l(\varphi) = 1$  ist. In diesem Falle sagen wir,  $\varphi$  gilt **fast sicher**. Der Satz  $\varphi$  gilt für **fast alle** Strukturen in  $H$ , falls  $l(\varphi|H) = 1$  ist. Eine Klasse  $\Phi$  von Sätzen erfüllt das **0-1-Gesetz**, falls für alle  $\varphi \in \Phi$  gilt:  $l(\varphi) = 0$  oder  $l(\varphi) = 1$ .

In dieser Definition stehen  $L$  und  $l$  für “labeled”, da die Elemente der Strukturen die “Labels”  $1, \dots, n$  tragen.

**Beispiel 3.2.** a) Sei  $K$  die Klasse aller endlichen  $\tau$ -Strukturen mit einer geraden Anzahl von Elementen. Dann ist  $l_n(K) = 1$  für alle geraden  $n$  und  $= 0$  für alle ungeraden  $n$ . Damit existiert  $l(K)$  nicht.

b) Sei  $\tau$  das Vokabular mit einem einstelligen Funktionssymbol  $f$ . Betrachte den erststufigen Satz

$$\varphi := \forall x (f(x) \neq x),$$



der besagt, dass die Abbildung  $f$  keine Fixpunkte hat. Auf der Menge  $\{1, \dots, n\}$  gibt es  $n^n$  einstellige Funktionen. Davon sind  $(n-1)^n$  fixpunktfrei. Damit gilt

$$l_n(\varphi) = \left(\frac{n-1}{n}\right)^n = \left(1 + \frac{1}{n}\right)^n.$$

Wie man aus der Analysis weiß, ist

$$l(\varphi) = \lim_{n \rightarrow \infty} \left(1 + \frac{1}{n}\right)^n = \frac{1}{e}.$$

Beispiel b) zeigt, dass kein 0-1-Gesetz für alle erststufige Aussagen über einem Vokabular mit mindestens einem einstelligen Funktionssymbol gilt. Man kann auch leicht zeigen, dass kein 0-1-Gesetz für alle erststufigen Aussagen über einem Vokabular mit mindestens einem Konstantensymbol und mindestens einem Relationssymbol gilt.

Wir werden aber zeigen, dass das 0-1-Gesetz für alle erststufigen Aussagen über einem Vokabular gilt, das nur Relationssymbole enthält.

Zunächst stellen wir fest, dass die Menge der fast sicheren Sätzen gewisse Abchlusseigenschaften hat.

**Lemma 3.3.** *Seien  $\varphi$  und  $\psi$  Sätze.*

- (1) *Existiert  $l(\varphi)$ , so existiert auch  $l(\neg\varphi)$  und es gilt  $l(\neg\varphi) = 1 - l(\varphi)$ .*
- (2) *Sind  $\varphi$  und  $\psi$  fast sicher, so auch ist auch  $\varphi \wedge \psi$  fast sicher.*
- (3) *Ist  $\Phi$  eine Menge von fast sicheren Sätzen und  $\psi$  aus  $\Phi$  ableitbar, so ist auch  $\psi$  fast sicher.*

*Beweis.* (1) Angenommen,  $l(\varphi) = \lim_{n \rightarrow \infty} L_n(\varphi)/L_n(\tau)$  existiert. Für jedes  $n \in \mathbb{N}$  gilt

$$\frac{L_n(\neg\varphi)}{L_n(\tau)} = \frac{L_n(\tau) - L_n(\varphi)}{L_n(\tau)} = 1 - \frac{L_n(\varphi)}{L_n(\tau)}.$$

Damit ist

$$l(\neg\varphi) = \lim_{n \rightarrow \infty} \left(1 - \frac{L_n(\varphi)}{L_n(\tau)}\right) = 1 - l(\varphi).$$

(2) Seien  $\varphi$  und  $\psi$  fast sicher und  $\varepsilon > 0$ . Sei  $n_0 \in \mathbb{N}$  so groß, dass für alle  $n \geq n_0$  gilt:

$$\frac{L_n(\varphi)}{L_n(\tau)} > 1 - \varepsilon \text{ und } \frac{L_n(\psi)}{L_n(\tau)} > 1 - \varepsilon$$

Dann ist

$$\frac{L_n(\varphi \wedge \psi)}{L_n(\tau)} = \frac{L_n(\text{Mod}(\varphi) \cap \text{Mod}(\psi))}{L_n(\tau)} > 1 - 2\varepsilon.$$

Das zeigt  $l(\varphi \wedge \psi) = 1$ .

(3) Ist  $\psi$  aus  $\Phi$  ableitbar, so ist  $\psi$  bereits aus einer endlichen Teilmenge  $\{\varphi_1, \dots, \varphi_k\}$  von  $\Phi$  ableitbar. Da die Sätze in  $\Phi$  fast sicher sind, ist nach (2) auch  $\varphi_1 \wedge \dots \wedge \varphi_k$  fast sicher. Wegen  $\varphi_1 \wedge \dots \wedge \varphi_k \models \psi$  ist damit auch  $\psi$  fast sicher.  $\square$

**Definition 3.4.** Sei  $\tau$  ein endliches Vokabular, das nur Relationssymbole enthält,  $r \in \mathbb{N}$  und

$$\Delta_{r+1} := \{\varphi(y_1, \dots, y_{r+1}) : \varphi \text{ hat die Form } R(\bar{x}) \text{ für ein } R \in \tau, \text{ wobei } y_{r+1} \text{ in } \bar{x} \text{ vorkommt}\}$$

Für eine Teilmenge  $\Phi$  von  $\Delta_{r+1}$  sei

$$\chi_\Phi := \forall y_1, \dots, y_r \left( \bigwedge_{1 \leq i < j \leq r} y_i \neq y_j \rightarrow \exists y_{r+1} \left( \bigwedge_{1 \leq i \leq r} y_i \neq y_{r+1} \wedge \bigwedge_{\varphi \in \Phi} \varphi \wedge \bigwedge_{\varphi \in \Delta_{r+1} \setminus \Phi} \neg \varphi \right) \right).$$

Eine Aussage der Form  $\chi_\Phi$  heißt  $(r+1)$ -**Erweiterungsaxiom**. Mit  $T_{\text{random}}(\tau)$  oder einfach  $T_{\text{random}}$  bezeichnen wir die Menge aller Erweiterungsaxiome über  $\tau$ .

Wir werden zeigen, dass jedes Erweiterungsaxiom in fast jeder Struktur gilt und dass für jeden Satz  $\varphi$  entweder  $\varphi$  selbst oder  $\neg\varphi$  aus  $T_{\text{random}}$  ableitbar ist. Mit Lemma 3.3 folgt daraus

**Satz 3.5.** *Für jeden Satz  $\varphi$  über  $\tau$  gilt  $l(\varphi) = 0$  oder  $l(\varphi) = 1$ .*

**Lemma 3.6.** *Sei  $\Phi \subseteq \Delta_{r+1}$ . Dann gilt  $\chi_\Phi$  fast sicher.*

*Beweis.* Wir zeigen  $l(\neg\chi_\Phi) = 0$ . Der Satz  $\neg\chi_\Phi$  ist äquivalent zu

$$\exists y_1, \dots, y_r \left( \bigwedge_{1 \leq i < j \leq r} y_i = y_j \wedge \forall y_{r+1} \left( \bigvee_{1 \leq i \leq r} y_i = y_{r+1} \vee \bigvee_{\varphi \in \Phi} \neg \varphi \vee \bigvee_{\varphi \in \Delta_{r+1} \setminus \Phi} \varphi \right) \right).$$

Sei  $A = \{1, \dots, n\}$  und seien  $a_1, \dots, a_r, a \in A$ . Die Wahrscheinlichkeit, dass das Tupel  $(a_1, \dots, a_r, a)$  alle Formeln in  $\Phi \cup \{\neg\varphi : \varphi \in \Delta_{r+1} \setminus \Phi\}$  erfüllt, sei  $\delta$ . Ist  $c$  die Anzahl der Teilmengen von  $\Delta_{r+1}$ , so ist  $\delta = \frac{1}{c}$ . Damit gilt

$$l_n(\neg\chi_\Phi) \leq n^r \cdot \left( \frac{c-1}{c} \right)^{n-r} = n^r (1-\delta)^{n-r}.$$

Damit ist  $l(\neg\chi_\Phi) = \lim_{n \rightarrow \infty} l_n(\neg\chi_\Phi) = 0$ .  $\square$

Als nächstes zeigen wir, dass  $T_{\text{random}}$  genau ein abzählbares Modell hat (welches unendlich ist).

**Lemma 3.7.**  *$T_{\text{random}}(\tau)$  hat ein Modell.*

*Beweis.* Wir konstruieren eine abzählbar unendliche  $\tau$ -Struktur  $A$ , die alle Erweiterungsaxiome erfüllt. Die Trägermenge von  $A$  wird  $\mathbb{N}$  sein. Wir müssen also nur für jedes Relationssymbol  $R \in \tau$  die Interpretation  $R^A$  erklären. Das geschieht induktiv. Dazu konstruieren wir eine Folge  $A_0 \subseteq A_1 \subseteq \dots$  endlicher Teilmengen von  $\mathbb{N}$  mit  $\bigcup_{n \in \mathbb{N}} A_n = \mathbb{N}$  und für jedes Relationssymbol  $R \in \tau$  eine Folge  $R^{A_0} \subseteq R^{A_1} \subseteq \dots$  von Interpretationen von  $R$  in den verschiedenen  $A_n$ . Dabei werden die  $R^{A_n}$  so gewählt, dass  $A_n$  zusammen mit den  $R^{A_n}$ ,  $R \in \tau$ , eine Unterstruktur von  $A_{n+1}$  zusammen mit den  $R^{A_{n+1}}$ ,  $R \in \tau$ , ist. Am Schluss setzen wir  $R^A := \bigcup_{n \in \mathbb{N}} R^{A_n}$  für jedes  $R \in \tau$ .

Setze  $A_0 := \emptyset$  und  $R^{A_0} := \emptyset$  für jedes  $R \in \tau$ . Angenommen,  $A_n$  und alle  $R^{A_n}$ ,  $R \in \tau$ , sind bereits gewählt. Wähle  $k \in \mathbb{N}$  und Folgen  $(r_i)_{i < k}$ ,  $(\Phi_i)_{i < k}$  und  $(\bar{a}_i)_{i < k}$  mit folgenden Eigenschaften:

- (1) Die  $r_i$  sind natürliche Zahlen  $\leq |A_n|$ .
- (2) Für alle  $i < k$  ist  $\Phi_i \subseteq \Delta_{r_i+1}$ .
- (3) Für alle  $i < k$  ist  $\bar{a}_i$  ein  $r_i$ -Tupel paarweise verschiedener Elemente von  $A_n$ .
- (4) Für jedes  $r \leq |A_n|$ , jedes  $r$ -Tupel  $\bar{a}$  paarweise verschiedener Elemente von  $A_n$  und alle  $\Phi \subseteq \Delta_{r+1}$  existiert ein  $i < k$  mit  $r_i = r$ ,  $\Phi_i = \Phi$  und  $\bar{a}_i = \bar{a}$ .

Für  $i \leq k$  definieren wir zunächst  $A_n^i$  und  $R_n^{A_n^i}$ ,  $R \in \tau$ , wie folgt: Setze  $A_n^0 := A_n$ . Sei  $i < k$ . Angenommen  $A_n^i$  und  $R_n^{A_n^i}$ ,  $R \in \tau$ , sind bereits definiert. Sei  $m := \min(\mathbb{N} \setminus A_n^i)$ . Setze  $A_n^{i+1} := A_n^i \cup \{m\}$ . Für alle  $R \in \tau$  setze  $R_n^{A_n^i}$  so zu  $R_n^{A_n^{i+1}}$  auf  $A_n^{i+1}$  fort, dass für alle  $\varphi \in \Delta_{r_i+1}$  gilt:

$$A_n^{i+1} \models \varphi(\bar{a}_i, m) \quad \Leftrightarrow \quad \varphi \in \Phi_i$$

Setze schließlich  $A_{n+1} := A_n^k$  und  $R_n^{A_{n+1}} := R_n^{A_n^k}$  für alle  $R \in \tau$ .

Das schließt die Definition der  $A_n$  und der  $R_n^{A_n}$  ab. Wir zeigen, dass  $A$  das Gewünschte leistet. Sei  $\psi \in T_{\text{random}}$ . Es ist  $A \models \psi$  zu zeigen.

Seien  $r \in \mathbb{N}$  und  $\Phi \subseteq \Delta_{r+1}$ , so dass  $\psi = \chi_\Phi$  gilt. Seien  $a_1, \dots, a_r \in A$  paarweise verschieden. Dann existiert ein  $n \in \mathbb{N}$  mit  $a_1, \dots, a_r \in A_n$ . Insbesondere ist  $r \leq |A_n|$ . Seien  $k, (r_i)_{i < k}, (\Phi_i)_{i < k}$  und  $(\bar{a}_i)_{i < k}$  wie in der Definition von  $A_{n+1}$ .

Dann existiert  $i < k$  mit  $r_i = r$ ,  $\Phi_i = \Phi$  und  $\bar{a}_i = (a_1, \dots, a_r)$ . Sei  $m$  diejenige natürliche Zahl mit  $A_n^{i+1} = A_n^i \cup \{m\}$ . Nach Definition von  $R_n^{A_n^{i+1}}$ ,  $R \in \tau$ , gilt für alle  $\varphi \in \Delta_{r+1}$

$$A_n^{i+1} \models \varphi(a_1, \dots, a_r, m) \quad \Leftrightarrow \quad \varphi \in \Phi.$$

Da die Relationen auf  $A$  diejenigen auf  $A_n^{i+1}$  fortsetzen, gilt das Entsprechende auch für  $A$  anstelle von  $A_n^{i+1}$ . Damit erfüllt  $A$  das Erweiterungsaxiom  $\chi_\Phi$ . Insgesamt gilt also  $A \models T_{\text{random}}$ .  $\square$

**Lemma 3.8.** *Jedes Modell von  $T_{\text{random}}$  ist unendlich.*

*Beweis.* Sei  $B$  eine endliche Struktur mit Mächtigkeit  $r$ . Es ist klar, dass jedes  $(r+1)$ -Erweiterungsaxiom zu je  $r$  paarweise verschiedenen Elementen einer Struktur die Existenz eines weiteren Elements fordert.  $B$  erfüllt also keines der  $(r+1)$ -Erweiterungsaxiome. Damit ist  $B$  nicht Modell von  $T_{\text{random}}$ .  $\square$

**Lemma 3.9.** *Je zwei abzählbare Modelle von  $T_{\text{random}}$  sind isomorph.*

*Beweis.* Seien  $A$  und  $B$  abzählbare Modelle von  $T_{\text{random}}$ . Nach Lemma 3.8 sind  $A$  und  $B$  unendlich. Seien  $(a_n)_{n \in \mathbb{N}}$  und  $(b_n)_{n \in \mathbb{N}}$  Aufzählungen von  $A$  bzw.  $B$ . Wir definieren eine aufsteigende Folge  $(f_m)_{m \in \mathbb{N}}$  partieller Isomorphismen von  $A$  nach  $B$ , so dass  $f := \bigcup_{m \in \mathbb{N}} f_m$  Isomorphismus  $A$  nach  $B$  ist.

Setze  $f_0 := \emptyset$ . Sei  $f_m$  bereits definiert. Ist  $m$  gerade, so sei  $a \in A \setminus \text{dom}(f_m)$  dasjenige Element, welches in der Aufzählung  $(a_n)_{n \in \mathbb{N}}$  von  $A$  den kleinsten Index hat. Sei  $r := |\text{dom}(f_m)|$  und  $\text{dom}(f_m) = \{x_1, \dots, x_r\}$ . Setze

$$\Phi := \{\varphi \in \Delta_{r+1} : A \models \varphi(x_1, \dots, x_r, a)\}.$$

Da  $B$  ein Modell von  $\chi_\Phi$  ist, existiert ein  $b \in B \setminus \text{ran}(f_m)$  mit

$$\Phi = \{\varphi \in \Delta_{r+1} : B \models \varphi(f_m(x_1), \dots, f_m(x_r), b)\}.$$

Setze  $f_{m+1} := f_m \cup \{(a, b)\}$ . Nach Wahl von  $b$  ist  $f_{m+1}$  ein partieller Isomorphismus.

Ist  $m$  ungerade, so sei  $b \in B \setminus \text{ran}(f_m)$  dasjenige Element mit dem kleinsten Index in der Aufzählung  $(b_n)_{n \in \mathbb{N}}$  von  $B$ . Wie oben existiert  $a \in A$ , so dass  $f_{m+1} := \{(a, b)\}$  ein partieller Isomorphismus ist. Das schließt die induktive Definition der  $f_m$  ab.

Es ist klar, dass  $f = \bigcup_{m \in \mathbb{N}} f_m$  ein partieller Isomorphismus ist. Es bleibt  $\text{dom}(f) = A$  und  $\text{ran}(f) = B$  zu zeigen. Wir zeigen nur  $\text{dom}(f) = A$ . Das Argument für  $\text{ran}(f) = B$  geht analog.

Angenommen,  $\text{dom}(f) \neq A$ . Sei  $n \in \mathbb{N}$  minimal mit  $a_n \in A \setminus \text{dom}(f)$ . Da unterhalb von  $n$  nur endlich viele natürliche Zahlen liegen, existiert ein  $m \in \mathbb{N}$ , so dass  $n$  bereits minimal ist mit  $a_n \in A \setminus \text{dom}(f_m)$ . Da  $\text{dom}(f_m)$  mit  $m$  wächst, können wir annehmen, dass  $m$  gerade ist. Nach Konstruktion von  $f_{m+1}$  ist  $a_n \in \text{dom}(f_{m+1}) \subseteq \text{dom}(f)$ . Ein Widerspruch.  $\square$

**Lemma 3.10.** *Sei  $A$  ein abzählbares Modell von  $T_{\text{random}}$ . Dann folgt eine Aussage  $\varphi$  genau dann aus  $T_{\text{random}}$ , wenn  $\varphi$  in  $A$  gilt.*

*Beweis.* Die Aussage  $\varphi$  folgt genau dann nicht aus  $T_{\text{random}}$ , wenn  $T_{\text{random}} \cup \{\neg\varphi\}$  widerspruchsfrei ist. Nach dem üblichen Beweis des Vollständigkeitsatzes ist letzteres genau dann der Fall, wenn  $T_{\text{random}} \cup \{\neg\varphi\}$  ein abzählbares Modell hat. Da es nach Lemma 3.9 bis auf Isomorphie nur ein abzählbares Modell von  $T_{\text{random}}$  gibt, nämlich  $A$ , ergibt sich, dass  $\varphi$  genau dann nicht aus  $T_{\text{random}}$  folgt, wenn  $\neg\varphi$  in  $A$  gilt. Mit anderen Worten,  $\varphi$  folgt genau dann aus  $T_{\text{random}}$ , wenn  $A$  Modell von  $\varphi$  ist.  $\square$

*Beweis von Satz 3.5.* Nach Lemma 3.6 gelten alle Aussagen in  $T_{\text{random}}$  fast sicher. Nach Lemma 3.3 gelten alle Sätze  $\varphi$ , die aus  $T_{\text{random}}$  folgen, fast sicher.

Nach Lemma 3.10 folgt eine Aussage  $\varphi$  genau dann aus  $T_{\text{random}}$ , wenn  $\varphi$  in dem bis auf Isomorphie eindeutigen abzählbaren Modell  $A$  von  $T_{\text{random}}$  gilt. Da jede Aussage  $\varphi$  in  $A$  entweder wahr oder falsch ist, folgt entweder  $\varphi$  oder  $\neg\varphi$  aus  $T_{\text{random}}$ . Damit ist für jede Aussage  $\varphi$  entweder  $l(\varphi) = 1$  oder  $l(\varphi) = 0$ .  $\square$

Zum Schluss dieses Abschnitts bemerken wir noch, dass Satz 3.5 auch relativ zur Klasse aller Graphen gilt. Dazu fixieren wir ein endliches Vokabular  $\tau$ , das nur Relationssymbole enthält, darunter mindestens ein zweistelliges Relationssymbol  $E$ . Ein  $\tau$ -Struktur  $G$  ist ein  $\tau$ -**Graph**, falls  $G$  die Aussage  $\psi$  erfüllt, wobei

$$\psi := \forall x \neg E(x, x) \wedge \forall x \forall y (E(x, y) \rightarrow E(y, x))$$

sei.

**Satz 3.11.** *Sei  $H$  die Klasse aller  $\tau$ -Graphen. Dann gilt für jede  $\tau$ -Aussage  $\varphi$  entweder  $l(\varphi|H) = 0$  oder  $l(\varphi|H) = 1$ .*

*Beweis.* Der Beweis von Satz 3.5 geht im wesentlichen auch in diesem Fall durch. Man muss allerdings diejenigen Erweiterungsaxiome weglassen, die der Symmetrie von  $E$  widersprechen, die also für gewisse  $x$  und  $y$  gleichzeitig  $E(x, y)$  und  $E(y, x)$  fordern. Außerdem muss man diejenigen Erweiterungsaxiome weglassen, die für gewisse  $x$  die Relation  $E(x, x)$  fordern. Insgesamt betrachtet man also genau die Menge der Erweiterungsaxiome, die mit  $\psi$  vereinbar sind.

Wie oben kann man zeigen, dass es genau einen abzählbaren  $\tau$ -Graphen gibt, der Modell dieser etwas ausgedünnten Menge von Erweiterungsaxiomen ist. Außerdem kann man zeigen, dass diejenigen Erweiterungsaxiome, die  $\psi$  vereinbar sind, in fast allen  $\tau$ -Graphen gelten.  $\square$

Besteht  $\tau$  nur aus dem zweistelligen Relationssymbol  $E$ , so nennt man das bis auf Isomorphie eindeutige abzählbare Modell der mit  $\psi$  vereinbaren Erweiterungsaxiome den **Zufallsgraphen**.

Diejenigen Aussagen über Graphen, die in fast allen Graphen gelten, sind also genau die Aussagen, die im Zufallsgraphen gelten.

#### 4. TURING-MASCHINEN, KOMPLEXITÄTSKLASSEN UND DER SATZ VON TRAHTENBROT

In dem folgenden Abschnitt werden wir die Zusammenhänge zwischen endlicher Modelltheorie und Komplexitätstheorie studieren. Berechnungen führen wir dabei mit Hilfe von **Turing-Maschinen** aus.

Wir fixieren ein endliches Alphabet  $A$ . Eine Turing-Maschine  $M$  ist eine “Maschine” bestehend aus endlich vielen Zuständen, einem nach links und rechts unendlichem Band, das in einzelne Zellen unterteilt ist, und einem Schreib-/Lesekopf der jeweils eine Zelle des Bandes lesen oder beschreiben kann. Jede Zelle des Bandes enthält entweder genau ein Zeichen des Alphabets  $A$  oder ein festes Leerzeichen. Das Band hat eine ausgezeichnete Zelle, die Startzelle.

Unter den Zuständen von  $M$  befinden sich drei ausgezeichnete Zustände: Der Anfangszustand  $s_0$ , der ablehnende Zustand  $s_-$  und der annehmende Zustand  $s_+$ .

Zu der Maschine  $M$  gehört auch eine Übergangsfunktion, die für das Zeichen in der Zelle des Bandes, auf der der Schreib/Lesekopf gerade steht, und den aktuellen Zustand, in dem die Maschine sich befindet, angibt, in welchen Zustand sich die Maschine als nächstes begibt, welches Zeichen (aus  $A$  zusammen mit dem Leerzeichen) an der aktuellen Stelle auf das Band geschrieben wird und ob der Schreib/Lesekopf auf der aktuellen Zelle stehen bleibt, sich eine Zelle nach links bewegt oder sich eine Zelle nach rechts bewegt.

Sei nun  $w$  ein Wort über  $A$ , d.h., eine endliche Folge der Zeichen aus dem Alphabet  $A$ . Wir schreiben  $w$ , beginnend bei der Startzelle des Bandes, von links nach rechts auf das Band (die einzelnen Zeichen in aufeinanderfolgende Zellen). Der Rest des Bandes bleibt leer (also gefüllt mit Leerzeichen). Wir sagen, dass  $w$  die **Eingabe** der Maschinen  $M$  ist. Nun wird  $M$  im Startzustand gestartet. Der Kopf befindet sich dabei auf der Startzelle. Von nun an rechnet  $M$  schrittweise und verfährt in jedem Schritt, wie es die Übergangsfunktion vorschreibt. Gelangt  $M$  dabei in den Zustand  $s_-$  oder  $s_+$ , so stoppt die Maschine.

$M$  **akzeptiert** das Wort  $w$ , falls  $M$  irgendwann (nach endlich vielen Schritten) in den Zustand  $s_+$  gelangt.  $M$  **lehnt  $w$  ab**, falls  $M$  irgendwann in den Zustand  $s_-$  gelangt. Was eben beschrieben wurde, ist eine **deterministische** Turingmaschine.

Im Unterschied zum deterministischen Fall gehört zu einer **nicht-deterministischen** Turing-Maschine anstelle einer Übergangsfunktion eine Übergangsrelation, die für das Zeichen in der aktuellen Zelle des Bandes und den aktuellen Zustand verschiedene Kombinationen aus nächstem Zustand, Zeichen, das auf das Band geschrieben werden soll, und Kopfbewegung liefert. Im Unterschied zur deterministischen Maschine wird bei einer nicht-deterministischen in jedem Arbeitsschritt eine der von der Übergangsrelation erlaubten Möglichkeiten weiter zu rechnen ausgewählt, mit der dann die Rechnung fortgesetzt wird. Wieder stoppt die Maschine, wenn der Zustand  $s_-$  oder  $s_+$  erreicht wird.

Eine nicht-deterministische Turing-Maschine  $M$  akzeptiert ein Wort  $w$ , falls es eine Berechnung der Maschine gibt, die im Zustand  $s_+$  endet.  $M$  lehnt  $w$  ab, falls jede Berechnung im Zustand  $s_-$  endet. Man beachte, dass im deterministischen Fall Akzeptieren und Ablehnen eines Wortes symmetrisch definiert sind, nicht jedoch im nicht-deterministischen Fall.

Sei  $L$  eine **Sprache** über  $A$ , also eine Menge von Wörtern über  $A$ . Eine (deterministische oder nicht-deterministische) Turing-Maschine  $M$  entscheidet  $L$ , falls  $M$  alle Wörter in  $L$  akzeptiert und alle anderen Wörter ablehnt.

Für eine Turing-Maschine  $M$  (ob deterministisch oder nicht) und eine Funktion  $f : \mathbb{N} \rightarrow \mathbb{N}$  sagen wir, dass  $M$   **$f$ -zeitbeschränkt** ist, falls es für jedes Wort  $w$  der Länge  $n$ , das von  $M$  akzeptiert wird, eine Berechnung von  $M$  mit Eingabe  $w$  gibt, die im Zustand  $s_+$  endet und nicht mehr als  $f(n)$  Rechenschritte benötigt.

Die Komplexitätsklasse  $P$  (beziehungsweise  $NP$ ) ist die Klasse aller Sprachen  $L$  über  $A$ , für die ein Polynom  $p(x)$  mit positiven ganzzahligen Koeffizienten und eine deterministische (beziehungsweise nicht-deterministische) Turing-Maschine  $M$  existieren, so dass  $M$  die Sprache  $L$  entscheidet und  $p$ -zeitbeschränkt ist.

Das **Komplement** einer Sprache  $L$  über  $A$  ist die Menge aller Wörter über  $A$ , die nicht in  $L$  liegen. Die Komplexitätsklasse  $co-NP$  ist die Klasse der Komplemente der Sprachen in  $NP$ . Da Akzeptanz und Ablehnung im deterministischen Fall symmetrisch zueinander sind, liegt eine Sprache genau dann in  $P$ , wenn ihr Komplement in  $P$  liegt. Man kann also  $co-P$  analog zu  $co-NP$  definieren, es gilt dann aber  $co-P = P$ .

Das populärste offene Problem der Komplexitätstheorie ist die Frage, ob  $P = NP$  gilt. Ein weiteres offenes Problem ist die Frage, ob  $co-NP = NP$  gilt. Wegen  $co-P = P$  impliziert eine negative Antwort auf die letzte Frage sofort  $P \neq NP$ .

Für eine gegebene Sprache  $L$  über  $A$  ist es nicht klar, ob es überhaupt eine Turing-Maschine gibt, die  $L$  entscheidet. In der Tat kann man leicht zeigen, dass es nur abzählbar viele Turing-Maschinen gibt, aber überabzählbar viele Sprachen. Insbesondere gibt es eine Sprache, die nicht von einer Turing-Maschine entschieden wird.

Ein konkretes Beispiel für eine solche Sprache liefert das **Halteproblem**, also die Aufgabe, für eine gegebene (deterministische) Turing-Maschine  $M$  zu entscheiden, ob  $M$  anhält, wenn man  $M$  mit dem leeren Band startet. Dazu kodiert man jede Turing-Maschine  $M$  in geeigneter Weise als Wort  $w_M$  über  $A$ . Sei

$$L := \{w_M : M \text{ ist eine Turing-Maschine, die} \\ \text{anhält, wenn man sie mit leerem Band startet}\}.$$

Es gibt keine Turing-Maschine, die die Sprache  $L$  entscheidet: Angenommen doch. Dann gibt es auch eine Turing-Maschine  $M$ , die für jede Turing-Maschine  $N$  das Wort  $w_N$  akzeptiert, wenn  $N$  bei der Eingabe von  $w_N$  anhält, und sonst ablehnt. Aus  $M$  läßt sich nun eine Turing-Maschine  $M'$  konstruieren, die für jede Turing-Maschine  $N$  genau dann bei der Eingabe  $w_N$  anhält, wenn  $N$  bei der Eingabe von  $w_N$  nicht anhält. Wir starten nun  $M'$  mit der Eingabe  $w_{M'}$ . Nach Konstruktion hält  $M'$  bei Eingabe von  $w_{M'}$  genau dann, wenn  $M'$  bei der Eingabe von  $w_{M'}$  nicht anhält. Ein Widerspruch.

Zusammenhänge zwischen endlicher Modelltheorie und Komplexitätstheorie bestehen in zwei Richtungen: Zum einen kann man für eine gegebene, sinnvoll definierte Klasse  $K$  endlicher Strukturen fragen, wie lange es dauert für eine endliche Struktur  $A$  zu entscheiden, ob  $A$  in  $K$  liegt oder nicht. Ein Spezialfall davon ist das sogenannte **model checking**. Für einen gegebenen Satz  $\varphi$  (in erststufiger Logik oder auch in einer der höheren Logiken, die wir später betrachten werden) fragt man, ob eine endliche Struktur  $A$  Modell von  $\varphi$  ist.

Andererseits kann man Berechnungen von Turing-Maschinen mittels endlicher Strukturen simulieren. Das liefert unter anderem Sätze vom Typ “wenn sich die Zugehörigkeit einer Struktur zu einer Klasse  $K$  endlicher Strukturen schnell entscheiden läßt, so läßt sich die Klasse  $K$  einfach axiomatisieren”. (Mit “Axiomatisieren” ist hierbei nicht unbedingt Axiomatisieren durch eine erststufige Formel gemeint.)

Ein Beispiel der Simulation von Berechnungen von Turing-Maschinen durch endliche Strukturen ist der folgende Beweis des Satzes 1.6 von Trahtenbrot. Der Beweis beruht auf folgendem Lemma.

**Lemma 4.1.** *Für ein gewisses Vokabular  $\sigma(A)$  ist die Sprache*

$$\text{Sat}(\sigma(A)) := \{\varphi : \varphi \text{ ist eine erststufige Aussage über } \sigma(A), \\ \text{die ein endliches Modell hat}\}$$

*nicht entscheidbar.*

Bevor wir dieses Lemma beweisen, leiten wir daraus den Satz von Trahtenbrot her. Zunächst mache man sich klar, dass sich jede Struktur  $A$  in einem Vokabular  $\sigma$  so als Graph codieren läßt (in berechenbarer Weise), dass es zu jeder Aussage  $\varphi$  eine Aussage  $\varphi'$  gibt, so dass für jeden Graphen  $G$  entscheidbar ist, ob  $G$  die Struktur  $A$  codiert, und so dass gilt:

$$G \models \varphi' \Leftrightarrow G \text{ codiert eine Struktur } A \text{ mit } A \models \varphi$$

Mit Hilfe dieser Codierung sehen wir, dass für jedes Vokabular  $\tau$ , das mindestens ein zweistelliges Relationssymbol enthält, die Sprache

$$\text{Sat}(\tau) = \{\varphi : \varphi \text{ ist eine erststufige Aussage über } \tau, \text{ die ein endliches Modell hat}\}$$

nicht entscheidbar ist.

Andererseits ist die Sprache  $\text{Sat}(\tau)$  aber rekursiv aufzählbar. Man braucht nur alle Paare  $(A, \varphi)$  aufzuzählen und zu testen, ob  $A$  Modell von  $\varphi$  ist. Wenn ja, so gibt man  $\varphi$  aus.

Eine Aussage  $\varphi$  gilt genau dann in allen endlichen Strukturen, wenn  $\neg\varphi$  nicht in  $\text{Sat}(\tau)$  liegt. Wäre nun die Menge aller Aussagen über  $\tau$ , die in allen endlichen Strukturen gilt, rekursiv aufzählbar, so könnte man auch für jede Aussage  $\varphi$  entscheiden, ob  $\varphi$  in allen endlichen Strukturen gilt.

Man zähle nämlich einfach parallel  $\text{Sat}(\tau)$  und die Menge der Aussagen, die in allen endlichen Strukturen war sind, auf und warte bis in der ersten Aufzählung  $\neg\varphi$  oder in der zweiten  $\varphi$  erscheint. Das beweist den Satz von Trahtenbrot.

*Beweis von Lemma 4.1.* Das Vokabular  $\sigma(A)$  wird sich aus dem folgenden Beweis ergeben. Wir führen die Nichtentscheidbarkeit von  $\text{Sat}(\sigma(A))$  auf das Halteproblem zurück. Dazu geben wir für jede Turing-Maschine  $M$  eine Aussage  $\varphi_M$  an, die genau dann ein endliches Modell hat, wenn  $M$  anhält, wenn man die Maschine mit dem leeren Band startet. Es ist dann klar, dass die Nichtentscheidbarkeit des Halteproblems die Nichtentscheidbarkeit von  $\text{Sat}(\sigma(A))$  impliziert.

Sei also  $M$  eine Turing-Maschine. Wir können annehmen, dass die Zustände von  $M$  genau die Zahlen  $0, \dots, s_M$  sind, wobei 0 der Startzustand ist, 1 der akzeptierende Zustand und 2 der ablehnende Zustand. Die Zellen des Bandes von  $M$  seien mit ganzen Zahlen indiziert, wobei die Zelle mit der Nummer 0 die Startposition des Kopfes ist. Falls  $M$  mindestens  $n$  Schritte rechnet (nachdem man  $M$  mit leerem Band startet), so sei  $C_n$  die **Konfiguration** von  $M$  nach  $n$  Rechenschritten.  $C_n$  enthält folgende Informationen: Den aktuellen Zustand, die aktuelle Position des Kopfes und den aktuellen Bandinhalt.

Das Vokabular  $\sigma(A)$  enthalte das einstellige Relationssymbol  $\text{Start}$ , die zwei-stelligen Relationssymbole  $<$ ,  $\text{Zustand}$  und  $\text{Kopf}$ , sowie für jedes Zeichen  $a \in A \cup \{\text{Leerzeichen}\}$  ein zweistelliges Relationssymbol  $\text{Zeichen}_a$ .

Für jedes  $n \geq s_M$  definieren wir eine Struktur  $B_n$  mit der unterliegenden Menge  $\{-n, \dots, n\}$ , so dass  $B_n$  das Anfangsstück  $C_0, \dots, C_n$  der Berechnung von  $M$  beschreibt (beziehungsweise  $C_0, \dots, C_k$ , falls es ein  $k < n$  gibt, so dass  $M$  nach  $k$  Schritten anhält). Die Interpretation von  $<$  in der Struktur  $B_n$  sei einfach die natürliche Ordnung der Zahlen  $-n, \dots, n$ . Das Prädikat  $\text{Start}$  treffe nur auf 0 zu.

Für  $s, t \in \{0, \dots, n\}$ ,  $i \in \{-n, \dots, n\}$  und alle Zeichen  $a$  sei

$$\begin{aligned} \text{Zustand}^{B_n}(s, t) &:\Leftrightarrow \text{ Gemäß } C_t \text{ befindet sich } M \text{ im Zustand } s \\ \text{Kopf}^{B_n}(i, t) &:\Leftrightarrow \text{ Gemäß } C_t \text{ befindet sich der Kopf auf Zelle } i \\ \text{Zeichen}_a^{B_n}(i, t) &:\Leftrightarrow \text{ Gemäß } C_t \text{ steht in Zelle } i \text{ das Zeichen } a. \end{aligned}$$

Wir geben nun eine Aussage  $\varphi_M$  an, die folgende Eigenschaften hat:

- (i) Falls  $M$ , mit leerem Band gestartet, nach  $k$  Schritten anhält und falls  $n \geq \max(k, s_M)$  ist, so gilt  $B_n \models \varphi_M$ .
- (ii) Falls  $B$  ein Model von  $\varphi_M$  ist und  $M$ , mit leerem Band gestartet, mindestens  $k$  Schritte rechnet, so gilt  $|B| \geq k$ .

Jede Aussage  $\varphi$ , die (i) und (ii) erfüllt, hat genau dann ein endliches Modell, wenn  $M$ , auf dem leerem Band gestartet, anhält.

Die Aussage  $\varphi_M$  sei die Konjunktion folgender Sätze (die wir, der besseren Lesbarkeit halber, umgangssprachlich aufschreiben):

- (1)  $<$  ist eine lineare Ordnung und genau ein Element erfüllt das Prädikat Start. (Wir nennen das Element, welches das Prädikat Start erfüllt, in Zukunft 0. Jede natürliche Zahl  $t$  können wir dann einfach mit dem  $t$ -ten Nachfolger (bezüglich  $<$ ) von 0 identifizieren, falls der  $t$ -te Nachfolger von 0 in der Struktur existiert. Analog interpretieren wir negative Zahlen in der Struktur.)
- (2) Es gibt mindestens  $s_M + 1$  verschiedene Elemente.
- (3) Nach 0 Rechenschritten befinden wir uns im Zustand 0, der Kopf steht auf der Zelle 0 und das Band ist leer.
- (4) Zu jedem Zeitpunkt gibt es genau einen aktuellen Zustand und eine aktuelle Kopfposition. Zu jedem Zeitpunkt steht in jeder Zelle des Bandes genau ein Zeichen (wobei auch das Leerzeichen erlaubt ist).
- (5) Wenn  $M$  aus dem Zustand  $s$  bei aktuellem Zelleninhalt  $a$  in den Zustand  $s'$  übergeht, das Zeichen  $b$  auf das Band schiebt und die Kopfposition um den Wert  $h \in \{0, 1, -1\}$  ändert, so gilt entsprechendes in der Struktur, d.h., für alle  $y$  und alle  $t$  gilt:

$$\text{Zustand}(s, t) \wedge \text{Kopf}(y, t) \wedge \text{Zeichen}_a(y, t)$$

impliziert

$$\text{Zustand}(s', t + 1) \wedge \text{Zeichen}_b(y, t + 1) \wedge \text{Kopf}(y + h, t + 1).$$

Dabei stehen  $t + 1$  und  $y + h$  für die Elemente der Struktur mit den naheliegenden Beschreibungen.

- (6) Sei 1 der Nachfolger von 0 bezüglich  $<$  und 2 der Nachfolger von 1. Dann existiert ein Element  $t > 0$  mit Zustand(1,  $t$ ) oder Zustand(2,  $t$ ). Die Berechnung endet also irgendwann.

Es ist klar, dass  $\varphi_M$  die Eigenschaften (i) und (ii) hat. □

Dieser Beweis zeigt, wie man Berechnungen von Turing-Maschinen mit Hilfe endlicher Strukturen beschreiben kann. Als nächstes werden wir sehen, wie sich endliche Strukturen mit Hilfe von Turing-Maschinen analysieren lassen. Der Einfachheit halber beschränken wir uns auf geordnete Strukturen.

Sei  $\tau_1$  ein endliches Vokabular, das nur Relations- und Konstantensymbole enthält, und zwar  $k$  Relationssymbole und  $l$  Konstantensymbole. Weiter sei  $\tau_0$  das Vokabular, das nur das zweistellige Relationssymbol  $<$  enthält. Schließlich sei  $\tau := \tau_0 \cup \tau_1$ . Alle  $\tau$ -Strukturen, die wir im Folgenden betrachten, seien durch  $<$  linear geordnet. Für eine Struktur  $A$  mit  $|A| = n$  können wir also annehmen, dass die unterliegende



Menge von  $A$  genau die Menge  $\{0, \dots, n-1\}$  ist und dass die Ordnung  $<$  auf  $A$  einfach die natürliche Ordnung der Zahlen  $0, \dots, n-1$  ist.

Wir wollen nun  $\tau$ -Strukturen in Turing-Maschinen eingeben. Wir benutzen Turing-Maschinen mit  $k+l+1$  Eingabebändern, auf die nichts geschrieben wird, und  $m$  Arbeitsbändern (für ein gewisses  $m$ ), die wie gewohnt beschrieben werden können. Man kann sich überlegen, dass sich Turing-Maschinen mit mehreren Bändern durch Maschinen mit nur einem Band simulieren lassen und dass die Definition der Klassen P und NP nicht davon abhängt, wieviele Bänder die Maschinen zu Verfügung haben.

Das Alphabet unserer Turing-Maschinen besteht aus 0 und 1. Zusätzlich gibt es, wie üblich, ein Leerzeichen. Sei nun  $B$  eine  $\tau$ -Struktur. Wir geben  $B$  wie folgt in eine Turing-Maschine ein:

Auf das erste Band wird, beginnend bei der Startzelle, nach rechts eine Folge von 1-en der Länge  $n := |B|$  geschrieben. Für  $i \leq k$  wird auf das  $(i+1)$ -te Eingabeband die  $i$ -te Relation  $R_i^B$  geschrieben, und zwar in folgendem Format:

Angenommen  $R_i^B$  ist  $r$ -stellig, also  $R_i^B \subseteq B^r$ . Für  $j < n^r$  enthalte die  $j$ -te Zelle des Bandes genau dann eine 1, wenn das  $j$ -te  $r$ -Tupel von  $B^r$  (bezüglich der lexicographischen Ordnung auf  $B^r$ ) Element von  $R_i^B$  ist. Sonst enthalte die  $j$ -te Zelle des Bandes eine 0.

Für  $j \leq l$  wird die Interpretation der  $j$ -ten Konstante auf das  $(k+j+1)$ -te Eingabeband geschrieben, und zwar in Binärdarstellung ohne führende Nullen.

Nun ist klar, wie eine Struktur  $B$  in eine Turing-Maschine eingegeben wird. Die Maschine wird mit dieser Eingabe und leeren Arbeitsbändern gestartet. Und akzeptiert die Struktur, lehnt die Struktur ab oder rechnet ewig weiter. Es ist klar, wann eine Klasse  $K$  endlicher Strukturen von einer Turing-Maschine  $M$  entschieden wird. Es ist auch klar, wann eine Klasse  $K$  endlicher Strukturen in den Komplexitätsklassen P oder NP liegt und wann nicht. (Zumindest sollte klar sein, wie die entsprechenden Definitionen lauten.)

## 5. ZWEITSTUFIGE LOGIK UND DIE KOMPLEXITÄT VON MODEL CHECKING

**5.1. Erststufige Logik.** Wir zeigen, dass für eine gegebene erststufige Aussage  $\varphi$  (über irgendeinem Vokabular) das Problem, festzustellen, ob eine vorgelegte Struktur  $A$  Modell von  $\varphi$  ist, in der Klasse P liegt.

Man kann sich leicht überlegen, dass es genügt, Vokabulare zu betrachten, die nur Relationssymbole enthalten. Aus technischen Gründen werden wir jedoch Vokabulare mit Konstanten- und Relationssymbolen, aber ohne Funktionssymbole betrachten. Sei also  $\tau$  ein solches Vokabular (endlich).

**Lemma 5.1.** *Für jede erststufige Aussage  $\varphi$  über  $\tau$  existiert eine deterministische Turing-Maschine, zeitbeschränkt durch ein Polynom, das von  $\varphi$  abhängt, die für jede  $\tau$ -Struktur  $A$  entscheidet, ob  $A$  Modell von  $\varphi$  ist.*

*Mit anderen Worten, die Modellklasse von  $\varphi$  liegt in P.*

*Beweis.* Wir führen den Beweis durch Induktion über den Formelaufbau. Die zu untersuchende Struktur  $A$  wird in irgendeiner Turing-Maschine eingegeben wie im letzten Abschnitt beschrieben.

Auch wenn im Lemma nur von Aussagen die Rede ist, müssen wir in der Induktion Formeln mit freien Variablen, die mit irgendwelchen Elementen aus der Struktur belegt sind, berücksichtigen. Es ist aber klar, dass sich Formeln mit freien Variablen, die mit Elementen der Struktur belegt sind, genauso behandeln lassen, wie Aussagen, in denen entsprechende Konstanten vorkommen.

Das setzt natürlich voraus, dass in dem Vokabular die entsprechenden Konstantensymbole vorhanden sind. Da wir jedoch von einem festen, aber (im wesentlichen) beliebigen Vokabular ausgehen, bereitet das keine Probleme. Es genügt also, die einzelnen Schritte der Induktion für Aussagen zu beweisen.

Zunächst die trivialen Fälle: um die Gültigkeit Boolescher Kombinationen erststufiger Aussagen in einer Struktur festzustellen, muss man zunächst die Gültigkeit der einzelnen Aussagen, die Boolesch kombiniert werden, untersuchen. Das geht jeweils in polynomieller Zeit, nach Induktionsvoraussetzung. Die Zeit, die dann noch zum Auswerten des Booleschen Ausdrucks benötigt wird, hängt nicht mehr von der Größe untersuchten Struktur ab, sondern nur von der Komplexität des Booleschen Ausdrucks.

Als nächstes betrachten wir atomare Aussagen, also Aussagen von der Form  $R(c_1, \dots, c_r)$ , wobei  $R$   $r$ -stelliges Relationssymbol ist und  $c_1, \dots, c_r$  Konstantensymbole sind.

Um zu testen, ob das  $r$ -Tupel  $(c_1^A, \dots, c_r^A)$  in  $R^A$  liegt, kann man wie folgt vorgehen: auf dem Eingabeband, das für die Relation  $R$  zuständig ist, läuft man, bei der Startzelle beginnend, schrittweise nach rechts. In jedem Schritt wird ein  $n$ -Tupel von Zahlen zwischen 0 und  $n - 1$ , wobei  $n$  die Mächtigkeit der untersuchten Struktur ist, lexicographisch um 1 hochgezählt (in Binärdarstellung). Dann wird mit den Werten der Konstanten  $c_1, \dots, c_r$  verglichen, die auf den entsprechenden Eingabebändern in Binärdarstellung vorliegen.

Ist das Tupel  $(c_1^A, \dots, c_r^A)$  erreicht, sieht man nach, ob an der entsprechenden Stelle des Eingabebandes für die Relation  $R$  eine 1 steht. Wenn ja, dann gilt  $R(c_1, \dots, c_r)$  in der untersuchten Struktur  $A$ , sonst nicht. Der Zeitaufwand dieser Berechnung ist proportional zu  $n^r$ , ein Polynom in der Mächtigkeit der eingegebenen Struktur. (Der Zeitaufwand für diese Berechnung ist linear in der Gesamtlänge der Eingabe der Turingmaschine, also in der Länge der Codierung der untersuchten Struktur.)

Um schließlich die Gültigkeit einer Existenzaussage  $\exists x\varphi(x)$  zu festzustellen, durchläuft man einfach alle Elemente  $a$  der zu untersuchenden Struktur  $A$  und bestimmt den Wahrheitswert von  $\varphi(a)$  in  $A$ . Letzteres geht nach Voraussetzung in

polynomieller Zeit. Um alle Elemente der Struktur zu durchlaufen, benötigt man offenbar  $n = |A|$  Schritte. Der Zeitaufwand bleibt also insgesamt polynomiell. (Ist die Bestimmung des Wahrheitswertes von  $\varphi(a)$   $p(n)$ -zeitbeschränkt, so ist die Bestimmung des Wahrheitswertes von  $\exists x\varphi(x)$   $(n \cdot p(n))$ -zeitbeschränkt.)  $\square$

Man beachte, dass es mehr Klassen endlicher Strukturen in  $P$  gibt, als es erststufig axiomatisierbare Klassen gibt. Ein Beispiel ist die Klasse aller endlichen Strukturen mit einer geraden Anzahl von Elementen über einer beliebigen (aber natürlich festen) Signatur. Wir werden später sehen, wie sich die Klassen in  $P$  mit Hilfe einer abgeschwächten zweitstufigen Logik charakterisieren lassen.

**5.2. Zweitstufige Logik.** Zweitstufige Logik unterscheidet sich von der erststufigen dadurch, dass auch Quantifikation über Relationen erlaubt ist. Dadurch büßt man zwar viele gute Eigenschaften der erststufigen Logik ein, gewinnt aber drastisch an Ausdrucksstärke.

Sei  $\tau$  ein endliches Vokabular. Wir definieren, was eine **zweitstufige Formel** über  $\tau$  ist. Zunächst sind alle erststufigen  $\tau$ -Formeln auch zweitstufige Formeln. Boolesche Kombinationen zweitstufiger Formeln sind wieder zweitstufige Formeln. Ist  $\varphi(x)$  eine zweitstufige Formel, so auch  $\exists x\varphi(x)$ , wobei  $x$  eine **Individuenvariable** ist, also eine Variable wie in der erststufigen Logik.

Zusätzlich zu den Individuenvariablen gibt es auch **zweitstufige Variablen** verschiedener Stelligkeit, die für Relationen stehen. Um Konflikte zu vermeiden, vereinbaren wir, dass zweitstufige Variablen immer so gewählt werden, dass sie nicht Elemente von  $\tau$  sind.

Ist  $X$  eine  $n$ -stellige zweitstufige Variable, so ist für jede zweitstufige Formel  $\varphi$  über dem Vokabular  $\tau \cup \{X\}$ , wobei  $X$  jetzt als  $n$ -stelliges Relationssymbol aufgefasst wird, die Formel  $\exists X\varphi$  eine zweitstufige Formel über dem Vokabular  $\tau$ .

Die Gültigkeit einer zweitstufigen  $\tau$ -Formel  $\varphi$  in einer  $\tau$ -Struktur  $A$  wird wie folgt erklärt:

Ist  $\varphi$  erststufig, so gilt  $\varphi$ , aufgefasst als zweitstufige Formel, in  $A$  genau dann, wenn  $\varphi$ , aufgefasst als erststufige Formel, in  $A$  gilt. Ist  $\varphi$  eine Boolesche Kombination zweitstufiger Formeln, so ist die Definition der Gültigkeit von  $\varphi$  in  $A$  die naheliegende. Ist  $\varphi$  von der Form  $\exists x\psi(x)$ , wobei  $x$  eine Individuenvariable ist, so gilt  $\varphi$  in  $A$  genau dann, wenn es ein  $a \in A$  gibt, so dass  $\psi(a)$  in  $A$  gilt. Ist  $\varphi$  von der Form  $\exists X\psi$ , wobei  $X$  eine  $n$ -stellige zweitstufige Variable ist und  $\psi$  eine zweitstufige Formel über  $\tau \cup \{X\}$ , so gilt  $\varphi$  genau dann in  $A$ , wenn es eine  $n$ -stellige Relation  $X^A$  auf  $A$  gibt, so dass  $\psi$  in  $(A, X^A)$  gilt.

Gilt die zweitstufige Formel  $\varphi$  in  $A$ , so schreiben wir  $A \models \varphi$ .

**Lemma 5.2.** *Seien  $X_1, \dots, X_n$  zweitstufige Variablen und  $\varphi$  eine erststufige Formel über dem Vokabular  $\tau \cup \{X_1, \dots, X_n\}$ . Dann ist die Klasse aller endlichen  $\tau$ -Strukturen  $A$  mit  $A \models \exists X_1 \dots \exists X_n \varphi$  in NP.*

*Beweis.* Wir benutzen eine nicht-deterministische Turing-Maschine mit  $n$  zusätzlichen Arbeitsbändern, die jeweils für eine der zweitstufigen Variablen  $X_1, \dots, X_n$  zuständig sind. Für jedes  $k \in \{1, \dots, n\}$  sei  $r_k$  die Stelligkeit von  $X_k$ .

Wir geben die Struktur  $A$  ein. Zunächst schreibt die Maschine für jedes  $k \in \{1, \dots, n\}$  auf das für  $X_k$  zuständige Band eine zufällige Folge von Nullen und Einsen der Länge  $|A|^{r_k}$ . (Mit "zufällig" ist hierbei eigentlich "auf nicht-deterministische Weise" gemeint. Jede Folge muss möglich sein.) Das geht in polynomieller Zeit (in Abhängigkeit von  $|A|$ ).

Dann benutzt die Maschine die für die  $X_k$  zuständigen Bänder als zusätzliche Eingabebänder und entscheidet (wieder in polynomieller Zeit) ob  $(A, X_1^A, \dots, X_n^A)$  Modell von  $\varphi$  ist, wobei  $X_k^A$  jeweils die Relation ist, deren charakteristische Funktion auf dem für  $X_k$  zuständigen Band steht.  $\square$

**5.3. Der Satz von Fagin.** Wieder sei  $\tau$  ein endliches Vokabular, das nur Relations- und Konstantensymbole enthält. In diesem Abschnitt beweisen wir die Umkehrung von Lemma 5.2, nämlich

**Lemma 5.3.** *Sei  $K$  eine Klasse endlicher  $\tau$ -Strukturen, die in NP liegt. Dann existiert eine zweistufige Formel  $\varphi$  der Form  $\exists X_1 \dots \exists X_k \psi$ , wobei  $\psi$  eine erststufige Formel in  $\tau \cup \{X_1, \dots, X_k\}$  ist, so dass  $K$  genau die Modellklasse von  $\varphi$  ist.*

Zusammen mit Lemma 5.2 erhält man sofort

**Satz 5.4 (Fagin).** *Eine Klasse  $K$  endlicher  $\tau$ -Strukturen liegt genau dann in NP, wenn sich  $K$  durch eine zweistufige Formel der Form  $\exists X_1 \dots \exists X_k \varphi$ , wobei  $\varphi$  erststufig ist, axiomatisieren lässt.*

*Beweis von Lemma 5.3.* Sei  $K$  eine Klasse endlicher  $\tau$ -Strukturen, die in NP liegt. Dann existieren eine nicht-deterministische Turing-Maschine  $M$  und ein Polynom  $p(x)$ , so dass  $M$  die Klasse  $K$  entscheidet und bei Eingabe einer  $\tau$ -Struktur  $A$  der Mächtigkeit  $n$  höchstens  $p(n)$  Schritte rechnet. Ist  $r$  größer als der Grad von  $p$ , so rechnet  $M$  für alle bis auf endlich viele Strukturen  $A$  bei Eingabe von  $A$  höchstens  $|A|^r$  Schritte. Die endliche Klasse der Strukturen  $A \in K$ , bei deren Eingabe  $M$  mehr als  $|A|^r$  Schritte rechnet, lässt sich erststufig axiomatisieren. Daher können wir annehmen, dass  $M$  für jede Eingabe  $A$  höchstens  $|A|^r$  Schritte rechnet.

Die Eingabe einer Struktur  $A$  in  $M$  erfolgt wie in Abschnitt 4 erklärt. Man erinnere sich, wie die Maschine gestartet wird: die Eingabebänder enthalten die Informationen über die Struktur  $A$ , das Arbeitsband ist leer. Bekanntlich kann man davon ausgehen, dass  $M$  zunächst in nicht-determinierter Weise eine Folge von Einsen und Nullen auf das Arbeitsband schreibt, dann mit dem Kopf wieder zur Startzelle zurückkehrt und die Berechnung von nun an deterministisch weiter geht.

Eine bequeme Modifikation davon ist folgende: wir gehen von einer deterministischen Maschine  $M$  aus und sagen, dass  $M$  die Struktur  $A$  akzeptiert, wenn es eine Folge von Nullen und Einsen gibt, so dass  $M$ , gestartet mit dieser Folge auf dem Arbeitsband und der Codierung von  $A$  auf den Eingabebändern, schließlich im akzeptierenden Zustand landet.  $M$  lehnt  $A$  ab, wenn  $M$  für jede Folge von Nullen und Einsen auf dem Arbeitsband im ablehnenden Zustand landet. Man beachte, dass  $M$  höchstens  $|A|^r$  Schritte rechnet. Damit werden auch nur  $|A|^r$  Zellen des Arbeitsbandes benutzt. Wir können annehmen, dass keine Zellen des Arbeitsbandes benutzt werden, die links von der Startzelle liegen.

Wir schreiben eine Formel  $\varphi$  auf, die im wesentlichen aussagt, dass es eine Folge der Länge  $|A|^r$ , wobei  $A$  die betrachtete Struktur ist, von Nullen und Einsen gibt, so dass  $M$  die Struktur  $A$  akzeptiert, wenn  $M$  mit dieser Folge auf dem Arbeitsband gestartet wird. Die Berechnung der Maschine  $M$  wird dabei auch durch Relationen auf  $A$  beschrieben.

Man erinnere sich, dass die betrachteten Strukturen als linear geordnet vorausgesetzt wurden. Sei also  $<$  die lineare Ordnung auf  $A$ . Mit Hilfe dieser linearen Ordnung können wir für jedes  $s$  die lexikographische Ordnung  $<^s$  von  $A^s$  definieren, eine  $2s$ -stellige Relation auf  $A$ , die genau dann das  $2s$ -Tupel  $(a_1, \dots, a_s, b_1, \dots, b_s)$  enthält, wenn  $(a_1, \dots, a_s)$  lexikographisch kleiner als  $(b_1, \dots, b_s)$  ist.

Wir benutzen  $A^r$  mit der linearen Ordnung  $<^r$  als

- Menge der Zeitpunkte in der Berechnung,
- Indexmenge der Zellen des Arbeitsbandes,
- Indexmenge der Zellen der einzelnen Eingabebänder (wobei bei wir annehmen, dass  $r$  größer ist als jede Stelligkeit eines Relationssymbols in  $\tau$ ).

Die Konfiguration von  $M$  zum Zeitpunkt  $t$  besteht aus

- (1) den aktuellen Positionen der Köpfe auf den jeweiligen Bändern,
- (2) dem Inhalt des Arbeitsbandes und
- (3) dem aktuellen Zustand.

Angenommen,  $M$  benutzt insgesamt  $l$  Bänder. Die Positionen des  $i$ -ten Kopfes,  $i \in \{1, \dots, l\}$ , beschreiben wir durch eine  $2r$ -stellige Relation  $H_i$ , wobei  $H_i$  genau dann auf  $(t, p) \in A^r \times A^r$  zutrifft, wenn sich der  $i$ -te Kopf zum Zeitpunkt  $t$  auf der Zelle mit Index  $p$  befindet.

Wir nehmen an, dass das Alphabet von  $M$  aus den Zeichen 0, 1 und dem Leerzeichen besteht. Den Inhalt des Arbeitsbandes beschreiben wir durch die  $2r$ -stellige Relationen  $B_0$ ,  $B_1$  und  $B_2$ . Trifft  $B_0$  auf  $(t, z) \in A^r \times A^r$  zu, so bedeutet das, dass zum Zeitpunkt  $t$  in der Zelle mit dem Index  $z$  des Arbeitsbandes eine 0 steht. Analog ist  $B_1$  für die Einsen und  $B_2$  für die Leerzeichen zuständig. Man beachte, dass es nicht nötig ist, den Inhalt der Eingabebänder zu codieren. Das erledigen schon die auf  $A$  ursprünglich vorhandenen Relationen.

$M$  habe  $m$  Zustände. Der aktuelle Zustand wird durch  $r$ -stellige Relationen  $Z_i$ ,  $i \in \{1, \dots, m\}$ , beschrieben. Trifft  $Z_i$  auf  $t \in A^r$  zu, so bedeutet das, dass sich die Maschine zum Zeitpunkt  $t$  im Zustand  $i$  befindet.

Die gesuchte Aussage  $\varphi$  hat die Form

$$\exists H_1 \dots \exists H_l \exists B_0 \dots \exists B_2 \exists Z_1 \dots \exists Z_m \psi.$$

Dabei besagt  $\psi$ , dass die  $H_1, \dots, H_l$ ,  $B_0, \dots, B_2$  und  $Z_1, \dots, Z_m$  entsprechend dem oben Beschriebenen eine akzeptierende Berechnung von  $M$  codieren. Dabei darf der akzeptierende Zustand natürlich bereits vor dem letzten der  $|A|^r$  möglichen Zeitpunkte erreicht sein. Die Formel  $\psi$  konstruiert man im wesentlichen wie im Beweis des Satzes von Trahtenbrot. Man beachte, dass der Inhalt des Arbeitsbandes beim Start der Maschine nicht näher spezifiziert wird. Aber wir hatten ja auch festgelegt, dass  $M$  die Struktur  $A$  akzeptiert, wenn es irgendeinen Bandinhalt gibt, so dass  $M$ , gestartet mit diesem Inhalt des Arbeitsbandes und der Eingabe  $A$ , schließlich im akzeptierenden Zustand landet.

Es ist klar, dass die so konstruierte Formel  $\varphi$  genau die Klasse  $K$  axiomatisiert.  $\square$

**5.4. Least fixed point logic und die Klasse P.** Sei  $\tau$  ein endliches Vokabular ohne Funktionssymbole. Wir wissen bereits, dass alle erststufig axiomatisierbaren Klassen endlicher  $\tau$ -Strukturen in P liegen und dass eine Klasse endlicher  $\tau$ -Strukturen genau dann in NP liegt, wenn sie sich durch eine zweitstufige Formel der Form  $\exists X_1 \dots \exists X_n \varphi$  mit erstufigem  $\varphi$  axiomatisieren lässt.

Wir führen eine Logik ein, die zwischen erst- und zweitstufiger Logik liegt und mit deren Hilfe man genau die Klassen endlicher  $\tau$ -Strukturen, die in P liegen, axiomatisieren kann, **least fixed point logic (LFP-Logik)**. Die LFP-Logik erlaubt es, induktiv definierte Relationen zu verwenden.

Betrachte zum Beispiel das Vokabular  $\sigma = \{E, s, t\}$ , wobei  $E$  ein zweistelliges Relationssymbol ist und  $s$  und  $t$  Konstantensymbole sind. Sei  $G$  irgendeine  $\tau$ -Struktur,  $E = E^G$  die Interpretation von  $E$  in  $G$  und  $s = s^G$  und  $t = t^G$  die Interpretationen von  $s$  beziehungsweise  $t$  in  $G$ .  $E^*$  sei die transitive, reflexive Hülle von  $E$ , also die Relation

$$\{(x, y) \in G^2 : \text{es gibt } n \in \mathbb{N} \text{ und } x_0, \dots, x_n \in G \text{ mit } x = x_0 E x_1 E \dots E x_n = y\}.$$

Wie man leicht nachrechnet ist  $E^*$  die kleinste (bezüglich  $\subseteq$ ) zweistellige Relation auf  $G$ , die  $E$  umfasst. Mit Hilfe von  $E^*$  lässt sich leicht feststellen, ob es in  $G$  einen (gerichteten) Weg von  $s$  nach  $t$  gibt: so ein Weg existiert genau dann, wenn  $(s, t) \in E^*$  gilt.

Zweitstufig könnte man das wie folgt ausdrücken: Für zwei zweistellige Relationssymbole  $R$  und  $S$  sei

$$\varphi(R, S) := \forall x, y (R(x, y) \vee x = y \rightarrow S(x, y)) \wedge \forall x, y, z (S(x, y) \wedge S(y, z) \rightarrow S(x, z)).$$

Die Formel  $\varphi(R, S)$  sagt also, dass die zweistellige Relation  $S$  transitiv und reflexiv ist und die Relation  $R$  umfasst. Weiter sei

$$\psi := \forall R \left( \varphi(E, R) \wedge \forall S \left( \varphi(E, S) \rightarrow \forall x, y (R(x, y) \rightarrow S(x, y)) \right) \rightarrow R(s, t) \right).$$

Man beachte, dass es auf  $G$  genau eine zweistellige Relation  $R$  gibt, die die Prämisse des letzten Implikationspfeils wahr macht, nämlich  $E^*$ . Damit gilt  $G \models \psi$  genau dann, wenn es in  $G$  einen Weg von  $s$  nach  $t$  gibt.

Die LFP-Logik erlaubt es zum Beispiel die Relation  $E^*$  zu benutzen, wenn man  $E$  schon kennt, ohne dass man die volle Ausdruckskraft der zweitstufigen Logik gewinnt.

Sei  $R$  ein zweistelliges Relationssymbol. Betrachte die Formel

$$\varphi(R, x, y) := x = y \vee \exists z (E(x, z) \wedge R(z, y)).$$

Zu jeder zweistelligen Relation  $R$  auf  $G$  liefert  $\varphi$  eine neue Relation

$$\varphi^G(R) = \{(x, y) \in G^2 : G \models \varphi(R, x, y)\}.$$

Wie man leicht sieht, gilt für alle zweistelligen Relationen  $R$  und  $S$  mit  $R \subseteq S$  auch  $\varphi^G(R) \subseteq \varphi^G(S)$ . Diese Eigenschaft von  $\varphi^G$  hängt nicht von der Struktur  $G$  ab. Daher nennt man die Formel  $\varphi$  **monoton**.

Die Relation  $E^*$  ist ein **Fixpunkt** von  $\varphi^G$ , d.h., es gilt  $\varphi^G(E^*) = E^*$ . Ausserdem ist  $E^*$  der kleinste Fixpunkt von  $\varphi^G$ . Die Existenz eines kleinsten Fixpunktes ist kein Zufall.

**Lemma 5.5.** *Sei  $R$  ein  $k$ -stelliges Relationssymbol und  $\varphi(R, x_1, \dots, x_k)$  eine monotone erststufige Formel über  $\tau \cup \{R\}$ . Für jede endliche  $\tau$ -Struktur  $A$  existiert ein kleinster Fixpunkt der Abbildung  $\varphi^A$ , die  $k$ -stellige Relationen auf  $k$ -stellige Relationen abbildet. Dieser kleinste Fixpunkt ist  $(\varphi^A)^r(\emptyset)$ , wobei  $r$  minimal ist mit  $(\varphi^A)^r(\emptyset) = (\varphi^A)^{r+1}(\emptyset)$ . Dabei ist  $r \leq |A|^k$ .*

*Beweis.* Setze  $R_0 := \emptyset$  und  $R_{l+1} := \varphi^A(R_l)$  für alle  $l \in \mathbb{N}$ . Für alle  $l \in \mathbb{N}$  gilt  $R_l \subseteq R_{l+1}$ , da  $\varphi$  monoton ist. Falls  $R_l \neq R_{l+1}$  für ein  $l \in \mathbb{N}$  gilt, so existiert ein  $k$ -Tupel  $\bar{a} \in A^k$  mit  $\bar{a} \in R_{l+1} \setminus R_l$ . Da es aber nur  $|A|^k$   $k$ -Tupel von Elementen in  $A$  gibt, existiert  $r \leq |A|^k$  mit  $R_r = R_{r+1}$ . O.B.d.A. sei  $r$  minimal mit dieser Eigenschaft. Es ist klar, dass  $R_r = (\varphi^A)^r(\emptyset)$  ein Fixpunkt von  $\varphi^A$  ist.

Sei  $S \subseteq A^k$  ein weiterer Fixpunkt von  $\varphi^A$ . Offenbar gilt  $\emptyset \subseteq S$ . Vollständige Induktion liefert nun  $R_l = (\varphi^A)^l(\emptyset) \subseteq (\varphi^A)^l(S) = S$  für alle  $l \in \mathbb{N}$ , da  $\varphi$  monoton ist. Insbesondere gilt  $R_r \subseteq S$ . Also ist  $R_r$  der kleinste Fixpunkt von  $\varphi^A$ .  $\square$

Für eine monotone Formel  $\varphi(R, x_1, \dots, x_k)$  sei  $\text{LFP}(\varphi)$  der kleinste Fixpunkt von  $\varphi$ . Leider ist es unentscheidbar, ob eine gegebene Formel  $\varphi(R, x_1, \dots, x_k)$  monoton ist oder nicht. (Das liegt daran, dass man alle endlichen Strukturen  $A$  ansehen müsste, um festzustellen, dass die Funktion  $\varphi^A$  jeweils monoton ist.) Daher benutzt man eine etwas gröbere, aber leicht nachprüfbare syntaktische Eigenschaft von Formeln, die garantiert, dass eine Formel monoton ist.

Sei  $R$  ein  $k$ -stelliges Relationssymbol und  $\varphi(R)$  eine erststufige Formel über dem Vokabular  $\tau \cup \{R\}$ . Die Formel  $\varphi$  ist  **$R$ -positiv**, wenn  $R$  nur innerhalb einer geraden Anzahl von Negationen vorkommt. Wie man leicht sieht, ist jede  $R$ -positive Formel der Form  $\varphi(R, x_1, \dots, x_k)$  monoton.

**Definition 5.6.** LFP-Logik ist die Logik die man erhält, wenn man zur erststufigen Logik noch den Operator LFP für  $R$ -positive Formeln der Form  $\varphi(R, x_1, \dots, x_k)$  hinzufügt. Dabei kann  $\text{LFP}(\varphi(R, x_1, \dots, x_k))$  wie ein neues  $k$ -stelliges Relationssymbol benutzt werden. Die Gültigkeit von LFP-Formel in Strukturen ist auf die naheliegende Weise definiert, nämlich indem man  $\text{LFP}(\varphi(R, x_1, \dots, x_k))$  in einer Struktur  $A$  als diejenige  $k$ -stellige Relation interpretiert, die der kleinste Fixpunkt von  $\varphi^A$  ist.

**Lemma 5.7.** *Für jede endliche  $\tau$ -Struktur  $A$  und jede LFP-Formel  $\varphi$  über  $\tau$  ist die benötigte Rechenzeit, um  $A \models \varphi$  zu entscheiden, polynomiell in  $|A|$ .*

*Beweis.* Man erinnere sich an den Beweis der Tatsache, dass sich  $A \models \varphi$  für erststufige Formeln  $\varphi$  in polynomieller Zeit (in  $|A|$ ) entscheiden lässt. Wie in jenem Beweis benutzen wir Induktion über den Formelaufbau. Die Induktionsschritte sind im wesentlichen die gleichen. Der einzige Unterschied ergibt sich, wenn entschieden werden muss, ob ein Ausdruck der Form

$$\text{LFP}(\varphi(R, x_1, \dots, x_k))(a_1, \dots, a_k)$$

für gewisse  $a_1, \dots, a_k \in A$  gilt.

Nach Lemma 5.5 gibt es ein  $r \leq |n^k|$ , so dass  $(\varphi^A)^r(\emptyset)$  der kleinste Fixpunkt von  $\varphi^A$  ist. Es gilt aber  $(\varphi^A)^{|A|^k}(\emptyset) = (\varphi^A)^r(\emptyset)$ . Damit ist auch  $(\varphi^A)^{|A|^k}(\emptyset)$  der kleinste Fixpunkt von  $\varphi^A$ .

Für gegebenes  $R \subseteq A^k$  lässt sich die Relation  $\varphi^A(R)$  in polynomieller Zeit berechnen. Das Polynom hängt dabei nur von der Formel  $\varphi$  ab. Damit lässt sich auch  $\varphi^{|A|^k}(\emptyset)$  in polynomieller Zeit bestimmen. Insbesondere lässt sich

$$\text{LFP}(\varphi(R, x_1, \dots, x_k))(a_1, \dots, a_k)$$

in polynomieller Zeit entscheiden.  $\square$

Für geordnete Strukturen gilt auch die Umkehrung dieses Lemmas.

**Lemma 5.8.** *Sei  $\tau$  ein endliches Vokabular ohne Funktionssymbole mit mindestens einem zweistelligen Relationssymbol  $<$ . Weiter sei  $K$  eine Klasse endlicher, durch  $<$  linear geordneter  $\tau$ -Strukturen. Liegt  $K$  in  $\mathbf{P}$ , so lässt sich  $K$  durch eine LFP-Aussage axiomatisieren.*

*Beweis.* Sei  $M$  eine deterministische Turing-Maschine, die  $K$  entscheidet und in polynomieller Zeit (in der Mächtigkeit der Eingabestruktur) rechnet. Da wir  $K$  um endlich viele Strukturen abändern dürfen, können wir annehmen, dass es ein  $r \in \mathbb{N}$  gibt, so dass  $M$  bei Eingabe einer beliebigen Struktur  $A \in K$  höchstens  $|A|^r$  Schritte rechnet.

Wie im Beweis der schwierigen Richtung des Satzes von Fagin (Lemma 5.3) beschreiben wir die Berechnung von  $M$  durch Relationen auf der vorgelegten Struktur. Im Beweis von Lemma 5.3 haben wir mehrere zweistufige Existenzquantoren benutzt, um die entsprechenden Relationen zu erhalten. Wirklich wesentlich war der Existenzquantor jedoch nur für den Inhalt des Arbeitsbandes beim Start der Maschine. Dieser geratene Startinhalt des Arbeitsbandes war der Nicht-Determiniertheit der simulierten Turing-Maschine geschuldet.

Die restlichen zweistufigen Existenzquantoren lieferten dann nur noch Relationen, die man auch relativ schnell hätte berechnen können. Genauer gesagt, dieser Teil lässt sich auch mit dem LFP-Operator beschreiben.

Zunächst stellen wir fest, dass es im Beweis von Lemma 5.3 auch ein einzelner zweistufiger Existenzquantor getan hätte, da man viele Relationen mittels einer einzelnen (von höherer Stelligkeit) codieren kann.

Sei nämlich  $R_1, \dots, R_n$  eine Folge von Relationen auf einer endlichen Menge  $A$ , die mindestens  $n$  Elemente hat und linear geordnet ist. Weiter sei  $m$  die maximale Stelligkeit dieser Relationen. Ist  $R_i$   $l$ -stellig für ein  $l < m$ , so ersetzen wir  $R_i$  durch die  $m$ -stellige Relation  $R_i \times A^{m-i}$ , die offenbar die gleiche Information beinhaltet. Wir nehmen also o.B.d.A. an, dass alle  $R_i$  dieselbe Stelligkeit  $m$  haben.

Seien  $a_1, \dots, a_n$  die ersten  $n$  Elemente von  $A$ . Setze

$$R := \{a_1\} \times R_1 \cup \dots \cup \{a_n\} \times R_n.$$

$R$  ist damit eine  $(m+1)$ -stellige Relation. In erststufiger Logik ist  $R$  definierbar, wenn man  $R_1, \dots, R_n$  kennt, und die Relationen  $R_1, \dots, R_n$  sind definierbar, wenn man  $R$  kennt.

Sei nun  $A$  die vorgelegte Struktur. Um die Berechnung von  $M$  mit Relationen zu beschreiben, gehen wir genauso vor wie im Beweis von Lemma 5.3.  $M$  habe ein Arbeitsband und  $l-1$  Eingabebänder. Das Alphabet sei  $\{0, 1\}$  zusammen mit dem Leerzeichen. Die Anzahl der Zustände von  $M$  sei  $m$ .

Die Menge der möglichen Zeitpunkte der Berechnung ist  $A^r$ , durch die von  $<$  induzierte lexicographische Ordnung linear geordnet. Wir benutzen Relationen  $H_1, \dots, H_l$  für die Positionen der Köpfe,  $B_0, B_1, B_2$  für den Inhalt des Arbeitsbandes und  $Z_1, \dots, Z_m$  für den aktuellen Zustand, genau wie im Beweis von Lemma 5.3. Zusätzlich genehmigen wir uns eine  $r$ -stellige Relation  $L$ , die beschreiben wird, wie weit die Berechnung bereits fortgeschritten ist. ( $L$  wird immer genau auf ein Anfangsstück der linearen Ordnung  $A^r$  zutreffen.)

Alle diese Relationen codieren wir mittels einer einzigen Relation  $R$ , wie oben beschrieben. Es gilt nun, eine solche Relation, die eine akzeptierende Berechnung von  $M$  beschreibt, als kleinsten Fixpunkt darzustellen.

Wenn man genau nachrechnet, erhält man, dass die Stelligkeit von  $R$  genau  $2r+1$  ist. Wir definieren eine  $R$ -positive Formel  $\varphi(R, x_0, \dots, x_{2r})$ , so dass  $\text{LFP}(\varphi)$  die Berechnung von  $M$  bei Eingabe von  $A$  codiert. Dabei benutzen wir die Relationen  $H_1, \dots, H_l, B_0, B_1, B_2, Z_1, \dots, Z_m$  und  $L$  anstelle von  $R$  selbst. Wenn ein



Tupel  $(a_0, \dots, a_{2r}) \in A^{2r+1}$  vorgelegt ist, so zeigt  $a_0$  an, welche Relation aus der Menge  $\{H_1, \dots, H_l, B_0, B_1, B_2, Z_1, \dots, Z_m, L\}$  für  $(a_1, \dots, a_{2r})$  zu betrachten ist. Diese Relation nennen wir die **aktive** Relation.

Zunächst soll  $\varphi(R)$  auf ein Tupel  $(a_0, \dots, a_{2r}) \in A^{2r+1}$  zutreffen, wenn  $R$  bereits auf dieses Tupel zutraf. Weiter soll  $\varphi$  auf  $(a_0, \dots, a_{2r})$  zutreffen, wenn eine der folgenden Bedingungen gilt:

- (H0) Die aktive Relation ist  $H_i$  (die für den  $i$ -ten Kopf zuständige Relation) und  $(a_1, \dots, a_{2r})$  codiert „zum Zeitpunkt 0 befindet sich der  $i$ -te Kopf auf der Startzelle“.
- (B0) Die aktive Relation ist  $B_2$  (die für Leerzeichen auf dem Arbeitsband zuständige Relation) und  $(a_1, \dots, a_{2r})$  codiert irgendeine Zelle des Arbeitsbandes zum Zeitpunkt 0.
- (Z0) Die aktive Relation ist  $Z_1$  (die für den Startzustand zuständige Relation) und  $(a_1, \dots, a_{2r})$  codiert den Zeitpunkt 0.
- (L0) Die aktive Relation ist  $L$  und  $(a_1, \dots, a_{2r})$  codiert den Zeitpunkt 0.

Diese Bedingungen sorgen dafür, dass der Start der Berechnung von  $M$  korrekt beschrieben wird. Als nächstes widmen wir uns dem Verlauf der Berechnung. Die Formel  $\varphi$  soll auf ein Tupel  $(a_0, \dots, a_{2r})$  zutreffen, wenn eine der folgenden Bedingungen gilt:

- (H1) Die aktive Relation ist  $H_i$ ,  $(a_1, \dots, a_{2r})$  codiert einen Zeitpunkt  $t > 0$  und eine Kopfposition  $k$ ,  $L$  trifft auf  $t - 1$  zu (d.h., die Maschine hat bereits bis zum Zeitpunkt  $t - 1$  gerechnet) und die Kopfposition  $k$  wird in der Berechnung von  $M$  von der durch  $R$  codierten Konfiguration der Maschine zum Zeitpunkt  $t - 1$  aus erreicht.
- (B1) Die aktive Relation ist  $B_i$ ,  $(a_1, \dots, a_{2r})$  codiert einen Zeitpunkt  $t > 0$  und eine Zelle  $k$ ,  $L$  trifft auf  $t - 1$  zu und das von  $B_i$  beschriebene Zeichen (0, 1 oder Leerzeichen) befindet sich, nachdem die Maschine von der in  $R$  codierten Konfiguration zum Zeitpunkt  $t - 1$  aus einen Schritt weiter gerechnet hat, in der  $k$ -ten Zelle des Arbeitsbandes.
- (Z1) Die aktive Relation ist  $Z_i$ ,  $(a_1, \dots, a_{2r})$  codiert einen Zeitpunkt  $t > 0$ ,  $L$  trifft auf  $t - 1$  zu und  $Z_i$  ist der Zustand, der von der in  $R$  codierten Konfiguration zum Zeitpunkt  $t - 1$  aus erreicht wird.
- (L1) Die aktive Relation ist  $L$ ,  $(a_1, \dots, a_{2r})$  codiert einen Zeitpunkt  $t > 0$  und  $L$  trifft auf  $t - 1$  zu.

Längeres Hinsehen zeigt, dass  $\varphi$   $R$ -positiv ist und dass  $\text{LFP}(\varphi)$  genau eine korrekte Berechnung von  $M$  codiert. Damit lässt sich die Klasse  $K$  axiomatisieren durch die Aussage „es gibt einen Zeitpunkt  $t$ , so dass sich die Maschine in der durch  $\text{LFP}(\varphi)$  codierten Berechnung zum Zeitpunkt  $t$  im akzeptierenden Zustand befindet“.  $\square$

Lemma 5.7 und Lemma 5.8 liefern sofort

**Korollar 5.9.** *Eine Klasse geordneter endlicher Strukturen über einem Vokabular ohne Funktionssymbole liegt genau dann in  $\mathbf{P}$ , wenn sie Modellklasse einer LFP-Aussage ist.*