# Fixpunktlogik mit Zählquantoren

Seminar *Logik, Komplexität, Spiele*

Fixpunktlogiken

am

Lehr- und Forschungsgebiet

*Mathematische Grundlagen der Informatik*

Prof. Dr. Erich Grädel

Rheinisch-Westfälische Technische Hochschule Aachen

Florian Weingarten

**Betreuer:**
Dipl.-Inform.
Roman Rabinovich

Aachen, 21. Juni 2009

# Inhaltsverzeichnis

# 1 Einleitung

Die Prädikatenlogik erster Stufe (First Order Logic, kurz FO) ist ein Standard-Formalismus in der mathematischen Logik und eine natürliche Erweiterung der Aussagenlogik. In vielen Situationen ist FO aber zu schwach. Beispiele dafür lassen sich bereits in der Graphentheorie finden, so sind z.B. Erreichbarkeit, Zusammenhang und Regularität eines Graphen, sowie Parität der Knotenmenge Eigenschaften, die sich in FO nicht ausdrücken lassen. Der Hauptgrund dieser Schwäche ist, intuitiv ausgedrückt, das Fehlen von echter *Rekursion* bzw. unbeschränkter *Iteration*, sowie die Unfähigkeit in FO zu *zählen*. Aussagen wie „es gibt genausoviele Elemente $x$, für die $\varphi(x)$ gilt, wie es Elemente $x$ gibt, für die $\varphi(x)$ nicht gilt" lassen sich z.B. in FO nicht formulieren.

Fixpunktlogiken sind Erweiterungen von FO, die *Rekursion* erlauben, damit ist es z.B. unmittelbar möglich die transitive Hülle einer binären Relation zu definieren und somit Erreichbarkeit in Graphen auszudrücken.

In dieser Ausarbeitung soll das Konzept des Zählens formalisiert werden, um anschliessend verschiedene Logiken um diese Fähigkeit zu erweitern, insbesondere *Fixpunktlogiken mit Zählquantoren* werden behandelt.

Motivationen für diese Fragestellungen kommen aus der endlichen Modelltheorie und der deskriptiven Komplexitätstheorie, die unter anderem den Zusammenhang zwischen Logiken und Komplexitätsklassen untersuchen. Eine zentrale Frage ist, ob es eine Logik gibt, die (in noch zu spezifizierender Weise) zur Komplexitätsklasse PTIME passt. Inflationäre Fixpunktlogik mit Zählquantoren war ein Kandidat für eine solche Logik. Der Beweis von Cai, Fürer und Immerman [6], dass diese Vermutung nicht zutrifft, soll hier ausgeführt werden.

# 2 Komplexitätsklassen

Die *Modellklasse* einer Formel $\varphi \in L$ einer Logik $L$ bezeichnet die Klasse der Strukturen, die Modell von $\varphi$ sind. Für eine Formel $\varphi \in L$ und eine Struktur $\mathfrak{A}$ bezeichnet man das Problem, zu entscheiden ob $\mathfrak{A} \models \varphi$ gilt, als *Model-Checking-Problem*.

**Definition 2.1.** *Eine Logik $L$* erfasst *eine Komplexitätsklasse $C$ (englisch: $L$* captures *$C$), wenn gilt:*

- *Für jeden Satz $\psi \in L$ ist das Model-Checking-Problem für $\psi$ in der Komplexitätsklasse $C$.*
- *Für jede (unter Isomorphismen abgeschlossenen) Strukturklasse $\mathcal{K}$, deren Entscheidungsproblem in $C$ ist, existiert ein Satz $\psi \in L$, so dass die Modellklasse von $\psi$ gleich $\mathcal{K}$ ist.*

Ein bekanntes Beispiel ist der *Satz von Büchi, Elgot und Trakhtenbrot*, der besagt, dass die monadische Logik zweiter Stufe (MSO) über Wortstrukturen und Bäumen genau die regulären Sprachen, d.h. die Sprachen, die von endlichen Automaten erkannt werden, erfasst.

Ein weiteres Beispiel ist der *Satz von Fagin* [4], nach dem die Klasse NP genau von der existentiellen Logik zweiter Stufe über endlichen Strukturen erfasst wird.

Es ist eine offene Frage, ob es eine Logik gibt, die das Gleiche für deterministische Polynomialzeit leistet, d.h. die auf allen endlichen Strukturen, genau PTIME erfasst [4]. Gesucht ist also eine Logik $L$, so dass die in PTIME entscheidbaren Eigenschaften einer endlichen Struktur genau die Eigenschaften sind, die sich in $L$ ausdrücken lassen.

Eine negative Antwort auf diese offene Frage würde, nach dem Satz von Fagin, unmittelbar PTIME $\neq$ NP implizieren.

# 3 Fixpunktlogiken

Zunächst sollen einige Definitionen und Eigenschaften wiederholt werden. Grundlage für das folgende Kapitel sind [4] und [5].

## 3.1 Operatoren und Fixpunkte

In dieser Ausarbeitung werden wir nur endliche relationale Strukturen betrachten.

**Definition 3.1.** *Sei $D$ eine endliche Menge und $F : \mathcal{P}(D) \to \mathcal{P}(D)$ eine Abbildung (Operator), dann nennt man $F$*

- monoton, *falls aus $A \subseteq B$ stets $F(A) \subseteq F(B)$ folgt,*
- inflationär, *falls $A \subseteq F(A)$ für alle $A \subseteq D$ gilt und*
- induktiv, *falls $\emptyset \subseteq F(\emptyset) \subseteq F(F(\emptyset)) \subseteq ...$ gilt.*

*Eine Teilmenge $A \subseteq D$ heißt* Fixpunkt von $F$, *falls $F(A) = A$.*

**Satz 3.2.** *[4] Ist $F$ monoton oder inflationär, so ist $F$ bereits induktiv. Ist $F$ induktiv, so wird die Folge $(F^n(\emptyset))_{n\in\mathbb{N}}$ stationär, d.h. es existiert ein $k \in \mathbb{N}$ mit $F^{k+1}(\emptyset) = F^k(\emptyset)$.*

*Beweis.* Ist $F$ inflationär, dann gilt per Definition $X \subseteq F(X)$ für alle $X \subseteq D$, insbesondere also $F^i(X) \subseteq F(F^i(X)) = F^{i+1}(X)$ für alle $i \in \mathbb{N}$. Ist $F$ monoton, so folgt aus $F^i(\emptyset) \subseteq F^{i+1}(\emptyset)$ per Definition direkt, dass $F^{i+1}(\emptyset) = F(F^i(\emptyset)) \subseteq F(F^{i+1}(\emptyset)) = F^{i+2}(\emptyset)$. Mit $\emptyset \subseteq F(\emptyset)$ (als Induktionsanfang) folgt, dass $F$ induktiv ist. Da $D$ endlich ist, ist klar, dass die Folge $(F^n(\emptyset))_{n\in\mathbb{N}}$ periodisch werden muss. Da $F$ induktiv ist, kann die Periode offensichtlich nur trivial sein. □

Ist $X$ ein Fixpunkt von $F$, dann nennt man $X$ einen *kleinsten* (größten) Fixpunkt (englisch: least fixed-point (lfp) und greatest fixed-point (gfp)), wenn $X$ inklusionsminimal (bzw. maximal) ist, d.h. für jeden weiteren Fixpunkt $X'$ gilt $X \subseteq X'$ (bzw. $X \supseteq X'$).

**Satz 3.3** (Knaster, Tarski)**.** *Sei $F : \mathcal{P}(D) \to \mathcal{P}(D)$ monoton, dann besitzt $F$ einen kleinsten und einen größten Fixpunkt.*

**Definition 3.4.** *Sei $\psi(X, \overline{x})$ eine Formel mit freien Variablen $\overline{x} = x_1, ..., x_k$ und freier Relationsvariable $X$ der Stelligkeit $k$. Dann wird von $\psi$ für jede endliche Struktur $\mathfrak{A}$ mit Universum $A$ ein Operator auf der Menge der $k$-stelligen Relationen in $A$ induziert:*

$$\begin{aligned} F_\psi : \mathcal{P}(A^k) &\to \mathcal{P}(A^k) \\ R &\mapsto \{\overline{a} \in A^k \mid (\mathfrak{A}, R) \models \psi(R, \overline{a})\} \end{aligned}$$

Im Allgemeinen muss kein Fixpunkt von $F_\psi$ existieren, was man sich z.B. an der Formel $\psi(R, x) := \neg Rx$ überlegt, für die in einer Struktur $\mathfrak{A}$ mit Universum $A$ gilt: $F_\psi^{2i}(\emptyset) = \emptyset$ und $F_\psi^{2i+1}(\emptyset) = A$.

Wir sagen, dass $X$ in $\varphi$ nur positiv vorkommt, wenn jedes Vorkommen von $X$ im Bereich einer geraden Anzahl an Negationssymbolen ist. Fordert man, dass $X$ in $\psi$ nur positiv

vorkommt, so ist $F_\psi$ monoton (siehe [4]) und besitzt nach Satz 3.3 einen kleinsten und größten Fixpunkt.

Man nutzt nun diesen Operator um die folgenden *Fixpunktlogiken* zu definieren.

## 3.2 Least Fixed-Point Logic

Wir definieren zunächst induktiv die Syntax und die Semantik von LFP (Least Fixed-Point Logic).

**Definition 3.5** (LFP)**.** *Terme seien wie für FO definiert.*

- *Sind $t, t'$ Terme, so ist $t = t' \in \mathrm{LFP}$.*
- *Sind $t_1, ..., t_n$ Terme und $R$ ein $n$-stelliges Relationssymbol oder eine $n$-stellige Relationsvariable, so ist $Rt_1...t_n \in \mathrm{LFP}$.*
- *Sind $\varphi, \psi \in \mathrm{LFP}$-Formeln, so sind $\varphi \wedge \psi$, $\varphi \vee \psi$, $\neg\varphi \in \mathrm{LFP}$.*
- *Sei $\psi(\overline{x}, \overline{y})$ eine LFP-Formel mit freien Variablen $\overline{x} := x_1, ..., x_n$ und $\overline{y} := y_1, ..., y_r$, $R$ eine Relationsvariable der Stelligkeit $n$, die in $\psi$ nur positiv auftritt und seien $\overline{t} := (t_1, ..., t_n)$ Terme, so ist auch $[lfp\ R\overline{x}.\psi](\overline{t})$ eine LFP-Formel.*

*Die Semantik der ersten drei Punkte ist wie für* FO *definiert. Die Semantik des vierten Punktes ist die folgende: Eine Struktur $\mathfrak{A}$ mit Zuweisungen für die freien Variablen $R, \overline{x}$ ist genau dann Modell der Formel $[lfp\ R\overline{x}.\psi](\overline{t})$, wenn $\overline{t}^{\mathfrak{A}}$ im kleinsten Fixpunkt von $F_\psi$ enthalten ist (dieser Fixpunkt wird mit* $\mathrm{LFP}(F)$ *bezeichnet).*

Es ist bekannt (siehe z.B. [1]), dass Erreichbarkeit eine Eigenschaft ist, die sich in FO nicht ausdrücken lässt. An folgendem Beispiel wollen wir uns daher überlegen, dass LFP echt stärker als FO ist.

**Beispiel 3.6** (Transitive Hülle)**.** Ein Knoten $v$ in einem gerichteten Graphen $\mathcal{G} = (V, E)$ ist genau dann von einem Knoten $u$ aus erreichbar, wenn $(u, v)$ in der transitiven Hülle der Kantenrelation enthalten ist. Anders ausgedrückt: $v$ ist von $u$ aus erreichbar, wenn $u = v$ oder wenn es einen Nachfolger von $u$ gibt, von dem aus $v$ erreichbar ist. Betrachte die Formel $\psi(T, x, y) := (x = y) \vee \exists z(Exz \wedge Tzy)$ mit binärer Relationsvariable $T$. Man überlegt sich leicht, dass die transitive Hülle von $E$ ein Fixpunkt von $F_\psi$ ist. Nach Definition von LFP beschreibt also die folgende Formel Erreichbarkeit in einem Graphen: $\varphi(u, v) :=$ [lfp $Txy.\psi](u, v)$. Man beachte, dass $T$ in $\psi$ nur positiv vorkommt.

## 3.3 Inflationary Fixed-Point Logic

Um sich von der syntaktischen Einschränkung zu lösen, dass Relationssymbole nur positiv auftreten dürfen, betrachtet man, alternativ zum kleinsten Fixpunkt, den sogenannten inflationären Fixpunkt.

**Definition 3.7.** *Sei $D$ endlich und $F : \mathcal{P}(D) \to \mathcal{P}(D)$ ein (nicht notwendigerweise induktiver) Operator, dann betrachtet man hierzu den induzierten Operator*

$$\begin{aligned} F^+ : \mathcal{P}(D) &\to \mathcal{P}(D) \\ R &\mapsto R \cup F(R) \end{aligned}$$

Der Operator $F^+$ ist nun offensichtlich inflationär (und damit nach Satz 3.2 auch induktiv). Wie bereits erwähnt, wird die Folge $((F^+)^n(\emptyset))_{n\in\mathbb{N}}$ stationär, d.h. es existiert ein $k \in \mathbb{N}$ mit $(F^+)^{k+1}(\emptyset) = (F^+)^k(\emptyset) =: \mathrm{IFP}(F)$. Die Menge $\mathrm{IFP}(F)$ nennt man den *induktiven Fixpunkt* (oder *inflationären Fixpunkt*) von $F$.

Ausgehend von diesem induktiven Fixpunkt definiert man die zugehörige Logik: Inflationäre Fixpunktlogik (englisch: Inflationary Fixed-Point Logic, IFP).

Analog zu Definition 3.5 definieren wir die Syntax von IFP induktiv. Die Regeln für den Aufbau von Termen, Disjunktionen, Konjunktionen und Negationen seien wie bei LFP, mit dem Unterschied, dass Relationsvariablen nicht mehr nur positiv vorkommen dürfen.

**Definition 3.8.** *Sei $\psi(R, \overline{x}, \overline{y})$ eine IFP-Formel mit freien Variablen $\overline{x} := x_1, ..., x_n$ und freier Relationsvariable $R$ der Stelligkeit $n$ sowie $\overline{t} := t_1, ..., t_n$ Terme, so ist auch $[ifp\ R\overline{x}.\psi](\overline{t})$ eine IFP-Formel (in der $R$ und $\overline{x}$ nichtmehr frei sind). Die Semantik dieser neuen Formel ist, analog zu LFP, die folgende:* $\mathfrak{A} \models [ifp\ R\overline{x}.\psi](\overline{t}) \ :\Leftrightarrow\ \overline{t}^{\mathfrak{A}} \in \mathrm{IFP}(F)$

Es stellt sich heraus, dass die Ausdrucksstärke von IFP und LFP übereinstimmen.

**Satz 3.9.** *[11] IFP und LFP haben die gleiche Ausdrucksstärke.*

## 3.4 Partial Fixed-Point Logic

Anstatt den Operator $F$ künstlich inflationär zu machen (wie bei IFP) kann man alternativ auch „partielle Fixpunkte“ betrachten. Man definiert den partiellen Fixpunkt als den „normalen“ Fixpunkt, falls er existiert und als $\emptyset$, falls nicht.

**Definition 3.10** (PFP)**.** *Sei $D$ endlich und $F : \mathcal{P}(D) \to \mathcal{P}(D)$ ein (nicht notwendigerweise induktiver) Operator. Definiere nun*

$$\mathrm{PFP}(F) := \begin{cases} \mathrm{LFP}(F) & \textit{falls } \mathrm{LFP}(F) \textit{ existiert,} \\ \emptyset & \textit{sonst.} \end{cases}$$

Man beachte, dass die Folge $(F^n(\emptyset))_{n\in\mathbb{N}}$ periodisch wird (aber nicht unbedingt stationär).

Syntax und Semantik der zugehörigen Logik werden analog zu LFP/IFP definiert.

Ob PFP echt stärker ist als LFP bzw. IFP ist bis heute nicht bekannt, wie der folgende Satz deutlich macht.

**Satz 3.11** (Abiteboul, Vianu)**.** *[4] LFP/IFP und PFP sind genau dann gleich ausdrucksstark, wenn* PTIME = PSPACE.

Es stellt sich heraus, dass keine der drei gerade definierten Logiken in der Lage ist, PTIME zu erfassen.

**Beispiel 3.12.** Betrachte einen Graphen $\mathcal{G} = (V, E)$ mit $E = \emptyset$, d.h. es existieren keine Kanten, nur Knoten. Es ist in Polynomialzeit (in der Größe des Graphen) möglich zu testen, ob die Anzahl der Knoten gerade oder ungerade ist. Ausserdem sind die drei eingeführten Fixpunktkonstrukte nutzlos, wenn es keine Kanten gibt, d.h. in dieser Struktur sind LFP, IFP und PFP nicht ausdrucksstärker als FO. In FO ist es aber nicht möglich zu formulieren, dass die Knotenmenge gerade ist (Beweis z.B. über Ehrenfeucht-Fraïssé-Spiele [1]). Daher erfasst keine der drei Logiken PTIME auf der Klasse der endlichen Graphen ohne Kanten.

Um diese Unzulänglichkeit zu beheben, wollen wir unsere Logiken um die Möglichkeit zu *zählen* erweitern.

# 4 Zählen

## 4.1 Die Logiken $\mathcal{L}_k$ und $\mathcal{C}_k$

Mit $\mathcal{L}_k$ bezeichnen wir das Fragment von FO, in dem nur maximal $k$ viele Variablen benutzt werden dürfen, d.h. für jedes $\varphi \in \mathcal{L}_k$ ist die Menge der in $\varphi$ auftretenden Variablen eine Teilmenge von $\{x_1, ..., x_k\}$.

Wir wollen eine Erweiterung von $\mathcal{L}_k$ mit Zählquantoren $\exists^{\geq i}$ definieren.

**Definition 4.1** (Die Logik $\mathcal{C}_k$)**.** *Jede Formel aus $\mathcal{L}_k$ ist eine $\mathcal{C}_k$-Formel. Sei $\varphi \in \mathcal{C}_k$ eine Formel mit freier Variable $x$ (und eventuell noch weiteren freien Variablen), dann ist für jedes $i \in \mathbb{N}$ auch $\exists^{\geq i} x\varphi(x)$ eine Formel aus $\mathcal{C}_k$. Eine Struktur $\mathfrak{A}$ (mit Zuweisungen für die von $x$ verschiedenen freien Variablen von $\varphi$) ist genau dann Modell von $\exists^{\geq i} x\varphi(x)$, wenn es mindestens $i$ verschiedene Elemente $a \in A$ gibt, die $\varphi$ erfüllen.*

Es ist klar, dass man durch Hinzufügen solcher Zählquantoren zu FO keine Ausdrucksstärke gewinnt, da man jeden Zählquantor bereits in FO (allerdings mit mehr Variablen) simulieren kann. Also ist $\mathcal{C}_k$ nicht stärker als FO (aber echt stärker als $\mathcal{L}_k$).

Wir wollen aber nun eine Art zu zählen untersuchen, die unsere Logik tatsächlich echt ausdrucksstärker macht. Dafür reicht bereits FO mit Zählquantoren, wie wir im folgenden Abschnitt sehen werden.

## 4.2 Prädikatenlogik mit Zählquantoren

**Definition 4.2.** *Sei $\mathfrak{A} = (A, (R_i)^{\mathfrak{A}}_{i \in I})$ (mit Indexmenge $I$) eine endliche Struktur mit $A \cap \{0, 1, ..., |A|\} = \emptyset$. Dann definieren wir*

$$\mathfrak{A}^* := (A \cup \{0, 1, ..., |A|\}, (R_i)^{\mathfrak{A}}_{i \in I}, \leq, \min, \max)$$

*wobei $\leq$ die kanonische lineare Ordnung auf $\{0, 1, ..., |A|\}$, mit kleinstem Element* min *und größtem Element* max*, bezeichnet. Die Elemente der ursprünglichen Struktur nennt man Elemente* erster Art *(*Punkte*) und die neuen Elemente* zweiter Art *(*Zahlen*). Für Variablen erster Art benutzen wir Buchstaben $x, y, z, ...$, für solche zweiter Art $\mu, \lambda, \nu, ...$*

Die Elemente der beiden Arten sind durch sogenannte *Zählquantoren* miteinander verknüpft.

Wir sagen, dass eine Relation *gemischte Stelligkeit* $(k, l)$ hat, wenn sie eine Teilmenge von $A^k \times \{0, 1, ..., |A|\}^l$ ist.

**Definition 4.3** (Die Logik FO+C)**.** *Sei $\tau$ eine Signatur (mit $\tau \cap \{\leq, \min \max\} = \emptyset$).*

1. *Alle FO Terme über $\tau$ (mit Variablen $x, y, ...$) sind Terme der ersten Art in* FO+C.
2. *Alle FO Terme über $\{\leq, \min, \max\}$ (mit Variablen $\mu, \nu, ...$) sind Terme der zweiten Art in* FO+C.
3. *Alle atomaren $\tau$-Formeln und alle atomaren $\{\leq, \min, \max\}$-Formeln sind Formeln in* FO+C.
4. *Wenn $X$ eine Relationsvariable der Stelligkeit $(k, l)$ ist, dann ist $X\overline{t}\overline{\rho}$ (wobei $\overline{t} = t_1, ..., t_k$ und $\overline{\rho} = \rho_1, ..., \rho_l$) eine Formel in* FO+C.
5. *Wenn $\varphi$ und $\psi$ Formeln sind, dann sind $\neg\varphi$, $\varphi \wedge \psi$ und $\varphi \vee \psi$ Formeln in* FO+C.

6. *Wenn $\varphi$ eine Formel ist, dann sind auch $\exists x\varphi$ und $\exists\mu\varphi$ Formeln.*
7. *Wenn $\varphi$ eine Formel ist und $\mu$ eine Variable zweiter Art, dann ist auch $\exists^{\geq\mu}x\varphi(x)$ eine Formel.*

*Die Semantik der ersten sechs Punkte sei wie oben. Eine Formel, die nach der letzten Regel gebildet wurde, ist erfüllt, wenn es mindestens $\mu$ verschiedene Elemente $a \in A$ gibt, die $\varphi(a)$ erfüllen.*

Zur Vereinfachung der Notation schreibt man auch $\exists^{=\mu}x\varphi(x)$ als Abkürzung für die Formel $\exists^{\geq\mu}x\varphi(x) \wedge \forall\lambda(\lambda > \mu \rightarrow \neg\exists^{\geq\lambda}x\varphi(x))$.

**Beispiel 4.4** (Regularität)**.** Sei $\mathcal{G} = (V, E)$ ein ungerichteter Graph. Man nennt $\mathcal{G}$ *regulär*, wenn jeder Knoten den gleichen Grad hat. Die Modellklasse der folgenden Formel ist genau die Klasse der regulären Graphen: $\varphi := \exists\mu\forall x\forall y(\exists^{=\mu}zExz \wedge \exists^{=\mu}zEyz)$. Regularität ist in FO nicht ausdrückbar (Beweis z.B. über Ehrenfeucht-Fraïssé-Spiele [1]), FO+C ist über ungerichteten Graphen also echt stärker.

## 4.3 Inflationäre Fixpunktlogik mit Zählquantoren

Es liegt nahe, die beiden gerade genannten Konzepte zu verbinden und Fixpunktlogiken um die Möglichkeit zu zählen zu erweitern (bzw. FO+C um Fixpunkte zu erweitern).

Im Folgenden betrachten wir nur noch die Fixpunktlogik IFP.

**Definition 4.5** (Syntax von IFP+C)**.** *Die Logik IFP+C ist die Erweiterung von* FO+C *um die folgende Regel: Ist $\varphi(X, \overline{x}, \overline{\mu})$ eine Formel mit freier Relationsvariable $X$ vom Typ $(k, l)$, freien Variablen $\overline{x} = x_1, ..., x_k$ der ersten Art und $\overline{\mu} = \mu_1, ..., \mu_l$ der zweiten Art, $\overline{t} = t_1, ..., t_k$ Terme der ersten und $\overline{\rho} = \rho_1, ..., \rho_l$ Terme der zweiten Art, dann ist auch $[ifp\ X\overline{x}\overline{\mu}.\varphi](\overline{t}, \overline{\rho})$ eine Formel (in der $X$,$\overline{x}$ und $\overline{\mu}$ nichtmehr frei vorkommen).*

Eine solche Formel induziert ebenfalls einen Fixpunktoperator auf der Menge der Relationen mit Stelligkeit $(k, l)$ im Universum von $\mathfrak{A}^*$:

$$\begin{aligned} F^*_\varphi : \mathcal{P}(A^k \times \{0, 1, ..., |A|\}^l) &\rightarrow \mathcal{P}(A^k \times \{0, 1, ..., |A|\}^l) \\ R &\mapsto R \cup \{(\overline{a}, \overline{m}) \mid \mathfrak{A}^* \models \varphi(R, \overline{a}, \overline{m})\} \end{aligned}$$

**Definition 4.6** (Semantik von IFP+C)**.** *Eine Struktur $\mathfrak{A}$ erfüllt eine Formel, die nach der neuen Regel gebildet wurde, wenn $(\overline{t}, \overline{\rho})^{\mathfrak{A}^*}$ im kleinsten Fixpunkt des durch die Formel induzierten inflationären Fixpunktoperators enthalten ist.*

Grädel und Otto haben in [3] gezeigt, dass jede IFP+C Formel äquivalent ist zu einer, die nur eine einzige Fixpunktoperation enthält.

**Beispiel 4.7.** Sei $A$ das Universum einer Struktur $\mathfrak{A}$. Angenommen $|A|$ sei mindestens 2, dann können wir die Konstante 2 als das Element, das genau zwei Vorgänger (0 und 1) hat, definieren und es daher ohne Einschränkung als Konstantensymbol nutzen. Betrachte nun die folgende IFP+C Formel:

$$\psi := [\text{ifp } X\mu.(\underbrace{(\mu = \min) \vee \exists\nu(X\nu \wedge \mu = \nu + 2)}_{=:\varphi})]\max$$

mit freier Relationsvariable der Stelligkeit $(0, 1)$. Der zugehörige Fixpunktoperator lautet:

$$\begin{aligned} F^*_\varphi : \mathcal{P}(\{0, 1, ..., |A|\}) &\rightarrow \mathcal{P}(\{0, 1, ..., |A|\}) \\ R &\mapsto R \cup \{i \mid \mathfrak{A}^* \models \varphi(R, i)\} \end{aligned}$$

Es gilt nun:

- $F_\varphi(R) = \{i \mid i = 0 \text{ oder } i = j + 2 \text{ für ein } j \in R\}$
- $F_\varphi(\emptyset) = \{0\}$
- $F_\varphi(\{0\}) = \{i \mid i = 0 \text{ oder } i = 0 + 2\} = \{0, 2\}$
- $F_\varphi(\{0, 2\}) = \{0, 2, 4\}$
- ...
- $F_\varphi^k(\emptyset) = \{i \mid i \leq 2k \text{ und } i \text{ ist gerade}\}$
- Der Fixpunkt von $F_\varphi$ ist die Menge der geraden Zahlen in $\{0, 1, ..., |A|\}$.

Damit ist $\mathfrak{A}^*$ genau dann Modell von $\psi$, wenn $\max^{\mathfrak{A}^*} \in \text{IFP}(F_\varphi)$, d.h. wenn $|A|$ eine gerade Zahl ist (und damit haben wir eine Eigenschaft gefunden, die sich in FO nicht ausdrücken liess).

**Beispiel 4.8.** Betrachte die Klasse der ungerichteten Graphen und die folgende IFP+C Formel:

$$\psi(x, y, \lambda) := [\text{ifp } Xz\mu.\underbrace{((z = x \wedge \mu = 0) \vee (\neg\exists\nu Xz\nu \wedge \exists z'\exists\mu'(Xz'\mu' \wedge Ez'z \wedge \mu' + 1 = \mu))}_{=:\varphi}](y\lambda)$$

Der zugehörige Operator lautet:

$$\begin{aligned} F_\varphi^* : \mathcal{P}(V \times \{0, 1, ..., |V|\}) &\to \mathcal{P}(V \times \{0, 1, ..., |V|\}) \\ R &\mapsto R \cup \{(v, i) \mid \mathfrak{A}^* \models \varphi(R, v, i)\} \end{aligned}$$

und es gilt

- $F_\varphi^*(\emptyset) = \{(v, i) \mid v = x \text{ und } i = 0\} = \{(x, 0)\}$
- $(F_\varphi^*)^2(\emptyset) = \{(v, i) \mid (v, i) = (x, 0) \text{ oder } (v \neq x \text{ und } (x, v) \in E \text{ und } i = 1)\} = \{(x, 0), (x', 1)\}$ (wobei $(x, x') \in E$)
- ...
- $(F_\varphi^*)^k(\emptyset) = \{(v, i) \mid \text{dist}(v, x) = i \leq k\}$
- Die Formel $\psi(x, y, \lambda)$ gilt also genau dann in einem Graphen $\mathcal{G} = (V, E)$, wenn $(y, \lambda) \in \text{IFP}(F)$, d.h. wenn die Distanz zwischen $x$ und $y$ (Länge des kürzesten Pfades) genau $\lambda$ ist.

# 5 IFP+C erfasst PTIME nicht

Auf der Suche nach einer Logik für PTIME bzw. bei der Untersuchung von Fixpunktlogiken, stellt sich heraus, dass sich die Ausdrucksstärke von IFP bzw. LFP irgendwo zwischen FO und PTIME befindet (kurz: FO $\subseteq$ IFP, LFP $\subseteq$ PTIME).

Immerman und Vardi haben in [10] gezeigt: Auf geordneten Strukturen wird PTIME von IFP (bzw. LFP) erfasst (und PSPACE von PFP).

Alle Beispiele, die (vor der Publikation von [6]) belegten, dass PTIME im Allgemeinen (auf nicht notwendigerweise geordneten Strukturen) nicht von IFP bzw. LFP erfasst wird, benutzen Eigenschaften, für die gezählt werden muss. Es lag daher nahe sich zu fragen, ob Fixpunktlogiken mit Zählquantoren vielleicht ausreichen, um PTIME zu erfassen.

Im Folgenden soll der Beweis ausgeführt werden, der diese Annahme widerlegt. Wir gehen dabei nach [6] vor.

## 5.1 Konventionen und Definitionen

Unter einem *Graphen* $\mathcal{G} = (V, E)$ meinen wir im Folgenden immer einen *ungerichteten* und *schleifenfreien* Graphen ohne Multikanten.

**Definition 5.1** ($L$-Äquivalenz)**.** *Sei $L$ eine Logik und $\mathcal{G}$ und $\mathcal{H}$ zwei Graphen. Wir bezeichnen $\mathcal{G}$ und $\mathcal{H}$ als* $L$-äquivalent *($\mathcal{G} \equiv_L \mathcal{H}$), wenn $\mathcal{G}$ und $\mathcal{H}$ genau die gleichen $L$-Sätze erfüllen, d.h. für alle Sätze $\varphi \in L$ gilt, dass $\mathcal{G} \models \varphi \Leftrightarrow \mathcal{H} \models \varphi$. Die Logik $L$* identifiziert *$\mathcal{G}$, wenn aus $\mathcal{G} \equiv_L \mathcal{H}$ bereits folgt, dass $\mathcal{G} \cong \mathcal{H}$. Anders ausgedrückt: Nicht-isomorphe Graphen lassen sich durch einen Satz aus $L$ unterscheiden.*

Wir wollen jetzt sogenannte *Pebble-Spiele* (deutsch: Kieselstein) betrachten, die für die Logiken $\mathcal{L}_k$ und $\mathcal{C}_k$ eine ähnliche Rolle spielen wie Ehrenfeucht-Fraïssé-Spiele [1] für FO.

## 5.2 Pebble-Spiel für $\mathcal{L}_k$

**Definition 5.2** ($\mathcal{L}_k$-Spiel)**.** *Seien $\mathcal{G} = (V_\mathcal{G}, E_\mathcal{G})$, $\mathcal{H} = (V_\mathcal{H}, E_\mathcal{H})$ zwei Graphen mit $V_\mathcal{G} \cap V_\mathcal{H} = \emptyset$. Wir definieren das* $\mathcal{L}_k$-Spiel auf *$\mathcal{G} \cup \mathcal{H}$ wie folgt:*

- *Es gibt zwei Spieler und für jedes $1 \leq i \leq k$ zwei* Steine *$x_i$.*
- *In jedem Zug wählt Spieler I ein $i \in \{1, ..., k\}$ und platziert einen Stein $x_i$ auf einem Knoten in einem der beiden Graphen seiner Wahl.*
- *Spieler II antwortet, indem er den entsprechenden zweiten Stein $x_i$ in dem jeweils anderen Graphen platziert.*

Eine *$k$-Konfiguration* auf $\mathcal{G} \cup \mathcal{H}$ ist ein Paar von zwei injektiven partiellen Funktionen $(u, v)$ mit $u : \{x_1, ..., x_k\} \to V_\mathcal{G}$ und $v : \{x_1, ..., x_k\} \to V_\mathcal{H}$ mit gleichem Definitionsbereich $D_u = D_v \subseteq \{x_1, ..., x_k\}$.

Gilt $u(x_i) = g$, dann liegt auf dem Knoten $g \in V_\mathcal{G}$ ein Stein $x_i$. Die Steine der Variablen, die nicht in $D_u$ enthalten sind, wurden im Spiel noch nicht platziert. Mit $(u_r, v_r)$ bezeichnen wir die Konfiguration im Spiel nach $r$ Zügen.

Spieler I *gewinnt* die Partie (nach $r$ Zügen), falls $f_r : D_{u_r} \to D_{v_r}, u_r(x_i) \mapsto v_r(x_i)$ kein Isomorphismus der durch $D_{u_r}$ und $D_{v_r}$ induzierten Teilgraphen von $\mathcal{G}$ und $\mathcal{H}$ ist. Spieler II gewinnt unendliche Partien (d.h. wenn Spieler I für kein $r \in \mathbb{N}$ nach $r$ Zügen gewinnt). Man beachte, dass ein Isomorphismus eines gefärbten Graphen mit der Färbung verträglich sein muss.

Positionale Strategien (d.h. solche, die nur die aktuelle Position und keine vorherigen Positionen berücksichtigen) reichen aus um das Spiel zu gewinnen (da es sich um ein Erreichbarkeitsspiel handelt). Eine solche Strategie kann formal kodiert werden als eine Abbildung von der Menge der Konfigurationen in die Menge der Spielzüge.

Spieler II hat also eine Gewinnstrategie, wenn er immer passende Knoten finden kann, um den Isomorphismus zu erhalten. Anschaulich versucht Spieler II die Graphen „gleich aussehen zu lassen“, wobei Spieler I versucht sie zu unterscheiden.

## 5.3 Pebble-Spiel für $\mathcal{C}_k$

Das $\mathcal{L}_k$-Spiel lässt sich für die Logik $\mathcal{C}_k$ erweitern.

Das $\mathcal{C}_k$-Spiel auf $\mathcal{G} \dot\cup \mathcal{H}$ sei definiert wie das $\mathcal{L}_k$-Spiel, mit dem Unterschied, dass jeder Zug nun aus zwei Teilen besteht:

1. Spieler I wählt einen Stein $x_i$. Dann wählt er eine Teilmenge $A$ von Knoten in einem der Graphen. Spieler II muss nun eine Teilmenge $B$ von Knoten in dem anderen Graphen wählen mit $|B| = |A|$.

2. Spieler I platziert seinen Stein auf einem Knoten aus $B$. Spieler II platziert den zweiten Stein $x_i$ auf einem Knoten aus $A$.

Die Gewinnbedingung ist definiert wie für das $\mathcal{L}_k$-Spiel. Zusätzlich verliert Spieler II, falls er nicht entsprechend den Spielregeln ziehen kann (d.h. falls er keine Menge $B$ finden kann mit $|A| = |B|$).

Die Bedeutung des $\mathcal{C}_k$-Spiels wird durch den folgenden Satz deutlich. Zur Vereinfachung der Notation sagen wir, dass $\varphi \in \mathcal{C}_{k,m}$ ist, wenn $\varphi \in \mathcal{C}_k$ ist und Quantorentiefe $m$ hat. Außerdem schreiben wir $\mathcal{G}, u \equiv_{\mathcal{C}_{k,m}} \mathcal{H}, v$, wenn sich $\mathcal{G}$ und $\mathcal{H}$ durch Formeln aus $\mathcal{C}_{k,m}$, deren freie Variablen eine Teilmenge von $D_u = D_v$ sind, nicht unterscheiden lassen (d.h. wenn es kein $\varphi \in \mathcal{C}_{k,m}$ gibt mit $\mathcal{G} \models \varphi$ aber $\mathcal{H} \not\models \varphi$).

**Satz 5.3.** *Hat Spieler II eine Gewinnstrategie für das $\mathcal{C}_k$-Spiel mit $r$ Zügen auf $\mathcal{G}$ und $\mathcal{H}$ mit Startkonfiguration $(u, v)$, so gilt $\mathcal{G}, u \equiv_{\mathcal{C}_{k,r}} \mathcal{H}, v$.*

*Beweis.* Wir führen eine vollständige Induktion über die Anzahl der Züge $r$.

Gewinnt Spieler II das Spiel nach 0 Zügen, dann ist durch $(u, v)$ bereits ein Isomorphismus gegeben. Damit ist klar, dass $\mathcal{G}$ und $\mathcal{H}$ sich durch quantorenfreie Formeln, deren freie Variablen eine Teilmenge von $D_u = D_v$ sind, nicht unterscheiden lassen.

Angenommen, die Behauptung gelte für alle $m < r$. Wir führen einen Widerspruchsbeweis und nehmen an, dass es eine Formel $\varphi \in \mathcal{C}_{k,r}$ gibt, deren freie Variablen eine Teilmenge von $D_u = D_v$ sind, so dass $\mathcal{G} \models \varphi$ aber $\mathcal{H} \not\models \varphi$. Ohne Einschränkung können wir davon ausgehen, dass $\varphi$ von der Form $\exists^{\geq N} x_i \psi$ ist. Wäre $\varphi$ eine Konjunktion, so würde schon ein Konjunkt ausreichen um $\mathcal{G}$ und $\mathcal{H}$ zu unterscheiden; wäre $\varphi$ eine Disjunktion, so würde ein Konjunkt von $\neg\varphi$ ausreichen, und wäre $\varphi$ von der Form $\forall x \psi(x)$, so würde $\exists x \neg\psi(x)$ ausreichen. Zusäztlich können wir $i = k$ annehmen, d.h. der Stein $x_i$ ist im Spiel momentan noch nicht platziert.

Wir geben nun eine Gewinnstrategie für Spieler I, von der aktuellen Position $(u, v)$ aus, an.

**I:** Im ersten Zug wählt Spieler I einen Stein $x_k$ und eine Teilmenge $A$ von $\mathcal{G}$ mit $|A| = N$, so dass $\psi$ in $\mathcal{G}$ gilt, wenn $x_k$ durch $g$ interpretiert wird für jedes $g \in \mathcal{G}$. So eine Menge existiert nach Voraussetzung ($\varphi$ gilt in $\mathcal{G}$).

**II:** Spieler II wählt eine Menge $B$ von Knoten in $\mathcal{H}$. Es existiert nach Voraussetzung mindestens ein $h \in B$, so dass $\psi$ in $\mathcal{H}$ nicht gilt, wenn $x_k$ durch $h$ interpretiert wird (denn $\varphi$ gilt in $\mathcal{H}$ nicht, d.h. es kann höchstens $N - 1$ Elemente geben, die $\psi$ erfüllen).

**I:** Spieler I legt nun seinen Stein $x_k$ auf dieses $h$.

**II:** Spieler II antwortet mit einem beliebigen $g \in A$.

Wird also $x_k$ in $\mathcal{G}$ durch $g$ interpretiert und in $\mathcal{H}$ durch $h$, so unterscheiden sich die beiden Strukturen durch $\psi$. Der Quantorenrang von $\psi$ ist nun aber $r-1$. Per Induktion verliert Spieler II das $(r-1)$-Züge-Spiel. □

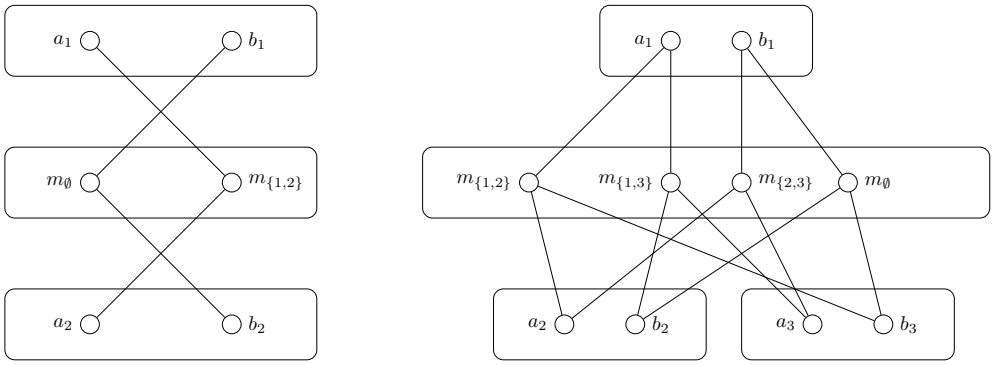
## 5.4 Identifizierbarkeit von Graphklassen mit $\mathcal{C}_k$

Ziel des nächsten Abschnitts ist die Konstruktion eines Gegenbeispiels für die Vermutung, dass die Logik $\mathcal{C}_k$ jede in Polynomialzeit entscheidbare Klasse von Graphen identifiziert. Wir werden bestimmte Paare von Graphen $\mathcal{G}_k$ und $\mathcal{H}_k$ angeben, die nicht isomorph sind, aber exakt die gleichen $\mathcal{C}_k$-Sätze erfüllen.

**Definition 5.4.** *Sei $\mathcal{X}_k = (V_k, E_k)$ der wie folgt definierte Graph:*

- $V_k := A_k \dot\cup B_k \dot\cup M_k$, *mit*
- $A_k := \{a_i \mid 1 \leq i \leq k\}$,
- $B_k := \{b_i \mid 1 \leq i \leq k\}$,
- $M_k := \{m_S \mid S \subseteq \{1,...,k\}, |S| \text{ gerade}\}$ *und*
- $E_k := \{(m_S, a_i) \mid m_S \in M_k, i \in S\} \dot\cup \{(m_S, b_i) \mid m_S \in M_k, i \notin S\}$.

*Zusätzlich seien die Knoten der Menge $\{a_i, b_i\}$ mit der Farbe $i$ gefärbt und alle Knoten in $M_k$ mit einer weiteren Farbe.*




(a) $\mathcal{X}_2$ (b) $\mathcal{X}_3$

Abbildung 1: Beispielgraphen zu Definition 5.4

Die Teilmenge $M_k$ der Knoten von $\mathcal{X}_k$ enthält also genau $2^{k-1}$ Knoten (es gibt $2^k$ Teilmengen von $\{1,...,k\}$ und nur genau die Hälfte davon enthält geradzahlig viele Elemente). Jeder Knoten in $M_k$ ist für jedes $1 \leq i \leq k$ entweder mit $a_i$ oder $b_i$ verbunden, d.h. die Knoten in $M_k$ haben alle Grad $k$.

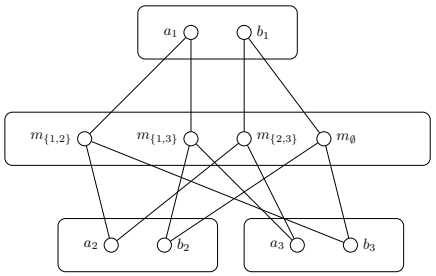
Wie bereits oben erwähnt muss jeder Isomorphismus die Färbung der Knoten respektieren. Insbesondere muss also jeder Automorphismus von $\mathcal{X}_k$ die Mengen $\{a_i, b_i\}$ fest lassen.

**Lemma 5.5** (Automorphismen von $\mathcal{X}_k$)**.** *Eine Permutation $\pi$ der Knoten $A_k \dot\cup B_k$, die für jedes $1 \leq i \leq k$ die Menge $\{a_i, b_i\}$ fest lässt, kann genau dann zu einem Automorphismus von $\mathcal{X}_k$ forgesetzt werden, wenn $\pi(a_i) = b_i$ und $\pi(b_i) = a_i$ für eine gerade Anzahl von Paaren $\{a_i, b_i\}$ gilt.*

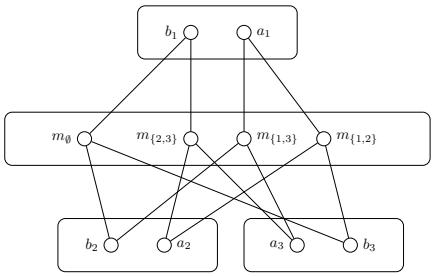
Per Definition kann jeder solche Automorphismus eindeutig durch einen Knoten $m_S \in M_k$ kodiert werden (nämlich durch den Knoten $m_S$, wobei $S$ die Menge der $i$ ist, für die $\pi(a_i) = b_i$ und $\pi(b_i) = a_i$ gilt). Es gibt also $2^{k-1}$ Automorphismen von $\mathcal{X}_k$.

*Beweis.* Sei $\pi$ eine Permutation der Knoten $A_k \cup B_k$ mit $\pi(\{a_i, b_i\}) = \{a_i, b_i\}$ für alle $1 \leq i \leq k$ und $\pi(a_i) = b_i$ für eine gerade Anzahl von $i$. Um $\pi$ zu einem Automorphismus fortzusetzen, müssen die Bilder der Knoten aus $M_k$ festgelegt werden. Jedes $m_S \in M_k$ ist per Definition eindeutig festgelegt durch die Angabe seiner $k$ Nachbarn. Damit $\pi$ ein Automorphismus ist, müssen Kanten erhalten bleiben, d.h. für $(v, w) \in E_k$ muss $(\pi(v), \pi(w)) \in E_k$ gelten. Eine Kante $(v, w)$ ist per Definition entweder von der Form $(m_S, a_i)$ für ein $S$ mit $i \in S$ oder von der Form $(m_S, b_i)$ für ein $S$ mit $i \notin S$. Auf diese Weise erhält man damit die $k$ Nachbarn von $\pi(m_S)$. Tauscht $\pi$ eine gerade Anzahl von $a_i$ mit $b_i$, so sind eine gerade Anzahl dieser $k$ Nachbarn $a$-Knoten und $\pi(m_S)$ damit wohldefiniert. □

**Beispiel 5.6.** Wir betrachten als Beispiel erneut den Graphen $\mathcal{X}_3$ und wählen den Automorphismus, der durch $m_{\{1,2\}}$ induziert wird, d.h. $a_1$ und $b_1$ sowie $a_2$ und $b_2$ werden vertauscht, $a_3$ und $b_3$ werden fest gelassen. Wegen $(a_1, m_{\{1,2\}})$, $(a_2, m_{\{1,2\}})$, $(b_3, m_{\{1,2\}}) \in E_k$ folgt, dass $f(m_{\{1,2\}}) = m_\emptyset$ gelten muss, denn $m_\emptyset$ ist das einzige Element aus $M_k$, dass $(f(a_1), m_\emptyset), (f(a_2), m_\emptyset), (f(b_3), m_\emptyset) \in E_k$ erfüllt. Die anderen drei $f(m_{S'})$ erhält man analog (siehe Abbildung).




(a) $\mathcal{X}_3$




(b) Bild von $\mathcal{X}_3$ unter dem durch $m_{\{1,2\}}$ induzierten Automorphismus; $a_1$ und $b_1$ sowie $a_2$ und $b_2$ wurden getauscht. Die Bilder der Elemente in $M_k$ sind dadurch bereits festgelegt.

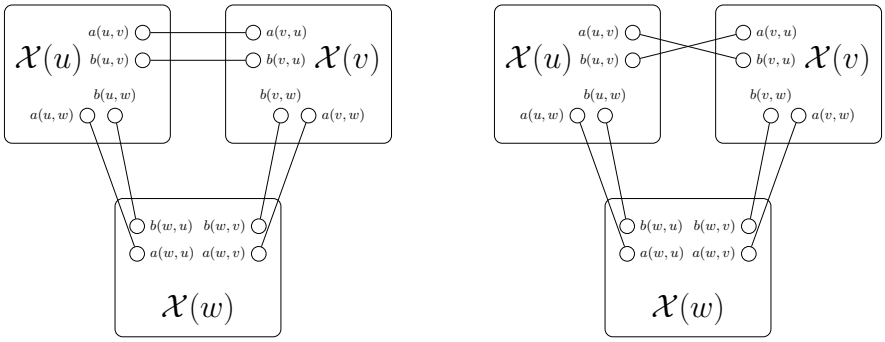
Abbildung 2: Graphen zu Beispiel 5.6

**Definition 5.7** ($\mathcal{X}(\mathcal{G})$)**.** *Sei $\mathcal{G}$ ein endlicher zusammenhängender ungerichteter Graph, so dass jeder Knoten mindestens Grad 2 hat. Dann bezeichnen wir mit $\mathcal{X}(\mathcal{G})$ einen Graphen, den man erhält, indem man jeden Knoten $v$ in $\mathcal{G}$ durch eine Kopie von $\mathcal{X}_k$ existiert, die wir $\mathcal{X}(v)$ nennen, wobei $k$ der Grad von $v$ ist. Ist $\mathcal{G}$ gefärbt, so erhält jeder Knoten von $\mathcal{X}(v)$ als zusätzliche zweite Farbe die Farbe von $v$. Jeder Kante $(v, w)$ in $\mathcal{G}$ wird eines der Paare $\{a_i, b_i\}$ von $\mathcal{X}(v)$ zugeordnet, im Folgenden mit $\{a(v, w), b(v, w)\}$ bezeichnet. Nun verbinden wir in $\mathcal{X}(\mathcal{G})$ die $a$-Knoten und die $b$-Knoten jeder Kante, d.h. für jede Kante $(u, v)$ in $\mathcal{G}$ gibt es in $\mathcal{X}(\mathcal{G})$ zwei Kanten $(a(u, v), a(v, u))$ und $(b(u, v), b(v, u))$. Diese neuen Kanten sind also in $\mathcal{X}(\mathcal{G})$ die einzigen Kanten, die die einzelnen $\mathcal{X}(v)$ miteinadner verbinden.*

**Definition 5.8.** *Mit $\tilde{\mathcal{X}}(\mathcal{G})$ bezeichnen wir einen Graphen, den man aus $\mathcal{X}(\mathcal{G})$ erhält, indem man genau eine beliebige Kante $(v, w)$* verdreht*, d.h. man fügt Kanten $(a(u, v), b(v, u))$ und $(b(u, v), a(v, u))$ hinzu statt $(a(u, v), a(v, u))$ und $(b(u, v), b(v, u))$. Mit $\hat{\mathcal{X}}(\mathcal{G})$ bezeichnen wir einen Graphen, den man erhält, indem man genau $t$ Kanten in $\mathcal{X}(\mathcal{G})$ verdreht.*

Die Wahl der zu verdrehenden Kanten in Definition 5.8 spielt keine Rolle, wie das folgende Lemma deutlich macht.

**Lemma 5.9.** *Die Graphen $\hat{\mathcal{X}}(\mathcal{G})$ und $\mathcal{X}(\mathcal{G})$ sind genau dann isomorph, wenn $t$ gerade ist, anderenfalls sind $\hat{\mathcal{X}}(\mathcal{G})$ und $\tilde{\mathcal{X}}(\mathcal{G})$ isomorph. Insbesondere sind $\mathcal{X}(\mathcal{G})$ und $\tilde{\mathcal{X}}(\mathcal{G})$ nicht isomorph.*




(a) $\mathcal{X}(\mathcal{G})$, jeder Knoten wurde ersetzt durch eine Kopie von $\mathcal{X}_2$

(b) $\tilde{\mathcal{X}}(\mathcal{G})$, die Kante $(u,v) \in E_\mathcal{G}$ wurde *verdreht*

Abbildung 3: Beispiel zu Definition 5.7 und Definition 5.8

*Beweis.* Sei $v$ ein Knoten von $\mathcal{G}$, dann hat $v$ nach Voraussetzung mindestens zwei Nachbarn, etwa $u$ und $w$. Betrachte jetzt den Graphen $\hat{\mathcal{X}}(\mathcal{G})$ (für ein $t$). Sei $a_i := a(v,u)$ und $a_j := a(w,u)$ und $S := \{i,j\} \subseteq \{1,...,k\}$ (wobei $k$ der Grad von $v$ ist). Dann wird nach Lemma 5.5 durch $S$ ein Automorphismus induziert, der genau $a_i$ mit $b_i$ und $a_j$ mit $b_j$ vertauscht. Damit folgt, dass der Graph, den man aus $\hat{\mathcal{X}}(\mathcal{G})$ erhält, indem man die beiden Kanten $(v,u)$ und $(v,w)$ verdreht, selbst wieder isomorph ist zu $\hat{\mathcal{X}}(\mathcal{G})$.

Sei nun $t \geq 2$ die Anzahl der Verdrehungen in $\hat{\mathcal{X}}(\mathcal{G})$. Durch wiederholtes Anwenden der Automorphismen der einzelnen $\mathcal{X}(v)$ lassen sich die Verdrehungen aufeinander zu bewegen bis sie sich gegenseitig aufheben. Dadurch wird klar, dass, falls $t$ gerade ist, $\hat{\mathcal{X}}(\mathcal{G})$ isomorph ist zu $\mathcal{X}(\mathcal{G})$ und anderenfalls ($t$ ungerade) $\hat{\mathcal{X}}(\mathcal{G})$ isomorph zu $\tilde{\mathcal{X}}(\mathcal{G})$ ist (da in diesem Fall immer genau eine Verdrehung übrig bleibt, die man mit keiner weiteren rückgängig machen kann).

Es bleibt zu zeigen, dass $\mathcal{X}(\mathcal{G}) \ncong \tilde{\mathcal{X}}(\mathcal{G})$. Angenommen es gäbe einen Isomorphismus $f$ von $\mathcal{X}(\mathcal{G})$ nach $\tilde{\mathcal{X}}(\mathcal{G})$, dann muss dieser mit der Färbung verträglich sein, d.h. in jedem $\mathcal{X}(v)$ muss $f(\{a_i, b_i\}) = \{a_i, b_i\}$ gelten. Insbesondere muss also für jede Kante $(v,w)$ in $\mathcal{G}$ gelten, dass $f(\{a(v,w), b(v,w)\}) = \{a(v',w'), b(v',w')\}$ für irgendwelche $v', w'$ in $\mathcal{G}$ (und auf Grund der Kanten damit auch $f(\{a(w,v), b(w,v)\}) = \{a(w',v'), b(w',v')\}$). Wir wollen nun die Anzahl der Fälle zählen, für die $f$ einen solchen $a$-Knoten auf einen $b$-Knoten abbildet. Aufgrund der Kantenrelation, die $f$ erhalten muss, ist klar, dass $f$ für jede Kante $(v,w)$ in $\mathcal{G}$ entweder $a(w,v)$ und $a(v,w)$ beide auf $a$-Knoten abbildet oder beide auf $b$-Knoten abbildet, d.h. die Anzahl ist hier 0 oder 2, abgesehen von der Kante, die in der Konstruktion von $\tilde{\mathcal{X}}(\mathcal{G})$ verdreht wurde. Für diese ist die Anzahl 1. Die Anzahl der Verdrehungen insgesamt ist also auf jeden Fall ungerade. Für jede Kopie von $\mathcal{X}_k$ in $\mathcal{X}(\mathcal{G})$ ist nach Lemma 5.5 aber klar, dass die Anzahl gerade sein muss (da die Größe jeder Menge $S$ gerade ist und es keinen solchen Automorphismus gibt, der ungerade viele $a_i$ mit $b_i$ tauscht). Also kann es ein solches $f$ nicht geben. □

**Definition 5.10** (Separator)**.** *Ein* Separator *eines Graphen $\mathcal{G} = (V,E)$ ist eine Knotenteilmenge $S \subseteq V$, so dass der von $V \setminus S$ induzierte Graph keine Zusammenhangskomponente mit mehr als $|V|/2$ Knoten enthält.*

**Satz 5.11.** *Sei $\mathcal{T}$ ein zusammenhängender Graph, so dass alle Knoten verschiedene Farben haben und jeder Separator von $\mathcal{T}$ mindestens $s+1$ Knoten hat. Dann gilt $\mathcal{X}(\mathcal{T}) \equiv_{\mathcal{C}_s} \tilde{\mathcal{X}}(\mathcal{T})$.*

*Beweis.* Nach Satz 5.3 reicht es, eine Gewinnstrategie für Spieler II im $\mathcal{C}_s$-Spiel anzugeben.

Sei $M(v)$ die Menge $M_k \subseteq \mathcal{X}_k$ eines $\mathcal{X}(v)$. Mit $P_r$ bezeichnen wir die Menge der Knoten $g$ in $\mathcal{T}$, so dass auf einem Knoten in $\mathcal{X}(g)$ nach $r$ Zügen ein Stein liegt. Es gilt $|P_r| \leq s$

und da $T$ keine Separatoren der Größe $\leq s$ hat, kann $P_r$ kein Separator von $T$ sein. Also gibt es eine Zusammenhangskomponente von $T \setminus P_r$, die mehr als die Hälfte der Knoten enthält. Diese größte Zusammenhangskomponente (nach $r$ Zügen) bezeichnen wir mit $Q_r$. Für $g \in Q_r$ bezeichnen wir mit $\mathcal{X}^g(\mathcal{T})$ den Graphen, den man aus $\mathcal{X}(\mathcal{T})$ erhält, indem man eine Kante, die adjazent zu $g$ ist, verdreht. Es gilt $\mathcal{X}^g(\mathcal{T}) \cong \tilde{\mathcal{X}}(\mathcal{T})$ nach Lemma 5.9.

Anschaulich: Spieler I versucht die Verdrehung aufzuzeigen wobei Spieler II versucht sie zu verstecken. Die Strategie von Spieler II wird sein, die Verdrehung innerhalb der zusammenhängenden steinfreien Komponente $Q_r$ zu verstecken. Diese Strategie wird erfolgreich sein, da die aufeinander folgenden Komponenten $Q_r$, $Q_{r+1}$ sich überschneiden.

**Lemma 5.12.** *Spieler I hat keinen Vorteil dadurch, dass er mehrfarbige Mengen $A$ wählt. D.h. falls er mit einfarbigen Mengen verliert, so verliert er auch mit mehrfarbigen.*

Es kann also ohne Einschränkung angenommen werden, dass Spieler I nur einfarbige Mengen wählt.

*Beweis.* Angenommen Spieler I verliert einfarbig, dann hat Spieler II eine Gewinnstrategie $\sigma$ für den einfarbigen Fall. Betrachte nun das Spiel ohne diese Einschränkung, d.h. Spieler I darf auch mehrfarbige Mengen $A$ wählen.

Spieler I wähle nun eine Menge $A$. Sei $F$ die Menge der Farben der Knoten in $A$ und für $f \in F$ sei $A_f$ die Teilmenge der Knoten in $A$ der Farbe $f$. Sei $B_f$ die Menge, die Spieler II im einfarbigen Fall nach seiner Strategie $\sigma$ wählen würde, falls Spieler I dort die Menge $A_f$ wählt.

Die Antwort von Spieler II ist nun die folgende:

$$B := \bigcup_{f \in F} B_f,$$

d.h. er wählt für jede Farbe $f$ seine Antwort separat nach seiner einfarbigen Strategie.

Da die Teilmengen $B_f$ disjunkt sind (sie bilden eine Partition von $B$) und $|A_f| = |B_f|$ für alle $f$ gilt (denn Spieler II gewinnt einfarbig!), folgt $|A| = |B|$.

Spieler I platziert nun einen $x_i$-Stein auf einem Knoten aus $B$. Dieser Knoten gehört zu genau einer der Teilmengen $B_f$. Spieler II kann diesen Zug nun mit $\sigma$ beantworten um einen Knoten aus $A_f \subseteq A$ zu wählen.

Da Spieler II auf diese Weise beliebig lange weiter spielen kann, verliert Spieler I.

□

Per Definition sind innerhalb eines $\mathcal{X}(v)$ die Knoten $a_i$ und $b_i$ mit Farbe $i$ gefärbt und alle Knoten in $M(v)$ sind gleich gefärbt. Zusätzlich erhält per Definition von $\mathcal{X}(\mathcal{T})$ jeder Knoten in $\mathcal{X}(v)$ eine zweite Farbe, nämlich die von $v$. Per Annahme haben alle Knoten in $T$ verschiedene Farben. Zusammen mit Lemma 5.12 folgt: Ohne Einschränkung wählt Spieler I nur innerhalb eines $\mathcal{X}(v)$ und dort nur Knoten mit gleicher Farbe, d.h. entweder $A \subseteq \{a_i, b_i\}$ für ein $i$ oder $A \subseteq M(v)$.

**Lemma 5.13.** *Spieler I hat keinen Vorteil dadurch, dass er $A \subseteq \{a_i, b_i\}$ wählen kann.*

*Beweis.* Angenommen Spieler I könnte die Verdrehung aufzeigen indem er $A \subseteq \{a_i, b_i\}$ wählt für ein $i$. Dann hätte er nach Lemma 5.5 dies auch schon durch Wahl eines $m_S \in M(v)$ mit $i \in S$ tun können, denn durch Wahl eines Knoten aus $M_k$ sind bereits alle anderen Knoten in $\mathcal{X}(v)$ festgelegt. □

Es kann also ohne Einschränkung angenommen werden, dass Spieler I nur Mengen $A \subseteq M(v)$ wählt.

**Lemma 5.14.** *Spieler I hat keinen Vorteil dadurch, Mengen A mit $|A| > 1$ zu wählen.*

Die Möglichkeit zu zählen hilft Spieler I hier also nicht.

*Beweis.* Angenommen Spieler I könnte die Verdrehung aufzeigen, indem er eine Menge mit mehr als einem Element wählt, dann könnte er dies nach Lemma 5.5 bereits mit einem einzigen $m_S$ tun. □

Es ist also keine Einschränkung anzunehmen, Spieler I wähle in jedem Zug nur *einelementige* Mengen $A = \{m_S\} \subseteq M(v)$ (für ein $S$).

Betrachte nun die folgende Bedingung, die Spieler II im Laufe des Spiels erhalten kann:

(*) Für jeden Knoten $g \in Q_r$ gibt es (nach $r$ Zügen) einen Isomorphismus $\alpha_{r,g} : \mathcal{X}^g(\mathcal{T}) \xrightarrow{\cong} \tilde{\mathcal{X}}(\mathcal{T})$, welcher die Platzierung der Steine respektiert (d.h. Knoten, auf denen ein $x_i$-Stein liegt werden auf solche abgebildet).

Falls (*) erfüllt ist, gewinnt Spieler II, denn dann ist die Abbildung, die die Steine im ersten Graphen auf die Steine im zweiten Graphen abbildet ein partieller Isomorphismus und Spieler II kann die Züge von Spieler I entsprechend des Isomorphismus $\alpha_{r,g}$ beantworten.

Wir zeigen per Induktion nach $r$, dass Spieler II die Bedingung (*) beibehalten kann.

Nach $r = 0$ Zügen sind noch keine Steine platziert und $Q_0 = \mathcal{T}$ ist die größte Zusammenhangskomponente von $\mathcal{T} \setminus P_0 = \mathcal{T}$. Nach Lemma 5.9 ist $\mathcal{X}^g(\mathcal{T}) \cong \tilde{\mathcal{X}}(\mathcal{T})$ und da keine Steine respektiert werden müssen, ist (*) erfüllt.

Angenommen (*) gilt nach $r$ Zügen und Spieler I platziert im $(r+1)$-ten Zug einen $x_i$-Stein auf einem Knoten in $M(w)$ für ein $w$. Da $Q_r$ und $Q_{r+1}$ beide mehr als die Hälfte der Knoten enthalten, sind sie nicht disjunkt, also sei etwa $g \in Q_r \cap Q_{r+1}$. Definiere $\alpha_{r+1,g} := \alpha_{r,g}$. Da $Q_{r+1}$ zusammenhängend ist, existiert zu jedem Knoten $h \in Q_{r+1}$ ein Pfad zu $g$. Analog zum Beweis von Lemma 5.9 lässt sich die Verdrehung durch wiederholte Anwendung von Automorphismen von $h$ zu $g$ „verschieben“, die Komposition dieser Automorphismen bezeichnen wir mit $\pi : \mathcal{X}^h(\mathcal{T}) \xrightarrow{\cong} \mathcal{X}^g(\mathcal{T})$. Dann ist $\alpha_{r+1,h} := \pi \circ \alpha_{r,g}$ ein Isomorphismus. Da $Q_{r+1}$ nur Knoten enthält, auf denen keine Steine platziert sind, der Pfad von $h$ zu $g$ also steinfrei ist (und $\pi$ damit alle Knoten, auf denen Steine liegen, fest lässt), erfüllt $\alpha_{r+1,h}$ für jedes $h \in Q_{r+1}$ die Bedingung (*).

□

**Folgerung 5.15.** *Sei $\mathcal{G}_k := \mathcal{X}(\mathcal{T}_k)$ und $\mathcal{H}_k := \tilde{\mathcal{X}}(\mathcal{T}_k)$ wobei $\mathcal{T}_k$ ein zusammenhängender Graph ist, in dem alle Knoten verschiedene Farben haben und für den jeder Separator mindestens $k+1$ Knoten hat. Dann sind $\mathcal{G}_k$ und $\mathcal{H}_k$ durch $\mathcal{C}_k$-Sätze nicht unterscheidbar.*

Dass es solche Graphen $\mathcal{T}_k$ tatsächlich gibt, kann z.B. in [8] nachgelesen werden.

## 5.5 Konsequenzen für IFP+C und PTIME

Man kann zeigen, dass aus Satz 5.11 folgt, dass auch keine IFP+C Formel die beiden Graphen $\mathcal{X}(\mathcal{T}_k)$ und $\tilde{\mathcal{X}}(\mathcal{T}_k)$ unterscheiden kann. Da sie sich aber in Polynomialzeit unterscheiden lassen, erhält man den gewünschten Widerspruch:

**Satz 5.16.** *IFP+C erfasst* PTIME *nicht.*

*Beweis.* Angenommen es existiert eine Formel $\varphi \in$ IFP+C, die die Graphen unterscheiden kann. Sei $k$ die Anzahl der Variablen in $\varphi$ und $n$ die Größe der Graphen.

Man kann eine Formel $\varphi_n$ angeben, die für Graphen der Größe maximal $n$ äquivalent ist zu $\varphi$. Die genaue Konstruktion ist sehr technisch und kann in [5] nachgelesen werden, daher geben wir hier nur eine Skizze an:

Fixpunkte werden „abgewickelt“ (Idee: Wenn die Größe der Struktur bekannt ist, ist auch die Anzahl der Fixpunktiterationen nach oben beschränkt und jeder Iterationsschritt kann durch eine Formel beschrieben werden). Als kurzes Beispiel betrachten wir die, in Beispiel 3.6 bereits erwähnte, Formel zur Beschreibung von Erreichbarkeit in Graphen:

$$[\text{ifp } Txy.(x = y) \vee \exists z(Exz \wedge Tzy)](xy).$$

Diese ist für Graphen der Größe kleinergleich 5 äquivalent zu:

$$x = y \vee \exists z(Exz \wedge (Ezy \vee \exists x(Ezx \wedge (Exy \vee \exists z(Exz \wedge Ezy))))).$$

Die Quantoren der Form $\exists\mu$ lassen sich, falls die Größe der Struktur nach oben beschränkt ist, durch Disjunktionen der Form $\bigvee_{i=0}^{n}$ ersetzen, z.B. kann die Formel $\exists\mu\exists^{\geq\mu}x\varphi(x)$ durch $\bigvee_{i=0}^{n}\exists^{\geq i}x\varphi(x)$ ersetzt werden. Die Anzahl der Variablen erhöht sich durch diese Konstruktionen nicht, d.h. $\varphi_n \in \mathcal{C}_k$ und $\varphi_n$ unterscheidet die Graphen auch, im Widerspruch zu Satz 5.11. □

# 6 Schlusswort

Obwohl IFP+C, im Vergleich zu FO, relativ ausdrucksstark ist, gibt es immernoch einige einfache Eigenschaften, von denen nicht bekannt ist, ob sie sich in IFP+C ausdrücken lassen [2].

Wir haben gesehen, dass Inflationäre Fixpunktlogik mit Zählquantoren (IFP+C) im Allgemeinen nicht ausreicht um PTIME zu erfassen. Es stellt sich also die Frage, welche Logik dies leistet (und ob es sich dabei eventuell um eine Erweiterung von IFP+C handelt). Diese Frage ist bis heute unbeantwortet.

Wie bereits erwähnt hätte eine negative Antwort auf diese Frage weitreichende Konsequenzen: Falls es keine Logik für PTIME gibt, so muss zwangsläufig PTIME $\neq$ NP gelten.

# Literatur

[1] Erich Grädel. *Mathematische Logik (Skript zur Vorlesung).* http://www.logic.rwth-aachen.de/files/MaLo/script.pdf, 2006.

[2] Erich Grädel, Dietmar Berwanger. Open Problems in Finite Model Theory. *http://www.logic.rwth-aachen.de/FMT/problems.pdf*, page 1, 2003.

[3] Erich Grädel, Martin Otto. Inductive Definability with Counting on Finite Structures. *Lecture Notes in Computer Science, no. 702*, pages 231–247, 1993.

[4] Erich Grädel. Finite Model Theory and Descriptive Complexity. *Finite Model Theory and Its Applications*, 2007.

[5] Heinz-Dieter Ebbinghaus, Jörg Flum. *Finite Model Theory.* Springer-Verlag, 1995.

[6] Jin-Yi Cai, Martin Fürer, Neil Immerman. An optimal lower bound on the number of variables for graph identification. *Combinatorica*, pages 389–410, 1992.

[7] Jorg Flum, Martin Grohe. On Fixed-Point Logic with Counting. *Journal of Symbolic Logic, Vol 65, No. 2*, pages 777–787, 2000.

[8] M. Ajtai. Recursive Construction for 3-Regular Expanders. *28th IEEE Symp. on Foundations of Computer Science*, pages 295–304, 1987.

[9] Martin Otto. Fixed-Point Logic with Counting. *Bounded Variable Logics and Counting: A Study in Finite Models*, pages 97–114, 1997.

[10] Neil Immerman. Relational queries computable in polynomial time. *Information and control, vol. 68*, pages 86–104, 1986.

[11] Stephan Kreutzer. Expressive Equivalence of Least and Inflationary Fixed-Point Logic. *Proceedings of the 17th IEEE Symp. on Logic in Computer Science (LICS)*, 2002.