Master-Arbeit

Logische Charakterisierungen von Symmetrischen Schaltkreisfamilien

Christoph Burschka

15. Mai 2016

Goethe-Universität Frankfurt am Main

Institut für Informatik

Inhaltsverzeichnis

1 Einleitung

Wir modellieren Graphen und Datenbanken als Strukturen, die ein Schema von relationalen Prädikaten über einem endlichen Universum interpretieren. Eine Datenbank-Anfrage in einem solchen Schema wird als Funktion modelliert, die jede endliche Struktur auf eine Relation abbildet.

Von besonderem Interesse ist die Daten-Komplexität solcher Anfragen: Die Zeit- und Platzkomplexität der Auswertung einer festen Anfrage in Abhängigkeit von der Größe der eingegebenen Struktur. Wir betrachten zwei Modelle, in denen alle beschreibbaren Anfragen eine beschränkte Datenkomplexität besitzen:

1. Klassen von booleschen Schaltkreisfamilien $(\mathcal{C}_n)_{n\in\mathbb{N}}$ (mit `AND-`, `OR-`, `NOT-`, und gegebenenfalls Majority-Gates).
2. Formeln der Prädikatenlogik erster Stufe (beziehungsweise deren Erweiterungen).

Boolesche Schaltkreise arbeiten per Definition auf einer geordneten Struktur. Für ungeordnete Strukturen wird deshalb eine beliebige Ordnung gewählt und gefordert, dass das Ergebnis bezüglich der Ordnung invariant ist. Wir führen eine strukturelle Einschränkung (Symmetrie) der Schaltkreise ein, die diese Invarianz garantiert.

Die Schaltkreisfamilie besteht aus einer unendlichen Sequenz von Schaltkreisen für jede Eingabegröße $n \in \mathbb{N}$ ist. Ohne Einschränkung kann eine solche Sequenz auch unentscheidbare Klassen von natürlichen Zahlen kodieren. In der Praxis ist es daher erwünscht, dass die Schaltkreise von einem effizienten Algorithmus berechnet werden: Ist zum Beispiel jeder Schaltkreis in Polynomialzeit oder mit logarithmischem Platz (in Abhängigkeit von n) berechenbar, dann nennen wir die Schaltkreisfamilie P- beziehungsweise LOGSPACE-uniform.

Die Logik erster Stufe ist in der Praxis zu eingeschränkt: Selbst einfache Probleme wie die Frage, ob eine Struktur eine gerade Anzahl von Elementen enthält, oder zwei Knoten durch einen Weg beliebiger Länge verbunden sind, können nicht ausgedrückt werden.[22] Daher erweitern wir die Logik um Fixpunkt-Operatoren, numerische Prädikate und Zähler. Insbesondere betrachten wir Logiken, in denen die numerischen Prädikate *disjunkt* von dem Universum der eigentlichen Struktur interpretiert werden, und weisen nach,

dass solche Logiken gerade die verschiedenen Klassen symmetrischer Schaltkreisfamilien charakterisieren.

Konkret ist die Klasse der symmetrischen P-uniformen booleschen Schaltkreisfamilien SBC^P äquivalent zu der Logik erster Stufe mit Fixpunkt-Operator und disjunktem Ordnungsprädikat $\mathrm{FP} + \mathbf{ORD}$. Das Ergebnis wurde 2014 von Matthew Anderson und Anuj Dawar[1] (nach einem ähnlichen Ergebnis für infinitäre Logik von Martin Otto in 1997[26]) veröffentlicht, und bildet die Grundlage dieser Arbeit.

Die logische Zählerweiterung $\mathrm{FP}+C$ charakterisiert die Schaltkreisklasse $(\mathrm{SBC} + \mathbf{MAJ})^P$ mit einem Majority-Gate, und die Erweiterung der Logik um beliebige numerische Prädikate $\mathrm{FP}+\mathbf{ARB}$ charakterisiert die nicht-uniforme Klasse $\mathrm{SBC}^{P/\mathrm{poly}}$. Diese beiden Erweiterungen sind miteinander kombinierbar.

Theorem 1.1. ***Anderson und Dawar (2014)***

Die folgenden Paare von Anfragenklassen sind auf endlichen Strukturen äquivalent:

1. $\mathrm{FP} + \mathbf{ORD}$ *und* SBC^P
2. $\mathrm{FP} + C$ *und* $(\mathrm{SBC} + \mathbf{MAJ})^P$
3. $\mathrm{FP} + \mathbf{ARB}$ *und* $\mathrm{SBC}^{P/\mathrm{poly}}$

Ein ähnliches Ergebnis gibt es für Schaltkreisfamilien konstanter Tiefe. Es wird eine Charakterisierung der LOGSPACE-uniformen symmetrischen AC^0-Schaltkreisfamilien $(\mathrm{SAC}^0)^{\mathrm{LOGSPACE}}$ durch die Logik $\mathrm{FO}+\mathbf{BIT}$ mit disjunktem `BIT`-Prädikat nachgewiesen.

Theorem 1.2. *Die folgenden Paare von Anfragenklassen sind auf endlichen Strukturen äquivalent:*

1. $\mathrm{FO} + \mathbf{BIT}$ *und* $(\mathrm{SAC}^0)^{\mathrm{LOGSPACE}}$
2. $\mathrm{FO} + \mathbf{BIT} + C$ *und* $(\mathrm{SAC}^0 + \mathbf{MAJ})^{\mathrm{LOGSPACE}}$
3. $\mathrm{FO} + \mathbf{ARB}$ *und* $(\mathrm{SAC}^0 + \mathbf{MAJ})^{P/\mathrm{poly}}$

Die Einschränkung auf symmetrische Schaltkreisfamilien bringt im Allgemeinen eine Reduktion der Ausdrucksstärke mit sich. So wird die Klasse AC^0 durch die invariante Logik $\mathrm{FO}(\mathbf{ARB})$ (Neil Immerman, 1987[16]), und P/poly durch $\mathrm{FP}(\mathbf{ARB})$ (Johann Makowsky, 1997[24, 25]) charakterisiert. $\mathrm{FO}(\mathbf{ARB})$ ist jedoch echt ausdrucksstärker als die disjunkte Variante $\mathrm{FO} + \mathbf{ARB}$:

Theorem 1.3. *Für die* $\mathrm{FO} + \mathbf{ARB}$*-Logik und die arb-invariante* $\mathrm{FO}(\mathbf{ARB})$*-Logik gilt:*

1. *Jede* $(\mathrm{FO} + \mathbf{ARB})\,[\sigma]$*-Formel* φ *beschreibt eine Anfrage, die durch eine arb-invariante* $\mathrm{FO}\,(\mathbf{ARB})\,[\sigma]$*-Formel definierbar ist.*
2. *Es existiert eine* σ*-Anfrage, die in der arb-invarianten* $\mathrm{FO}\,(\mathbf{ARB})\,[\sigma]$*-Logik, aber nicht* $(\mathrm{FO} + \mathbf{ARB})\,[\sigma]$ *definierbar ist.*

Ähnliche Bezüge bestehen vermutlich auch zwischen den symmetrischen und nicht-symmetrischen Teilen der übrigen betrachteten Schaltkreisklassen.

2 Grundlegende Definitionen

2.1 Notation

Zunächst legen wir einige Notationen und Abkürzungen fest. Im folgenden bezeichne $\mathbb{N}$ die Menge der natürlichen Zahlen einschließlich 0, $\mathbb{R}$ die Menge der reellen Zahlen, und „$\leqslant$“ (wenn nicht anders definiert) die natürliche Ordnung von $\mathbb{R}$ und $\mathbb{N}$. Mit „ex.“, „s.d.“ und „f.a.“ kürzen wir gegebenenfalls „es existiert“, „so dass“ und „für alle“ ab.

Definition 2.1. Mengen und Tupel

Mengen benennen wir im allgemeinen durch Großbuchstaben wie A, B, U oder X. Für eine Menge A bezeichne $2^A \coloneqq \{A' \mid A' \subseteq A\}$ die Menge aller Teilmengen von A.

Tupel benennen wir durch Kleinbuchstaben mit Balken wie $\bar{a}$, $\bar{b}$, $\bar{u}$ oder $\bar{x}$. Die Stelligkeit $\mathrm{ar}(\bar{x})$ eines Tupels $\bar{x}$ sei die Anzahl seiner Elemente, und ein n-stelliges Tupel heiße kurz „n-Tupel“. Implizit gelte stets $\bar{x} = \left(x_1, \cdots, x_{|\mathrm{ar}(x)|}\right)$. Die Menge aller k-Tupel einer Menge A sei A^k.

Für ein m-Tupel $\bar{x}$ und ein n-Tupel $\bar{y}$ sei $\bar{x}\bar{y}$ das $(m+n)$-Tupel $(x_1, \cdots, x_m, y_1, \cdots, y_n)$. Das 0-stellige Tupel wird durch $\langle\rangle$ notiert.

Definition 2.2. Intervall

Ein endliches Intervall von natürlichen Zahlen wird durch $[a, b]$ abgekürzt:

$$[a, b] \coloneqq \{i \in \mathbb{N} \mid a \leqslant i \leqslant b\}$$

Ein Intervall von reellen Zahlen wird durch $\mathbb{R}_{[a,b]}$ oder $\mathbb{R}_{[a,b[}$ abgekürzt:

$$\begin{aligned} \mathbb{R}_{[a,b]} &\coloneqq \{i \in \mathbb{R} \mid a \leqslant i \leqslant b\} \\ \mathbb{R}_{[a,b[} &\coloneqq \{i \in \mathbb{R} \mid a \leqslant i < b\} \end{aligned}$$

Als nächstes definieren wir Relationen als Mengen von Tupeln von Elementen eines Universums.

Definition 2.3. Relation

Für eine Menge A und $k \in \mathbb{N}$ sei $R \subseteq A^k$ eine k-stellige Relation über A. Für jede Relation $R \subseteq A^k$ sei $[R] : A^k \to \{0, 1\}$ die folgende Funktion:

$$[R](\bar{a}) \coloneqq \begin{cases} 1 & \text{falls } \bar{a} \in R \\ 0 & \text{sonst} \end{cases}$$

Für geordnete Mengen definieren wir die Operatoren min und max, die das kleinste und größte Element (sofern vorhanden) einer Menge unter einer bestimmten Ordnung bezeichnen.

Definition 2.4. Minimum und Maximum

Für eine Ordnung $\preceq$ auf einer Menge X seien $\min_{\preceq}(X) \in X$ und $\max_{\preceq}(X) \in X$ diejenigen Elemente (sofern vorhanden), so dass für alle Elemente $z \in X$ gilt:

$$\min_{\preceq}(X) \preceq z \preceq \max_{\preceq}(X)$$

Für $X \subseteq \mathbb{R}$ wird die natürliche Ordnung $\leqslant$ nicht explizit notiert. Für eine Funktion $f : U \to \mathbb{R}$ und eine Menge $X \subseteq U$ bezeichnen $\min_{x \in X} f(x) \in \mathbb{R}$ und $\max_{x \in X} f(x) \in \mathbb{R}$ die folgende Abkürzungen:

$$\begin{aligned} \min_{x \in X} f(x) &\coloneqq \min\{f(x) \mid x \in X\} \\ \max_{x \in X} f(x) &\coloneqq \max\{f(x) \mid x \in X\} \end{aligned}$$

Definition 2.5. Asymptotische Klassen

Für jede Funktion $f : \mathbb{N} \to \mathbb{R}$ definieren wir die Funktionsklassen $\mathcal{O}(f)$ und $\Omega(f)$:

- Es gelte $g \in \mathcal{O}(f)$ genau dann wenn ein $n_0, c \in \mathbb{N}$ existieren, so dass für alle $n \geqslant n_0$ gilt: $g(n) \leqslant c \cdot f(n)$.
- Es gelte $g \in \Omega(f)$ genau dann wenn $f \in \mathcal{O}(g)$.

Für $f : \mathbb{R} \to \mathbb{R}$ und eine Klasse $\mathcal{F}$ sei $f(\mathcal{F}) \coloneqq \{f \circ g \mid g \in \mathcal{F}\}$. Zum Beispiel ist $f \in 2^{\mathcal{O}(n)}$ genau dann wenn $f \in \mathcal{O}\left(2^{kn}\right)$ für ein festes $k \in \mathbb{N}$.

Wir legen mehrere einfache Operationen für Abbildungen fest, darunter die Verkettung, Vereinigung disjunkter Definitionsbereiche und Reduktion auf einen Teilbereich.

Definition 2.6. Abbildung

Für eine Abbildung $\pi : A \to B$ und $a \in A$ schreiben wir statt $\pi(a)$ gegebenenfalls πa ohne Klammern.

Jede Abbildung $\pi : A \to B$ wird auf natürliche Weise auf Tupel, Teilmengen und Relationen von A erweitert:

$$\begin{aligned} \pi(x_1, \cdots, x_k) &:= (\pi x_1, \cdots, \pi x_n) \\ \pi\{x_1, \cdots, x_n\} &:= \{\pi x_1, \cdots, \pi x_n\} \end{aligned}$$

Eine Abbildung $\pi : A \to B$ mit $A = \{a_1, \cdots, a_n\}$ schreiben wir gegebenenfalls extensional wie folgt auf. Für ein Tupel $\bar{a} = (a_1, \cdots, a_n)$ kürzen wir diese Abbildung auch durch $(\bar{a} \mapsto \pi\bar{a})$ ab.

$$\begin{aligned} \pi &:= \begin{pmatrix} a_1 & \cdots & a_n \\ \pi a_1 & & \pi a_n \end{pmatrix} \\ \pi &:= (\bar{a} \mapsto \pi\bar{a}) \end{aligned}$$

Für zwei Abbildungen $\pi_1 : B \to C$ und $\pi_2 : A \to B$ sei $\pi_1 \circ \pi_2 : A \to C$ (kurz $\pi_1\pi_2$) die folgende Abbildung:

$$\pi_1\pi_2 := (\bar{a} \mapsto \pi_1(\pi_2(\bar{a})))$$

Für zwei Abbildungen $\pi : A \to B$ und $\pi' : A' \to B'$ mit disjunkten Definitionsbereichen $A \cap A' = \emptyset$ sei $\pi'' := \pi \cup \pi'$ die folgende Abbildung:

$$\begin{aligned} \pi'' &: A \uplus A' \to B \cup B' \\ \pi''x &:= \begin{cases} \pi x & \text{falls } x \in A \\ \pi' x & \text{falls } x \in A' \end{cases} \end{aligned}$$

Für $\pi : A \to B$ und $A' \subseteq A$ sei $\pi_{|A'} : A' \to B$ die Reduktion von π auf eine Teilmenge des Definitionsbereichs, und $\pi_{\setminus A'} : A \setminus A' \to B$ die Reduktion auf das Komplement.

Es sei $\mathbf{id}$ die Identität mit $\mathbf{id}(a) = a$ für alle Elemente a. Mit $\mathbf{id}_X$ bezeichnen wir die Identitätsfunktion auf einer Menge X.

Die Menge $\mathrm{Abb}(A, B)$ bezeichne alle Funktionen $\pi : A \to B$, und $\mathrm{Bij}(A, B)$ bezeichne für endliche $|A| = |B| = n$ alle $n!$ bijektiven Abbildungen $\pi : A \rightleftarrows B$.

Definition 2.7. Permutation

Eine Permutation von U ist eine bijektive Abbildung $\pi : U \rightleftarrows U$. Die Menge aller

Permutationen $\mathrm{Bij}(U,U)$ bezeichnen wir auch als Sym_U. Diese bilden eine Symmetrie-Gruppe bezüglich der Verkettung $\circ$ mit dem neutralen Element $\mathbf{id}_U$.

Es sei π^{-1} die inverse Abbildung mit $\pi^{-1}\pi = \pi\pi^{-1} = \mathbf{id}_U$.

Eine Transposition sei eine Permutation, die zwei Elemente u_i und u_j vertauscht und alle anderen Elemente fixiert. Die Permutation $\begin{pmatrix} u_i & u_j \\ u_j & u_i \end{pmatrix} \cup \mathbf{id}_{U \setminus \{u_i, u_j\}}$ wird kurz durch $(u_i u_j)$ notiert.

Definition 2.8. Orbit

In einer Permutationsgruppe $G \subseteq \mathrm{Sym}_U$ sei $\mathrm{Orb}_G(u) \coloneqq \{\pi u \mid \pi \in G\}$ die Menge aller Elemente, auf die u abgebildet wird.

2.2 Endliche relationale Strukturen

Wir betrachten Anfragen und Eigenschaften auf Graphen und allgemeinen endlichen Strukturen über eine beliebige relationale Signatur σ.

Definition 2.9. Relationale Signaturen

Eine relationale Signatur σ ist eine Menge von Relationssymbolen. Jedes Symbol $R \in \sigma$ hat eine feste Stelligkeit $\mathrm{ar}(R) = k \in \mathbb{N}_{\geqslant 1}$. Gegebenenfalls wird die Stelligkeit kompakt durch $R/k \in \sigma$ beziehungsweise $\sigma = \{R_1/k_1, \cdots, R_k/k_k\}$ notiert.

Definition 2.10. Endliche Strukturen

Eine endliche σ-Struktur $\mathfrak{A} = \left(A, \left(R^{\mathfrak{A}}\right)_{R \in \sigma}\right)$ über einer Signatur σ und einem endlichen nicht-leeren Universum A besteht aus einer Interpretation $R^{\mathfrak{A}} \subseteq A^k$ für jedes Symbol $R/k \in \sigma$. Strukturen benennen wir im Allgemeinen durch die Frakturbuchstaben $\mathfrak{A}$ und $\mathfrak{B}$.

- Für eine endliche Menge U sei $\mathbf{FIN}^U(\sigma)$ die Menge aller σ-Strukturen über dem Universum U.
- Für $n \in \mathbb{N}_{\geqslant 1}$ seien $\mathbf{FIN}^{(n)}(\sigma)$ die σ-Strukturen über einem beliebigen Universum der Größe n.
- Seien $\mathbf{FIN}(\sigma) \coloneqq \bigcup_{n \in \mathbb{N}_{\geqslant 1}} \mathbf{FIN}^{(n)}(\sigma)$ die endlichen σ-Strukturen.

Die Signatur σ kann in Ausnahmefällen unendlich sein; da wir jedoch nur endlich repräsentierbare σ-Anfragen betrachten, können diese sich nur auf eine endlichen Menge von Relationssymbolen $\sigma' \subseteq_{\mathrm{fin}} \sigma$ beziehen.

Wir formalisieren die Interpretation als eine Abbildung $\square^{\mathfrak{A}} : \sigma \to \bigcup_{k\in\mathbb{N}} 2^{\left(A^k\right)}$, die jedem Symbol eine Relation der entsprechenden Stelligkeit zuweist. Daher kann die Interpretation gegebenenfalls auch explizit durch $\mathfrak{A} = \left(A, \square^{\mathfrak{A}}\right)$ notiert werden, um die Zuordnung von Symbolen und Relationen zu verdeutlichen:

$$\mathfrak{A} := \left(A, \begin{pmatrix} R_1 & \cdots & R_k \\ R_1^{\mathfrak{A}} & & R_k^{\mathfrak{A}} \end{pmatrix}\right)$$

Definition 2.11. Geordnete Strukturen

Sei σ eine relationale Signatur, die nicht das zweistellige Symbol $\leqslant$ enthält.

Für $a, b \in \mathbb{N}$ sei

$$\mathbf{FIN}_{\leqslant}^{[a,b]}(\sigma) \subseteq \mathbf{FIN}^{[a,b]}(\sigma \cup \{\leqslant\})$$

die Menge der endlichen $\sigma \cup \{\leqslant\}$-Strukturen mit dem Universum $[a, b]$, wobei $\leqslant$ durch die natürliche Ordnung von $[a, b]$ interpretiert wird, und sei

$$\mathbf{FIN}_{\leqslant}^{a}(\sigma) \coloneqq \bigcup_{b\in\mathbb{N}} \mathbf{FIN}_{\leqslant}^{[a,b]}(\sigma)$$

die Menge aller endlichen geordneten $\sigma \cup \{\leqslant\}$-Strukturen über Intervallen, die mit a beginnen (normalerweise mit $a \in \{0, 1\}$).

Der Lesbarkeit halber verwenden wir die Infixnotation $a \leqslant b$ anstelle von $(a, b) \in \leqslant$ oder $[\leqslant](a, b)$. Die Symbole $\dot{\leqslant}$ und $\doteq$ seien gleichbedeutend mit den Symbolen $\leqslant$ und $=$, und werden gegebenenfalls in Gleichungen wie $\varphi = x \doteq y$ und $\varphi = x \dot{\leqslant} y$ verwendet.

Definition 2.12. Isomorphismus

Für zwei σ-Strukturen $\mathfrak{A}$ und $\mathfrak{B}$ sei eine bijektive Abbildung $\pi : A \rightleftarrows B$ ein Isomorphismus, falls $\pi R^{\mathfrak{A}} = R^{\mathfrak{B}}$ für alle Symbole $R \in \sigma$ gilt.

Die Abbildung π wird auf natürliche Weise auf Strukturen erweitert:

$$\pi\mathfrak{A} \coloneqq \left(\pi A, \left(\pi R^{\mathfrak{A}}\right)_{R\in\sigma}\right)$$

Die Menge aller Isomorphismen bezeichnen wir mit $\mathrm{Bij}(\mathfrak{A}, \mathfrak{B})$. Zwei Strukturen heißen isomorph (kurz $\mathfrak{A} \cong \mathfrak{B}$), falls $\mathrm{Bij}(\mathfrak{A}, \mathfrak{B})$ nicht leer ist.

Ein Automorphismus $\pi \in \mathrm{Bij}(\mathfrak{A}, \mathfrak{A})$ sei ein Isomorphismus von $\mathfrak{A}$ zu sich selbst. Die Menge der Automorphismen $\mathrm{Bij}(\mathfrak{A}, \mathfrak{A})$ nennen wir $\mathrm{Aut}_{\mathfrak{A}}$; diese bilden (so wie die Permutationen einer Menge) eine Gruppe bezüglich der Verkettung $\circ$ und dem neutralen Element $\mathbf{id}_A$.

Der Orbit eines Elements $a \in A$ sei analog zu Definition 2.8 die Menge $\mathrm{Orb}_{\mathfrak{A}}(a) \coloneqq \{\pi a \mid \pi \in \mathrm{Aut}_{\mathfrak{A}}\}$ aller Elemente, auf die a von einem Automorphismus abgebildet werden kann.

Definition 2.13. Vereinigung von Strukturen

Zwei Strukturen können vereinigt werden, wenn sie entweder disjunkte Signaturen oder die gleiche Signatur besitzen. Für eine σ_1-Struktur $\mathfrak{A}$ und eine σ_2-Struktur $\mathfrak{B}$ gelte:

1. Wenn $\sigma_1 \cap \sigma_2 = \emptyset$, so ist $\mathfrak{A} \cup \mathfrak{B}$ die folgende $(\sigma_1 \cup \sigma_2)$-Struktur:

$$\mathfrak{A} \cup \mathfrak{B} \coloneqq \left(A \cup B, \left(R^{\mathfrak{A}}\right)_{R \in \sigma_1}, \left(R^{\mathfrak{B}}\right)_{R \in \sigma_2}\right)$$

2. Wenn $\sigma_1 = \sigma_2 = \sigma$, so ist $\mathfrak{A} \cup \mathfrak{B}$ die folgende σ-Struktur:

$$\mathfrak{A} \cup \mathfrak{B} \coloneqq \left(A \cup B, \left(R^{\mathfrak{A}} \cup R^{\mathfrak{B}}\right)_{R \in \sigma}\right)$$

Falls das Universum der beiden Strukturen ebenfalls disjunkt ist, so heiße $\mathfrak{A} \cup \mathfrak{B} = \mathfrak{A} \uplus \mathfrak{B}$ die **disjunkte Vereinigung** der Strukturen.

Definition 2.14. Induzierte Teilstruktur

Für eine Relation $R \subseteq A^k$ und eine Teilmenge $A' \subseteq A$ sei $R_{|A'} \coloneqq R \cap (A')^k$ die von A' induzierte Teilrelation. Für eine σ-Struktur $\mathfrak{A}$ sei $\mathfrak{A}_{|A'} \coloneqq \left(A', \left(R^{\mathfrak{A}}_{|A'}\right)_{R \in \sigma}\right)$ die von der Teilmenge A' in $\mathfrak{A}$ induzierte Teilstruktur.

Definition 2.15. σ-Anfragen

Eine **σ-Anfrage** q mit der Stelligkeit $\mathrm{ar}(q) = k$ sei eine Abbildung jeder endlichen σ-Struktur $\mathfrak{A} \in \mathbf{FIN}(\sigma)$ auf eine Relation $q(\mathfrak{A}) \subseteq A^k$. Eine **$\sigma$-Eigenschaft** $S \subseteq \mathbf{FIN}(\sigma)$ sei eine Menge von σ-Strukturen und entspreche der 0-stelligen Anfrage q_S:

$$q_S(\mathfrak{A}) \quad \coloneqq \quad \begin{cases} \{\langle\rangle\} & \text{falls } \mathfrak{A} \in S \\ \emptyset & \text{sonst} \end{cases}$$

Per Definition sind alle σ-Anfragen und σ-Eigenschaften unter Isomorphismen abgeschlossen: Für $\mathfrak{A} \cong \mathfrak{B}$ und $\pi \in \mathrm{Bij}(\mathfrak{A}, \mathfrak{B})$ gilt $\pi q(\mathfrak{A}) = q(\mathfrak{B})$ und $\mathfrak{A} \in S \Leftrightarrow \mathfrak{B} \in S$.

3 Logik

3.1 Grundlagen der relationalen Logik

Wir betrachten logische Sprachen auf relationalen Signaturen σ, deren Ausdrücke auf endlichen σ-Strukturen ausgewertet werden.

Zunächst definieren wir **var** als die Menge aller erststufigen Variablen. Für einen Ausdruck ω sei $\mathrm{var}(\omega)$ die Menge der darin vorkommenden Variablen, und $\mathrm{frei}(\omega) \subseteq \mathrm{var}(\omega)$ die Menge der freien Variablen.

In einer Struktur $\mathfrak{A}$ sei eine **Belegung** β eine partielle Abbildung $\beta : \mathbf{var} \to A$ von Variablen auf Elemente des Universums.

Eine Auswertungsfunktion für eine Struktur $\mathfrak{A}$ und eine Belegung β wird durch $[\![\cdot]\!](\mathfrak{A}, \beta)$ notiert.

Definition 3.1. Eine Logik $\mathcal{L}[\sigma]$ besteht aus der Sprache der $\mathcal{L}[\sigma]$-Terme, der Sprache der $\mathcal{L}[\sigma]$-Formeln, und einer Auswertungsfunktion $[\![\omega]\!](\mathfrak{A}, \beta)$ für jede Struktur $\mathfrak{A}$ und Belegung $\beta : X \to A$ und jeden Ausdruck ω mit $\mathrm{frei}(\omega) \subseteq X$.

Für einen $\mathcal{L}[\sigma]$-Term t ist $[\![t]\!](\mathfrak{A}, \beta) \in A$ ein Element des Universums. Für eine $\mathcal{L}[\sigma]$-Formel φ ist $[\![\varphi]\!](\mathfrak{A}, \beta) \in \{0, 1\}$ ein Wahrheitswert.

Notation 3.2. Wir verwenden den Begriff „Ausdruck“ als Oberbegriff der Formeln und Terme einer Logik, und bezeichnen Ausdrücke mit dem Buchstaben ω. Terme werden mit kleinen Buchstaben benannt, und Formeln mit den Buchstaben φ, ψ oder χ.

Definition 3.3. Für eine Formel φ und ein Tupel $\bar{x} \in \mathbf{var}^k$ mit $\mathrm{frei}(\varphi) = \{x_1, \cdots, x_k\}$ und $|\{x_1, \cdots, x_k\}| = k$ nennen wir das Tupel $\bar{x} = (x_1 \cdots x_k)$ ein **Argument** von φ. Verschiedene Argumente von φ unterscheiden sich nur in der Reihenfolge der Variablen. Durch die Notation $\varphi(\bar{x})$ legen wir ein beliebiges Argument $\bar{x}$ für φ fest.

Die **Stelligkeit** einer logischen Formel (beziehungsweise ihrer Argumente) bezeichne die Anzahl der frei vorkommenden Variablen: Für $\varphi(\bar{x})$ gelte:

$$\mathrm{ar}(\varphi) = \mathrm{ar}(\bar{x}) = |\mathrm{frei}(\varphi)|$$

Ein **Satz** sei eine Formel ohne freie Variablen.

Mit $\mathtt{MF}(\omega)$ bezeichnen wir die maximale Anzahl freier Variablen jedes Teilausdrucks von ω.

Definition 3.4. Für eine k-stellige Formel φ und eine Belegung $\beta : \operatorname{frei}(\varphi) \to A$ schreiben wir $\mathfrak{A} \models \varphi^\beta$ genau dann wenn $[\![\varphi]\!](\mathfrak{A}, \beta) = 1$.

Für $\varphi(\bar{x})$ und $\bar{a} \in A^{\operatorname{ar}(\bar{x})}$ schreiben wir $[\![\varphi]\!](\mathfrak{A}, \bar{a})$ anstelle von $[\![\varphi]\!]\left(\mathfrak{A}, \left(\bar{x} \mapsto \bar{b}\right)\right)$, und $\mathfrak{A} \models \varphi[\bar{a}]$ anstelle von $\mathfrak{A} \models \varphi^{\bar{x} \mapsto \bar{a}}$.

Entsprechend sei

$$q_{\varphi(\bar{x})}(\mathfrak{A}) := \left\{\bar{a} \in A^{\operatorname{ar}(\bar{x})} \mid \mathfrak{A} \models \varphi[\bar{a}]\right\}$$

die Relation aller φ erfüllenden Tupel.

Somit beschreibt jede $\mathcal{L}[\sigma]$-Formel $\varphi(\bar{x})$ eine σ-Anfrage $q_{\varphi(\bar{x})}$, und jeder Satz eine σ-Eigenschaft. Da die Reihenfolge der Spalten der Relation von der Wahl des Arguments $\bar{x}$ abhängt, wird es durch $q_{\varphi(\bar{x})}$ mit angegeben.

In manchen Fällen möchten wir einige Variablen einer Formel belegen und sie erst dann als Anfrage auswerten.

Definition 3.5. Für eine Formel φ und eine Belegung $\beta : X \to A$ mit $\operatorname{frei}(\varphi) \nsubseteq X$ sei φ^β ein **partiell belegter** Ausdruck; es sei $\operatorname{frei}\left(\varphi^\beta\right) = \operatorname{frei}(\varphi) \setminus X$.

Für $\beta' : \operatorname{frei}\left(\varphi^\beta\right) \to A$ bezeichne $[\![\varphi^\beta]\!](\mathfrak{A}, \beta')$ die Auswertung $[\![\varphi]\!](\mathfrak{A}, \beta \cup \beta')$. Für ein Argument $\bar{x}'$ von φ^β definieren wir die folgende Anfrage:

$$q_{\varphi^\beta(\bar{x}')} := \left\{\bar{a} \in A^\ell \mid \mathfrak{A} \models \varphi^\beta[\bar{a}]\right\}$$

Definition 3.6. Für eine $\mathcal{L}[\sigma]$-Formel φ und $n \in \mathbb{N}$ drücke $\models_n \varphi$ aus, dass diese von allen σ-Strukturen $\mathfrak{A} \in \mathbf{FIN}^{(n)}(\sigma)$ der Größe n unter allen Belegungen erfüllt wird. Die Notation $\models_{\text{fin}} \varphi$ drücke aus, dass φ von allen endlichen σ-Strukturen $\mathfrak{A} \in \mathbf{FIN}(\sigma)$ unter allen Belegungen erfüllt wird.

Falls $\models_n (\varphi \leftrightarrow \psi)$, so heißen φ und ψ n-**äquivalent**. Insbesondere bedeutet dies, dass φ und ψ die gleiche Anfrage $q_{\varphi(\bar{x})} = q_{\psi(\bar{x})}$ auf Strukturen der Größe n definieren.

3.2 Die Logik erster Stufe

Definition 3.7. Für eine relationale Signatur σ sind die Syntax und Semantik der Logik erster Stufe $\mathrm{FO}[\sigma]$ wie folgt definiert.

(TV) Für jede Variable $x \in \mathbf{var}$ ist x ein FO $[\sigma]$-Term.

$$\operatorname{frei}(x) = \operatorname{var}(x) \coloneqq \{x\}$$

$$[\![x]\!](\mathfrak{A}, \beta) \coloneqq \beta x$$

(AR) Für jedes Relationssymbol $R/k \in \sigma$ und jedes k-Tupel von FO $[\sigma]$-Termen $\bar{x}$ ist $R\bar{x}$ eine FO $[\sigma]$-Formel.

$$\operatorname{frei}(R\bar{x}) \coloneqq \bigcup_{i=1}^{k} \operatorname{frei}(x_i) \qquad \operatorname{var}(R\bar{x}) \coloneqq \bigcup_{i=1}^{k} \operatorname{var}(x_i)$$

$$[\![R\bar{x}]\!](\mathfrak{A}, \beta) \quad \coloneqq \quad \left[R^{\mathfrak{A}}\right]([\![x_1]\!](\mathfrak{A}, \beta), \cdots, [\![x_k]\!](\mathfrak{A}, \beta))$$

(AE) Für zwei FO $[\sigma]$-Terme x_1, x_2 ist $x_1 \doteq x_2$ eine FO $[\sigma]$-Formel.

$$\operatorname{frei}(x_1 \doteq x_2) \coloneqq \bigcup_{i=1}^{2} \operatorname{frei}(x_i) \qquad \operatorname{var}(x_1 \doteq x_2) \coloneqq \bigcup_{i=1}^{2} \operatorname{var}(x_i)$$

$$[\![x \doteq y]\!](\mathfrak{A}, \beta) \quad \coloneqq \quad \begin{cases} 1 & \text{falls } [\![x]\!](\mathfrak{A}, \beta) = [\![y]\!](\mathfrak{A}, \beta) \\ 0 & \text{sonst} \end{cases}$$

(N) Für eine FO $[\sigma]$-Formel φ ist $\neg\varphi$ eine FO $[\sigma]$-Formel.

$$\operatorname{frei}(\neg\varphi) \coloneqq \operatorname{frei}(\varphi) \qquad \operatorname{var}(\neg\varphi) \coloneqq \operatorname{var}(\varphi)$$

$$[\![\neg\varphi]\!](\mathfrak{A}, \beta) \coloneqq 1 - [\![\varphi]\!](\mathfrak{A}, \beta)$$

(J) Für $k \geqslant 2$ FO $[\sigma]$-Formeln $\varphi_1, \cdots, \varphi_k$ und einen Junktor $\gamma \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ (mit $k = 2$ für $\gamma \in \{\rightarrow, \leftrightarrow\}$) ist auch $(\varphi_1 \gamma \cdots \gamma \varphi_k)$ eine FO $[\sigma]$-Formel.

$$\operatorname{frei}(\varphi_1 \gamma \cdots \gamma \varphi_k) \coloneqq \bigcup_{i=1}^{k} \operatorname{frei}(\varphi_i) \qquad \operatorname{var}(\varphi_1 \gamma \cdots \gamma \varphi_k) \coloneqq \bigcup_{i=1}^{k} \operatorname{var}(\varphi_i)$$

$$\begin{aligned}
[\![\varphi_1 \wedge \cdots \wedge \varphi_k]\!](\mathfrak{A}, \beta) &:= \min_{1 \leqslant i \leqslant k} [\![\varphi_i]\!](\mathfrak{A}, \beta) \\
[\![\varphi_1 \vee \cdots \vee \varphi_k]\!](\mathfrak{A}, \beta) &:= \max_{1 \leqslant i \leqslant k} [\![\varphi_i]\!](\mathfrak{A}, \beta) \\
[\![\varphi_1 \to \varphi_2]\!](\mathfrak{A}, \beta) &:= [\![\neg\varphi_1 \vee \varphi_2]\!](\mathfrak{A}, \beta) \\
[\![\varphi_1 \leftrightarrow \varphi_2]\!](\mathfrak{A}, \beta) &:= [\![(\varphi_1 \to \varphi_2) \wedge (\varphi_2 \to \varphi_1)]\!](\mathfrak{A}, \beta)
\end{aligned}$$

(Q) Für einen Quantor $Q \in \{\exists, \forall\}$, eine Variable $x \in \mathbf{var}$ und eine FO $[\sigma]$-Formel φ ist $Qx\varphi$ eine FO $[\sigma]$-Formel.

$$\operatorname{frei}(Qx\varphi) := \operatorname{frei}(\varphi) \setminus \{x\} \qquad \operatorname{var}(Qx\varphi) := \operatorname{var}(\varphi) \cup \{x\}$$

$$\begin{aligned}
[\![\exists x\varphi]\!](\mathfrak{A}, \beta) &:= \max_{a \in A} \left([\![\varphi]\!](\mathfrak{A}, \beta_{\setminus\{x\}} \cup (x \mapsto a))\right) \\
[\![\forall x\varphi]\!](\mathfrak{A}, \beta) &:= \min_{a \in A} \left([\![\varphi]\!](\mathfrak{A}, \beta_{\setminus\{x\}} \cup (x \mapsto a))\right)
\end{aligned}$$

Ohne Beschränkung der Allgemeinheit gelte für $Qx\varphi$ stets $x \in \operatorname{frei}(\varphi)$, denn $Qx\varphi \equiv Qx\,(x \doteq x \wedge \varphi)$.

Wir kürzen $Qx_1 \cdots Qx_k\varphi$ durch $Q\bar{x}\varphi$ und $\bigwedge_{i=1}^{k}(x_i = y_i)$ durch $\bar{x} = \bar{y}$ ab. Im folgenden werden wir im Allgemeinen Formeln ohne Implikations-Pfeile betrachten.

Definition 3.8. Eine FO $[\sigma]$-Formel sei **implikationsfrei** wenn sie keine Teilformel der Form $(\varphi \to \psi)$ oder $(\varphi \leftrightarrow \psi)$ enthält.

Weil $(\varphi \to \psi) \equiv (\neg\varphi \vee \psi)$ und $(\varphi \leftrightarrow \psi) \equiv (\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi)$, sind alle FO $[\sigma]$-Formeln äquivalent zu implikationsfreien FO $[\sigma]$-Formeln. Hierbei entsteht ein fester Zuwachs in der Länge der Formel $\|\varphi\|$, der die Datenkomplexität unberührt lässt.

3.3 Logiken mit Fixpunkt-Erweiterung

Wir führen eine Erweiterung ein, die es erlaubt, den iterativen Fixpunkt einer selbstreferenziellen logischen Formel zu definieren.

Definition 3.9. Eine Logik $\mathcal{L}$ erweitert die Logik $\mathcal{L}'$, wenn sie die Syntax und Semantik von $\mathcal{L}'$ übernimmt, und zusätzliche Produktionen einführt.

Als erstes definieren wir einen neuen Typ von Variablen.

Definition 3.10. Sei $\mathbf{var}_2$ die Menge aller Relationsvariablen. Jede solche Variable $X \in \mathbf{var}_2$ besitzt eine Stelligkeit $\operatorname{ar}(X) = k \in \mathbb{N}_{\geqslant 1}$; diese wird auch durch $X/k \in \mathbf{var}_2$ notiert.

Die Funktionen frei und var, so wie die Belegungen β, werden auf $\mathbf{var} \uplus \mathbf{var}_2$ erweitert.

$$\begin{aligned} \text{frei}(\varphi), \text{var}(\varphi) &\subseteq \mathbf{var} \uplus \mathbf{var}_2 \\ \beta : \text{frei}(\varphi) &\to A \cup \bigcup_{k \in \mathbb{N}} A^k \\ \beta X &\subseteq A^{\text{ar}(X)} \text{ für } X \in \mathbf{var}_2 \end{aligned}$$

Wir möchten syntaktisch garantieren, dass die Iteration der Formel eine monoton wachsende Relation berechnet. Dafür wird verlangt, dass die selbstreferenzielle Relationsvariable nicht negiert vorkommt.

Definition 3.11. Positivität

Wir definieren die (nicht disjunkten) Mengen der X-positiven und X-negativen $\mathcal{L}[\sigma]$-Formeln für $X \in \mathbf{var}_2$ wie folgt:

- Jeder $\mathcal{L}[\sigma]$-Ausdruck ω mit $X \notin \text{frei}(\omega)$ ist sowohl X-positiv als auch X-negativ.
- Für jede X-positive Formel φ ist $\neg\varphi$ X-negativ, und umgekehrt.
- Für einen Junktor $\gamma \in \{\wedge, \vee\}$ und $k \geqslant 2$ X-positive (beziehungsweise X-negative) Formeln $\varphi_1, \cdots, \varphi_k$ ist $(\varphi_1 \gamma \cdots \gamma \varphi_k)$ ebenfalls X-positiv (beziehungsweise X-negativ).
- Für einen Quantor $Q \in \{\exists, \forall\}$, eine Variable $x \in \mathbf{var}$ und eine X-positive (beziehungsweise X-negative) Formel φ ist $Qx\varphi$ ebenfalls X-positiv (beziehungsweise X-negativ).

Nun definieren wir die Fixpunkt-Erweiterung.

Definition 3.12. Für eine Logik $\mathcal{L}$ und eine relationale Signatur σ erweitert $\text{LFP}(\mathcal{L})[\sigma]$ die Logik $\mathcal{L}[\sigma]$ wie folgt:

(AV) Für eine Relationsvariable $X/k \in \mathbf{var}_2$ und ein k-Tupel $\bar{x}$ von X-positiven $\text{LFP}(\mathcal{L})[\sigma]$-Termen ist $X\bar{x}$ eine X-positive $\text{LFP}(\mathcal{L})[\sigma]$-Formel.

$$\begin{aligned} \text{frei}(X\bar{x}) &:= \{X\} \cup \bigcup_{i=1}^{k} \text{frei}(x_i) \\ \text{var}(X\bar{x}) &:= \{X\} \cup \bigcup_{i=1}^{k} \text{var}(x_i) \\ [\![X\bar{x}]\!](\mathfrak{A}, \beta) &:= [\beta X](\beta\bar{x}) \\ &\quad \text{mit } \beta X \subseteq A^k, \\ &\quad\quad \beta\bar{x} \in A^k \end{aligned}$$

(LFP) Für eine Relationsvariable $X/k \in \mathbf{var}_2$, eine X-positive LFP $(\mathcal{L})\,[\sigma]$-Formel ψ, ein Tupel $\bar{x} \in \mathbf{var}^k$ und ein k-Tupel $\bar{y}$ von X-positiven LFP $(\mathcal{L})\,[\sigma]$-Termen ist $\varphi = \left[\mathrm{lfp}_{X,\bar{x}}\psi\right](\bar{y})$ eine X-positive LFP $(\mathcal{L})\,[\sigma]$-Formel.

$$\begin{aligned}\mathrm{frei}(\varphi) &= \mathrm{frei}(\psi) \setminus \{X, x_1, \cdots, x_k\} \cup \bigcup_{i=1}^{k} \mathrm{frei}(y_i)\\ \mathrm{var}(\varphi) &= \mathrm{var}(\psi) \cup \{X, x_1, \cdots, x_k\} \cup \bigcup_{i=1}^{k} \mathrm{var}(y_i)\end{aligned}$$

Für eine Belegung $\beta : \mathrm{frei}(\varphi) \to A$ prüft $\varphi = \left[\mathrm{lfp}_{X,\bar{x}}\psi\right](\bar{y})$, ob die Belegung des Tupels $\bar{y}$ im kleinsten Fixpunkt des Relationssymbols X liegt.

$$\begin{aligned}\beta' &:= \beta_{|\mathrm{frei}(\psi)\setminus\{X,x_1,\cdots,x_k\}}\\ [\![\left[\mathrm{lfp}_{X,\bar{x}}\psi\right](\bar{y})]\!](\mathfrak{A},\beta) &:= [\![X\bar{y}]\!]\left(\mathfrak{A}, \beta \cup \left(X \mapsto \mathrm{lfp}_{X,\bar{x}}(\psi)\right)\right)\end{aligned}$$

Im folgenden wird eine Berechnung definiert, die den kleinsten Fixpunkt $\mathrm{lfp}_{X,\bar{x}}(\psi)$ iterativ bestimmt.

Ohne Beschränkung der Allgemeinheit sei $\{x_1, \cdots, x_k\} \subseteq \mathrm{frei}(\psi)$, denn analog zu Definition 3.7 ist $\psi \equiv (\bar{x} = \bar{x} \wedge \psi)$. Die nicht durch den Operator gebundenen Variablen $P \coloneqq \mathrm{frei}(\psi) \setminus \{x_1, \cdots, x_k\} \subseteq \mathrm{frei}(\varphi)$ heißen **Parameter** der Fixpunkt-Operation.

Für eine Parameter-Belegung $\beta : P \to A$ sei F_β die folgende Abbildung:

$$\begin{aligned}F_\beta &: 2^{A^k} \to 2^{A^k}\\ F_\beta(Y) &:= \left\{\bar{a} \in A^k \mid \mathfrak{A} \models \psi^{\beta \cup (X \mapsto Y)}[\bar{a}]\right\}\end{aligned}$$

Das heißt: $F_\beta(Y)$ ist das Anfrageergebnis von φ auf $\mathfrak{A}$ unter der Belegung der Parameter mit β und der Variable X mit der Relation Y.

Aus der X-Positivität folgt nach [13, 22] die Monotonie von F_β

$$A \subseteq B \Rightarrow F_\beta(A) \subseteq F_\beta(B)$$

und daher induktiv die Existenz eines Fixpunkts $F^\infty(\emptyset)$, der nach höchstens $\left|A^k\right|$ Schritten erreicht wird:

$$\emptyset \subseteq F_\beta(\emptyset) \subseteq \cdots \subseteq F_\beta^\infty(\emptyset) \subseteq A^k$$

Für jeden anderen Fixpunkt Y' gilt $\emptyset \subseteq Y'$, und per Induktion auch $F^n(\emptyset) \subseteq F^n(Y') = Y'$. Daher ist $F^\infty(\emptyset) = \mathrm{lfp}_{X,\bar{x}}(\psi)$ der kleinste Fixpunkt.

Im folgenden wird die Logik LFP (FO) durch LFP abgekürzt. Ferner werden wir uns auf das *parameterfreie* Fragment der Logik beschränken, was (bis auf einen Zuwachs in der Anzahl der Variablen und Länge der Formel) die Allgemeinheit nicht einschränkt.

Definition 3.13. Eine LFP $[\sigma]$-Formel φ ist **parameterfrei**, falls der Fixpunktoperator stets alle Variablen bindet - das heißt, für jede Teilformel der Form $\left[\mathrm{lfp}_{X,\bar{x}}\psi\right](\bar{y})$ gilt:

$$\mathrm{frei}(\psi) \subseteq \left\{X, x_1, \cdots, x_{\mathrm{ar}(X)}\right\}$$

Satz 3.14. *Jede* LFP $[\sigma]$*-Formel* φ *kann (unter Zuwachs der Länge* $\|\varphi\|$ *und Größe* $|\mathrm{var}(\varphi)|$*) in eine parameterfreie* LFP $[\sigma]$*-Formel* φ' *übersetzt werden.[31, 12, 9]*

Beispiel 3.15. Die folgende LFP $[\{E\}]$-Formel $\varphi(u,v)$ ist erfüllt, wenn u und v durch einen Weg beliebiger Länge verbunden sind:

$$\varphi(u,v) \coloneqq \left[\mathrm{lfp}_{T,(x,y)}\ (\exists z\ (E(x,z) \wedge T(z,y)) \vee x \doteq y)\right](u,v)$$

Definition 3.16. Eine etwas robustere, aber äquivalente, Definition der Fixpunktlogik verwendet den inflationären Fixpunktoperator. Anstelle der Positivität einer Formel in einer Relationsvariable betrachten wir mit $\left[\mathrm{ifp}_{X,\bar{x}}\psi\right](\bar{y})$ implizit die Formel $\left[\mathrm{lfp}_{X,\bar{x}}(X\bar{x} \vee \psi)\right](\bar{y})$, die uns eine inflationäre Iteration garantiert:

$$F_\beta(Y) = Y \cup q_{\psi(\bar{x})}^{\beta \cup (X \to Y)}(\mathfrak{A}) \supseteq Y$$

In diesem Fall muss ψ nicht mehr X-positiv sein.

3.4 Logiken mit numerischen Erweiterungen

3.4.1 Disjunkte Orakel

Eine Erweiterung um ein numerisches Orakel fügt einer Logik eine Anzahl von Relationssymbolen hinzu, die für $\mathfrak{A} \in \mathbf{FIN}(\sigma)$ eine feste Interpretation über einem von A disjunkten numerischen Universum $[0, |A|]$ erhalten.

Definition 3.17. **η-Orakel, $\mathcal{L} + \Upsilon$-Logik**

Sei η eine relationale Signatur. Ein η-Orakel $\Upsilon : \mathbb{N} \to \mathbf{FIN}^0_{\leqslant}(\eta)$ ist eine Funktion, die jeder natürlichen Zahl n eine geordnete $(\eta \uplus \{\leqslant\})$-Struktur $\Upsilon(n)$ über $[0,n]$ zuweist.

Sei σ eine von $\eta \uplus \{\leqslant\}$ disjunkte relationale Signatur und $\mathcal{L}$ eine Logik (zum Beispiel FO oder LFP). Für ein η-Orakel Υ ist die Syntax der $(\mathcal{L} + \Upsilon)[\sigma]$-Logik die der Logik $\mathcal{L}[\sigma \uplus \eta \uplus \{\leqslant\}]$.

Für eine endliche σ-Struktur $\mathfrak{A}$ mit $A \cap [0, |A|] = \emptyset$ und eine Belegung $\beta : \mathbf{var} \to A \uplus [0, |A|]$ werden $(\mathcal{L} + \Upsilon)$-Ausdrücke auf der disjunkten Vereinigung von $\mathfrak{A}$ mit der entsprechenden Orakelstruktur $\Upsilon(|A|)$ ausgewertet:

$$[\![\varphi]\!](\mathfrak{A}, \beta) \coloneqq [\![\varphi]\!](\mathfrak{A} \uplus \Upsilon(|A|), \beta)$$

Notation 3.18. Nach unserem Begriff der logischen Erweiterung ist die Bezeichnung $\mathrm{LFP}(\mathcal{L} + \Upsilon)$ gleichbedeutend mit $\mathrm{LFP}(\mathcal{L}) + \Upsilon$. Im folgenden werden wir allgemein die erste Bezeichnung verwenden, aber weiterhin $\mathrm{LFP}(\mathrm{FO}) + \Upsilon$ durch $\mathrm{LFP} + \Upsilon$ abkürzen.

Definition 3.19. Uniformität

Wir nennen ein η-Orakel $\mathcal{K}$**-uniform** (für eine Komplexitätsklasse $\mathcal{K}$) wenn die Berechnung der Repräsentation von $\Upsilon(n)$ bei Eingabe von $\overbrace{1 \cdots 1}^{n}$ in $\mathcal{K}$ ist.

Insbesondere sei P die Klasse der $\mathrm{poly}(n)$-zeitbeschränkten, und LOGSPACE die Klasse der $\mathcal{O}(\log n)$-platzbeschränkten Turingmaschinen. P/poly sei die Klasse der $\mathrm{poly}(n)$-zeitbeschränkten Turingmaschinen, die eine $\mathrm{poly}(n)$-beschränkte Orakel-Eingabe erhalten.

Wir definieren die folgenden drei numerischen Orakel für die reine Ordnung, für Arithmetik, und für nicht berechenbare Prädikate.

Definition 3.20. Sei $\mathbf{ORD} : \mathbb{N} \to \mathbf{FIN}^0_<(\emptyset)$ ein $\emptyset$-Orakel, so dass das für $n \in \mathbb{N}$ die geordnete $\emptyset$-Struktur gilt:

$$\mathbf{ORD}(n) \coloneqq \left([0, n], \leqslant_{|[0,n]}\right) \in \mathbf{FIN}^{[0,n]}_<(\emptyset)$$

Definition 3.21. Sei $\mathbf{BIT} : \mathbb{N} \to \mathbf{FIN}^0_<(\{\mathtt{BIT}\})$ ein $\{\mathtt{BIT}\}$-Orakel, wobei das Prädikat $\mathtt{BIT}(a, b)$ ausdrückt, dass das $b$te Bit der Binärdarstellung von a den Wert 1 hat.

$$\begin{aligned}
\mathcal{N}_{\mathrm{bit}} &\coloneqq \left(\mathbb{N}, \leqslant, \mathtt{BIT}^{\mathcal{N}}\right) \\
\mathtt{BIT}^{\mathcal{N}} &\coloneqq \left\{(a, b) \in \mathbb{N}^2 \mid a = \Sigma_{i=0}^{\lceil \log a \rceil} x_i 2^i,\ \bar{x} \in \{0,1\}^{\lceil \log a \rceil},\ x_b = 1\right\} \\
\mathbf{BIT}(n) &\coloneqq (\mathcal{N}_{\mathrm{bit}})_{|[0,n]} \in \mathbf{FIN}^{[0,n]}_<(\{\mathtt{BIT}\})
\end{aligned}$$

Definition 3.22. Sei $\eta_{\mathrm{arb}} = \left\{R_X \mid X \in \bigcup_{k \in \mathbb{N}} 2^{\mathbb{N}^k}\right\}$ eine unendliche Signatur, die für jede beliebige Relation $X \subseteq \mathbb{N}^k$ mit $k \in \mathbb{N}$ auf den natürlichen Zahlen ein Symbol R_X/k enthält, und sei $\mathcal{N}_{\mathrm{arb}}$ die η_{arb}-Struktur über $\mathbb{N}$, die diese Symbole interpretiert. Dann sei $\mathbf{ARB} : \mathbb{N} \to \mathbf{FIN}^0_<(\eta_{\mathrm{arb}})$ ein η_{arb}-Orakel, das die endlichen Anfangsstücke dieser

Relationen ausgibt:

$$\begin{aligned} \mathcal{N}_{\text{arb}} &:= \left(\mathbb{N}, \leqslant, (R_X \mapsto X)_{R_X \in \eta_{\text{arb}}}\right) \\ \mathbf{ARB}\,(n) &:= (\mathcal{N}_{\text{arb}})_{|[0,n]} \in \mathbf{FIN}_{<}^{[0,n]}\,(\eta_{\text{arb}}) \end{aligned}$$

Hierbei ist leicht nachweisbar: **ORD** und **BIT** sind LOGSPACE-uniform, und **ARB** ist P/poly-uniform.

3.4.2 Zähl-Erweiterungen

Wir führen mehrere syntaktische Erweiterungen der Logik $\mathrm{FO} + \Upsilon$ ein, die es erlauben, erfüllende Belegungen einer Variable zu zählen: Den Zählterm $\#$, den Zählquantor $\exists^{=}$, und den Majority-Quantor $\exists^{\geqslant}$. Es wird nachgewiesen, dass alle drei Erweiterungen die gleiche Ausdrucksstärke modulo einem festen Zuwachs der Formellänge haben.

Definition 3.23. Zählterm $\#$ (wie in [1], und Abschnitt 8.4.2 von [10] für Fixpunktlogik)

Der Zählterm ist eine zusätzliche Termproduktion, die die erfüllenden Belegungen einer Formel zählt.

Sei $\mathcal{L}$ eine beliebige Logik, η eine relationale Signatur, und $\Upsilon : \mathbb{N} \to \mathbf{FIN}_{<}\,(\eta)$ ein η-Orakel.

Die $(\mathcal{L} + \Upsilon + \#)$-Logik erweitert die $(\mathcal{L} + \Upsilon)$-Logik um die folgende Regel:

(TC) Für eine $(\mathcal{L} + \Upsilon + \#)\,[\sigma]$-Formel φ und eine Variable $x \in \mathbf{var}$ ist $\#x\varphi$ ein $(\mathcal{L} + \Upsilon + \#)\,[\sigma]$-Term.

$$\begin{aligned} \operatorname{frei}(\#x\varphi) &:= \operatorname{frei}(\varphi) \setminus \{x\} \\ \operatorname{var}(\#x\varphi) &:= \operatorname{var}(\varphi) \cup \{x\} \end{aligned}$$

Auf einer endlichen Struktur $\mathfrak{A} \in \mathbf{FIN}^{(n)}\,(\sigma)$ mit $n \in \mathbb{N}$ und einer Belegung

$$\beta : \operatorname{frei}(\varphi) \setminus \{x\} \to A \uplus [0, n]$$

sei

$$[\![\#x\varphi]\!]\,(\mathfrak{A}, \beta) := \left|\left\{a \in A \mid \mathfrak{A} \models \varphi^{\beta \cup \binom{x}{a}}\right\}\right|$$

die Anzahl der unterschiedlichen Werte $a \in A$, für die $\mathfrak{A} \models \varphi^{\beta \cup \binom{x}{a}}$ gilt.

Beispiel. Diese Erweiterung erlaubt die Definition vieler arithmetischer Operatoren durch Terme, wie zum Beispiel die positive Differenz:

$$\begin{aligned} t_{\text{DIFF}}(x,y) &:= \#_z(\neg z \leqslant x \wedge z \leqslant y) \\ [\![t_{\text{DIFF}}]\!](\mathfrak{A},(a,b)) &= \max(b-a,0) \end{aligned}$$

Definition 3.24. Zählquantor $\exists^{=}$ (wie in [27], hier aber mit einem disjunkten numerischen Universum)

Der Zählquantor ist eine zusätzlicher Quantor, der die Zahl der erfüllenden Belegungen einer Formel mit einer Variable vergleicht.

Sei $\mathcal{L}$ eine beliebige Logik, η eine relationale Signatur, und $\Upsilon : \mathbb{N} \to \mathbf{FIN}_{<}^{[0,n]}(\eta)$ ein η-Orakel.

Die $\mathcal{L} + \Upsilon + \exists^{=}$-Logik erweitert die $\mathcal{L} + \Upsilon$-Logik um die folgende Regel:

(QC) Für eine $(\mathcal{L} + \Upsilon + \exists^{=})[\sigma]$-Formel φ und zwei Variablen $x, y \in \mathbf{var}$ ist $\exists^{=y} x\varphi$ eine $(\mathcal{L} + \Upsilon + \exists^{=})[\sigma]$-Formel.

$$\begin{aligned} \text{frei}(\exists^{=y} x\varphi) &:= \{y\} \cup (\text{frei}(\varphi) \setminus \{x\}) \\ \text{var}(\exists^{=y} x\varphi) &:= \text{var}(\varphi) \cup \{x, y\} \end{aligned}$$

Auf einer endlichen Struktur $\mathfrak{A} \in \mathbf{FIN}^{(n)}(\sigma)$ mit einer Belegung

$$\beta : (\text{frei}(\varphi) \setminus \{x\}) \cup \{y\} \to A \cup [0,n]$$

gelte:

$$[\![\exists^{=y} x\varphi]\!](\mathfrak{A},\beta) := \begin{cases} 1 & \text{falls } \beta y = \left\{ a \in A \mid \mathfrak{A} \models \varphi^{\beta \setminus \{x\} \cup \binom{x}{a}} \right\} \\ 0 & \text{sonst} \end{cases}$$

Definition 3.25. Majority-Quantor $\exists^{\geqslant}$ (wie in [10] Abschnitt 3.4, hier aber mit $\exists^{\geqslant x}$ für $x \in \mathbf{var}$ anstelle von unendlich vielen Quantoren $\left(\exists^{\geqslant n}\right)_{n \in \mathbb{N}}$)

Der Majority-Quantor funktioniert wie der Zählquantor und prüft, ob die Zahl der erfüllenden Belegungen mindestens den Wert einer Variable erreicht.

Sei $\mathcal{L}$ eine beliebige Logik, η eine relationale Signatur, und $\Upsilon : \mathbb{N} \to \mathbf{FIN}_{<}^{[0,n]}(\eta)$ ein η-Orakel.

Die $\mathcal{L} + \Upsilon + \exists^{\geqslant}$-Logik erweitert die $\mathcal{L} + \Upsilon$-Logik um die folgende Regel:

(QM) Für eine $\left(\mathcal{L} + \Upsilon + \exists^{\geqslant}\right)[\sigma]$-Formel φ und zwei Variablen $x, y \in \mathbf{var}$ ist $\exists^{\geqslant y} x\varphi$ eine $\left(\mathcal{L} + \Upsilon + \exists^{\geqslant}\right)[\sigma]$-Formel.

$$\operatorname{frei}\left(\exists^{\geqslant y} x\varphi\right) = \{y\} \cup (\operatorname{frei}(\varphi) \setminus \{x\}) \qquad \operatorname{var}\left(\exists^{\geqslant y} x\varphi\right) = \operatorname{var}(\varphi) \cup \{x, y\}$$

Auf einer endlichen Struktur $\mathfrak{A} \in \mathbf{FIN}^{(n)}(\sigma)$ mit einer Belegung

$$\beta : (\operatorname{frei}(\varphi) \setminus \{x\}) \cup \{y\} \to A \cup [0, n]$$

gilt:

$$\left[\!\left[\exists^{\geqslant y} x\varphi\right]\!\right](\mathfrak{A}, \beta) := \begin{cases} 1 & \text{falls } \beta y \in [0, n],\ \beta y \leqslant \left\{a \in A \mid \mathfrak{A} \models \varphi^{\beta_{\setminus\{x\}} \cup \binom{x}{a}}\right\} \\ 0 & \text{sonst} \end{cases}$$

Satz 3.26. *Die Logiken $\mathcal{L} + \Upsilon + \#$ und $\mathcal{L} + \Upsilon + \exists^{=}$ und $\mathcal{L} + \Upsilon + \exists^{\geqslant}$ sind äquivalent, modulo eines festen Zuwachses in $\|\varphi\|$ und $|\operatorname{var}(\varphi)|$.*

Beweis. Jede $(\mathcal{L} + \Upsilon + \#)[\sigma]$-Formel φ ist äquivalent zu einer $(\mathcal{L} + \Upsilon + \exists^{=})[\sigma]$-Formel φ'. Dazu ersetzen wir jede „pseudo-atomare“ Teilformel, die einen Zählterm enthält, wie folgt:

Fall 1. Falls $\varphi = y \doteq \#x\psi$ oder $\varphi = \#x\psi \doteq y$ für $x, y \in \mathbf{var}$, so sei $\varphi' := \exists^{=y} x\psi'$.

Fall 2. Falls $\varphi = \#x_1\psi_1 \doteq \#x_2\psi_2$ für $x_1, x_2 \in \mathbf{var}$, so sei $y \in \mathbf{var} \setminus (\operatorname{frei}(\psi_1) \cup \operatorname{frei}(\psi_2))$ eine neue Variable, und

$$\varphi' := \exists y \left(\exists^{=y} x_1\psi_1' \wedge \exists^{=y} x_2\psi_2'\right)$$

Fall 3. Falls $\varphi = R\bar{x}$ für $R/k \in \sigma \cup \eta \cup \{\leqslant\}$ und ein k-Tupel von $(\mathcal{L} + \Upsilon + \#)[\sigma]$-Termen $\bar{x}$, so sei $\bar{y} \in \left(\mathbf{var} \setminus \bigcup_{i=1}^{k} \operatorname{frei}(x_i)\right)^k$ ein Tupel von neuen Variablen, und:

$$\begin{aligned} \chi_i &:= \begin{cases} \exists^{=y_i} z_i\psi_i' & \text{falls } x_i = \#z_i\psi_i \\ y_i = x_i & \text{sonst} \end{cases} \\ \varphi' &:= \exists\bar{y}\left(R\bar{y} \wedge \bigwedge_{i=1}^{k} \chi_i\right) \end{aligned}$$

Jede $(\mathcal{L} + \Upsilon + \exists^{=})[\sigma]$-Formel φ ist äquivalent zu einer $\left(\mathcal{L} + \Upsilon + \exists^{\geqslant}\right)[\sigma]$-Formel φ':

Fall 1. Falls $\varphi = \exists^{=y} x\psi$, so sei ψ' eine zu ψ äquivalente $\left(\mathcal{L} + \Upsilon + \exists^{\geqslant}\right)[\sigma]$-Formel,

$z \in \mathbf{var} \backslash \mathrm{frei}(\psi)$ eine neue Variable, und:

$$\varphi' \coloneqq \forall z \left(\exists^{\geqslant z} x \psi' \leftrightarrow (z \leqslant y) \right)$$

Die Formel $\exists^{=y} x\psi$ ist mit $\beta(y) \in [0, n]$ erfüllt, genau dann wenn gilt: Die Formel $\exists^{\geqslant z} x\psi$ ist für alle $\beta(z) \in [0, n]$ erfüllt, genau dann wenn $\beta(z) \leqslant \beta(y)$.

Schließlich ist jede $\left(\mathcal{L} + \Upsilon + \exists^{\geqslant}\right)[\sigma]$-Formel φ äquivalent zu einer $(\mathcal{L} + \Upsilon + \#)[\sigma]$-Formel φ':

Fall 1. Falls $\varphi = \exists^{\geqslant y} x\psi$, so sei ψ' eine $\left(\mathcal{L} + \Upsilon + \exists^{\geqslant}\right)[\sigma]$-Formel mit $\psi \equiv \psi'$, und:

$$\varphi' \coloneqq y \leqslant \# x \psi$$

□

Notation 3.27. Im folgenden wird mit $\mathcal{L} + \Upsilon + C$ stets eine dieser äquivalenten Zähl-Logiken bezeichnet. Die Logik $\mathcal{L} + \mathbf{ORD} + C$ bezeichnen wir kurz als $\mathcal{L} + C$.

Beispiel 3.28. Die Logik FO + C kann ausdrücken, dass die σ-Struktur eine gerade Größe hat. Bekanntlich ist diese σ-Eigenschaft weder durch FO auf geordneten, noch LFP auf ungeordneten Strukturen definierbar[10, 22]:

$$\varphi_{\mathrm{EVEN}} \coloneqq \exists y \left(y = \#_z \left(\neg z \leqslant y \wedge z \leqslant \#_z \, z = z \right) \right)$$

3.4.3 Nicht-disjunkte Orakel

Eine alternative Erweiterung definiert über einer Struktur $\mathfrak{A}$ eine beliebige Bijektion $\pi : [1, n] \rightleftarrows A$ und interpretiert dann die numerischen Prädikate $R/k \in \eta$ über dem Universum der Struktur selbst. Diese Erweiterung bezeichnen wir (in Anlehnung an die disjunkte Erweiterung $\mathcal{L} + \Upsilon$) mit $\mathcal{L} \oplus \Upsilon$.

Definition 3.29. $\mathcal{L} \oplus \Upsilon$**-Logik**

Für eine relationale Signatur η, ein η-Orakel $\Upsilon : \mathbb{N} \to \mathbf{FIN}^1_<(\eta)$, eine von η disjunkte relationale Signatur σ und eine Logik $\mathcal{L}[\sigma]$ sei die Syntax von $\mathcal{L} \oplus \Upsilon[\sigma]$ gleich der Syntax von $\mathcal{L}[\sigma \uplus \eta \uplus \{\leqslant\}]$.

Für $\mathfrak{A} \in \mathbf{FIN}(\sigma)$ mit $n = |A|$ sei $\pi : [1, n] \rightleftarrows A$ eine beliebige Bijektion. Sei $\mathfrak{A}_\pi \in \mathbf{FIN}(\sigma \uplus \eta)$ definiert durch:

$$\begin{aligned} \mathfrak{A}_\pi &\coloneqq \mathfrak{A} \cup \pi\Upsilon(n) \\ &= \left(A, \left(R^{\mathfrak{A}} \right)_{R \in \sigma}, \left(\pi R^{\Upsilon(n)} \right) \right) \end{aligned}$$

Eine k-stellige $\mathcal{L} \oplus \Upsilon\,[\sigma]$-Formel φ heiße **invariant**, wenn für jede Struktur $\mathfrak{A} \in \mathbf{FIN}\,(\sigma)$, jedes Paar von Bijektionen $\pi, \pi' \in \mathrm{Bij}\,([1, |A|], A)$ und jedes Tupel $\bar{a} \in A^k$ gilt:

$$\mathfrak{A}_\pi \models \varphi\,[\bar{a}] \iff \mathfrak{A}_{\pi'} \models \varphi\,[\bar{a}]$$

Wir bezeichnen mit $\mathrm{inv}\,(\mathcal{L} \oplus \Upsilon)\,[\sigma]$ die Sprache der invarianten Formeln der $(\mathcal{L} \oplus \Upsilon)\,[\sigma]$-Logik.

Notation 3.30. Die Logik $\mathrm{inv}\,(\mathrm{FO} \oplus \mathbf{ARB})$ mit dem Orakel $\mathbf{ARB}\,(n) := (\mathcal{N}_{\mathrm{arb}})_{[1,n]}$ (mit $\mathcal{N}_{\mathrm{arb}}$ und η_{arb} wie in Definition 3.22) bezeichnen wir auch als die „arb-invariante $\mathrm{FO}\,(\mathbf{ARB})$-Logik“ in Anlehnung an [28, 2].

Es ist zu beachten, dass die hier betrachteten Orakel-Strukturen das Universum $[1, n]$ haben, und nicht $[0, n]$. Dies schließt unter anderem die Zählterm-Erweiterung $\mathcal{L} \oplus \Upsilon + \#$ aus, weil ein Zählterm nicht den Wert 0 erhalten kann und seine Auswertung nicht vollständig definiert ist. Die Zählquantor-Erweiterungen $\mathcal{L} \oplus \Upsilon + \exists^{=}$ und $\mathcal{L} \oplus \Upsilon + \exists^{\geqslant}$ haben dieses Problem nicht.

Nach dem Satz von Trakhtenbrot ist die endlichen Erfüllbarkeit von $\mathrm{FO}\,[\{\leqslant\}]$ unentscheidbar, und daher auch die Invarianz und die Sprache $\mathrm{inv}\,(\mathrm{FO} \oplus \mathbf{ARB})\,[\sigma]$ in $\mathrm{FO} \oplus \mathbf{ARB}\,[\sigma]$.[11, 22, 28]

4 Schaltkreise

4.1 Grundlagen der Schaltkreise

Definition 4.1. Boolesche Basis:

Eine boolesche Basis $\mathbb{B}$ besteht aus beliebigen über Permutation der Eingabe abgeschlossenen Relationen $\phi' \subseteq \{0,1\}^*$. Wir definieren dafür der Einfachheit halber die Relation $\phi \subseteq \mathbb{N}^2$ mit $\phi \coloneqq \left\{(i,j) \in \mathbb{N}^2 \mid 0^i 1^j \in \phi'\right\}$. Als Beispiel seien die folgenden booleschen Junktoren gegeben:

$$\begin{aligned} \texttt{AND} &\coloneqq \{0\} \times \mathbb{N} \\ \texttt{OR} &\coloneqq \mathbb{N} \times (\mathbb{N} \setminus \{0\}) \\ \texttt{MAJ} &\coloneqq \{(m,n) \in \mathbb{N} \times \mathbb{N} \mid m \leqslant n\} \\ \texttt{XOR} &\coloneqq \mathbb{N} \times (\mathbb{N} \setminus 2\mathbb{N}) \end{aligned}$$

Im folgenden stehe $\mathbb{B}_{\text{std}} \coloneqq \{\texttt{AND}, \texttt{OR}\}$ für die Basis mit boolescher Konjunktion und Disjunktion, und $\mathbb{B}_{\text{maj}} \coloneqq \mathbb{B}_{\text{std}} \cup \{\texttt{MAJ}\}$ für die Basis mit Konjunktion, Disjunktion und Majority.

Definition 4.2. Schaltkreis

Sei $\mathbb{B}$ eine boolesche Basis und σ eine relationale Signatur. Ein $(\sigma, \mathbb{B})$-Schaltkreis $\mathcal{C} \coloneqq (G, W, \Sigma, \Omega, U)$ mit der Stelligkeit $k \coloneqq \operatorname{ar}(C)$ besteht aus den folgenden Komponenten:

1. Ein azyklischer Graph mit den Knoten G („Gates“) und den Kanten $W \subseteq G \times G$.
2. eine Gate-Markierung Σ

$$\begin{aligned} \Sigma : G &\to \mathbb{B} \\ &\cup \{\mathbf{0}, \mathbf{1}, \texttt{NOT}\} \\ &\cup \left\{R\bar{t} \mid R \in \sigma, \bar{t} \in U^{\operatorname{ar}(R)}\right\} \end{aligned}$$

3. eine Ausgabefunktion[1] $\Omega : U^k \to G$ (bei $k = 0$ ist $\Omega(\langle\rangle) \in G$ ein einziges Output-Gate, und wird mit $\Omega = \Omega(\langle\rangle)$ abgekürzt) und
4. ein Universum U (üblicherweise $U = [1, n]$).

Hierbei haben alle mit $\phi \in \mathbb{B}$ markierten Gates mindestens einen[2] Vorgänger, alle mit $R\bar{x}$, $\mathbf{0}$ oder $\mathbf{1}$ markierten Gates keinen Vorgänger, und alle mit `NOT` markierten Gates genau einen Vorgänger.

Die mit $\mathbf{0}$ oder $\mathbf{1}$ markierten Gates heißen **Konstanten**, die mit $R\bar{x}$ markierten Gates heißen **Inputs**, und die Gates im Bild von Ω heißen **Outputs**.

Definition 4.3. Formal definieren wir den k-stelligen $(\sigma, \mathbb{B})$-Schaltkreis $\mathcal{C} = (G, W, \Sigma, \Omega, U)$ als eine relationale $\tau_{\sigma,\mathbb{B},k}$-Struktur über dem Universum $G \uplus U$, wobei gilt:

$$\begin{aligned}
\tau_{\sigma,\mathbb{B},k} &:= \left\{ W/2, (\Sigma_s/1)_{s \in \mathbb{B} \uplus \{\mathbf{0},\mathbf{1},\mathtt{NOT}\}}, (\Sigma_R/1+k)_{R/k \in \sigma}, \Omega/k+1 \right\} \\
W^{\mathcal{C}} &:= W \\
\Sigma_s^{\mathcal{C}} &:= \{g \in G \mid \Sigma(g) = s\} \text{ für } s \in \mathbb{B} \uplus \{\mathbf{0}, \mathbf{1}, \mathtt{NOT}\} \\
\Sigma_R^{\mathcal{C}} &:= \{g\bar{t} \mid \Sigma(g) = R\bar{t}\} \text{ für } R \in \sigma \\
\Omega^{\mathcal{C}} &:= \{\bar{t}g \mid \Omega(\bar{t}) = g\}
\end{aligned}$$

Definition 4.4. Auswertung von Schaltkreisen

Der $(\sigma, \mathbb{B})$-Schaltkreis $\mathcal{C} = (G, W, \Sigma, \Omega, U)$ wird auf einer σ-Struktur $\mathfrak{A} \in \mathbf{FIN}^U(\sigma)$ ausgewertet. Die Auswertung ist eine Abbildung $\mathcal{C}[\mathfrak{A}] : G \to \{0, 1\}$, die jedem Gate $g \in G$ den Wert 0 oder 1 zuweist, und ist rekursiv wie folgt definiert:

Fall 1. Für $\Sigma(g) = R\bar{t}$ gilt

$$\mathcal{C}[\mathfrak{A}](g) := \left[R^{\mathfrak{A}}\right]\bar{t}$$

Fall 2. Für $\Sigma(g) \in \{\mathbf{0}, \mathbf{1}\}$ gilt

$$\mathcal{C}[\mathfrak{A}](g) := \begin{cases} 1 & \text{falls } \Sigma(v) = \mathbf{1} \\ 0 & \text{sonst} \end{cases}$$

Fall 3. Für $\Sigma(g) = \mathtt{NOT}$ und $(h, g) \in W$ gilt

$$\mathcal{C}[\mathfrak{A}](g) := 1 - \mathcal{C}[\mathfrak{A}](h)$$

[1] In Anderson und Dawar 2014[1] wird zusätzlich die Injektivität von Ω verlangt; hier können aber mehrere Tupel dem gleichen Output-Gate zugeteilt werden.
[2] Alle hier betrachteten Schaltkreise haben einen unbeschränkten Fan-In.

Fall 4. Für $\Sigma(g) = \phi \in \mathbb{B}$ gilt:

$$\begin{aligned} j_1 &:= \sum_{(h,g)\in W} \mathcal{C}[\mathfrak{A}](h) \\ j_0 &:= |\{h \mid (h,g) \in W\}| - j_1 \end{aligned}$$

$$\mathcal{C}[\mathfrak{A}](g) := [\phi](j_0, j_1)$$

Für einen k-stelligen Schaltkreis $\mathcal{C}$ und ein Tupel $\bar{t} \in U^k$ sei die Ausgabe von $\mathcal{C}$ der Wert des Outputs $\Omega(\bar{t})$:

$$[\![\mathcal{C}]\!](\mathfrak{A}, \bar{t}) := \mathcal{C}[\mathfrak{A}](\Omega(\bar{t}))$$

Ferner sei $q_{\mathcal{C}} : \mathbf{FIN}^U(\sigma) \to U^k$ die Abbildung einer Struktur auf die Relation der Tupel, für die $\mathcal{C}$ den Wert 1 ausgibt.

$$q_{\mathcal{C}}(\mathfrak{A}) := \left\{\bar{t} \in U^k \mid [\![\mathcal{C}]\!](\mathfrak{A}, \bar{t}) = 1\right\}$$

Beispiel. Sei $\mathcal{C}_4 = (G, W, \Sigma, \Omega, [4])$ (siehe Abbildung 4.1) ein 1-stelliger $(\{E\}, \mathbb{B}_{\text{std}})$-Schaltkreis, der alle Knoten eines gerichteten Graphen findet, die Teil eines einfachen Kreises der Länge 2 sind.

$$\begin{aligned} G &:= \{g_{i,j} \mid i,j \in [4],\, i \neq j\} \\ &\cup \left\{g_{\{i,j\}} \mid \{i,j\} \subseteq [4],\, i \neq j\right\} \\ &\cup \{g_i \mid i \in [4]\} \end{aligned}$$

$$\begin{aligned} E &:= \left\{\left(g_{i,j}, g_{\{i,j\}}\right) \mid i,j \in [4],\, i \neq j\right\} \\ &\cup \left\{\left(g_{\{i,j\}}, g_i\right) \mid i,j \in [4],\, i \neq j\right\} \end{aligned}$$

$$\Sigma(g) = \begin{cases} E\,i\,j & \text{für } g = g_{i,j} \\ \texttt{AND} & \text{für } g = g_{\{i,j\}} \\ \texttt{OR} & \text{für } g = g_i \end{cases}$$

$$\Omega(i) := g_i$$

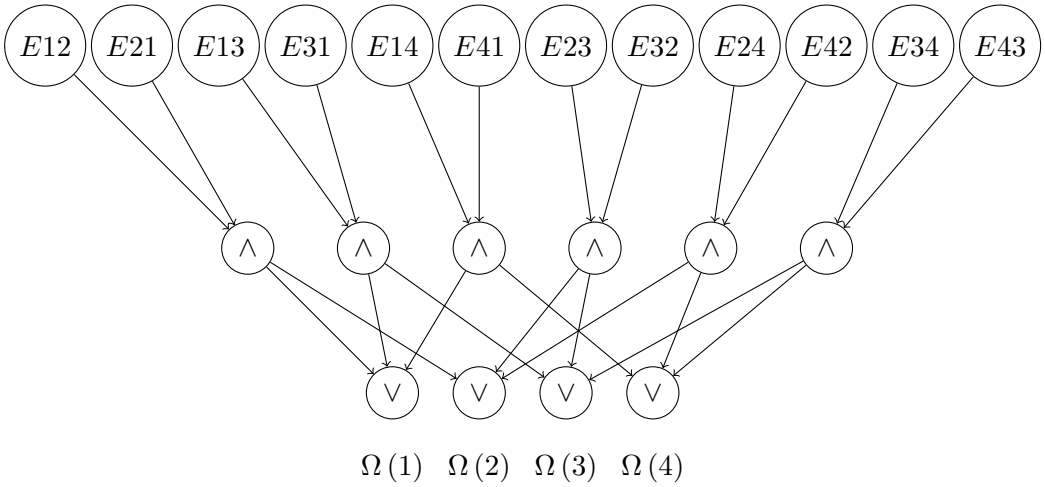

Abbildung 4.1: Schaltkreis $\mathcal{C}_4$

4.2 Eigenschaften von Schaltkreisen

Definition 4.5. Größe und Tiefe

Die Größe $|\mathcal{C}|$ eines Schaltkreises $\mathcal{C} = (G, W, \Sigma, \Omega, U)$ sei die Anzahl seiner Gates, $|G|$. Die Tiefe $T(\mathcal{C})$ sei die maximale Länge eines Wegs durch den Graphen (G, W).

Definition 4.6. Invarianz

Ein $(\sigma, \mathbb{B})$-Schaltkreis $\mathcal{C}$ mit dem Universum U heiße **invariant**, wenn für alle $\mathfrak{A} \in \mathbf{FIN}^U(\sigma)$, alle $\bar{t} \in U^{\mathrm{ar}(\mathcal{C})}$, und jede Permutation $\pi \in \mathrm{Sym}_U$ gilt:

$$[\![\mathcal{C}]\!](\pi\mathfrak{A}, \pi\bar{t}) = [\![\mathcal{C}]\!](\mathfrak{A}, \bar{t})$$

In diesem Fall definieren wir für jede Struktur $\mathfrak{A} \in \mathbf{FIN}^{(|U|)}(\sigma)$ und $\bar{a} \in A^{\mathrm{ar}(\mathcal{C})}$ die Auswertung von $\mathcal{C}$ implizit als die Auswertung auf $\pi\mathfrak{A} \in \mathbf{FIN}^U(\sigma)$ mit einer beliebigen Bijektion $\pi : A \rightleftarrows U$:

$$[\![\mathcal{C}]\!](\mathfrak{A}, \bar{a}) \coloneqq [\![\mathcal{C}]\!](\pi\mathfrak{A}, \pi\bar{a})$$

Definition 4.7. Symmetrie

Für einen Schaltkreis $\mathcal{C} = (G, W, \Sigma, \Omega, U)$, eine Permutation $\pi \in \mathrm{Sym}_U$ und einen Automorphismus $\rho \in \mathrm{Aut}_{\mathcal{C}}$ mit $\rho_{|U} = \pi$ nennen wir ρ von π **induziert**. (Nach den formalen Definitionen 4.3 und 2.12 ist $\rho \in \mathrm{Aut}_{\mathcal{C}} \subseteq \mathrm{Sym}_{G \uplus U}$ eine Permutation des Universums von $\mathcal{C}$.) Wir können aus der formalen Definition des Schaltkreises als $\tau_{\sigma,\mathbb{B},k}$-Struktur ableiten, dass ein von π induzierter Automorphismus ρ die folgenden Bedingungen erfüllt:

1. Die Kanten sind isomorph: $\rho W = W$.
2. Für alle Inputs g mit $\Sigma(g) = R\bar{x}$ gilt $\Sigma(\rho g) = R\bar{x'}$, mit $\bar{x'} = \pi\bar{x}$.
3. Für alle übrigen Gates gilt $\Sigma(\rho g) = \Sigma(g)$.
4. Für jedes Tupel $\bar{t} \in U^k$ gilt $\rho\Omega(\bar{x}) = \Omega(\pi\bar{t})$.

Ein Schaltkreis heiße **symmetrisch**, genau dann wenn jede Permutation des Universums $\pi \in \mathrm{Sym}_U$ einen Automorphismus $\hat{\pi} \in \mathrm{Aut}_{\mathcal{C}}$ des Schaltkreises induziert. (In Zukunft betrachten wir der Einfachheit halber nur den Teil $\hat{\pi}_{|G}$, der die Gates des Schaltkreises permutiert, da der Rest des Automorphismus $\hat{\pi} = \hat{\pi}_{|G} \uplus \pi$ lediglich die Permutation π ist.)

Satz 4.8. *Symmetrie ist eine hinreichende, aber nicht notwendige, Bedingung für die Invarianz eines Schaltkreises.*

Beweis. Sei $\mathcal{C}$ ein symmetrischer k-stelliger $(\sigma, \mathbb{B})$-Schaltkreis über U, und $\mathfrak{A} \in \mathbf{FIN}^U(\sigma)$. Sei $\pi \in \mathrm{Sym}_U$ eine beliebige Permutation, und sei $\bar{t} \in U^k$ ein beliebiges Tupel. Es ist zu zeigen, dass:

$$[\![\mathcal{C}]\!](\mathfrak{A}, \bar{t}) \quad = \quad [\![\mathcal{C}]\!](\pi\mathfrak{A}, \pi\bar{t})$$

Wegen der Symmetrie induziert π einen Automorphismus $\hat{\pi}$ auf $\mathcal{C}$:

$$\begin{aligned} \hat{\pi}(W) &= W \\ \Sigma(\hat{\pi}g) &= \begin{cases} R\pi\bar{x} & \text{für } \Sigma(g) = R\bar{x} \\ \Sigma(g) & \text{sonst} \end{cases} \\ \Omega(\pi\bar{x}) &= \hat{\pi}\Omega(\bar{x}) \text{ für alle } \bar{x} \in U^{\mathrm{ar}(\mathcal{C})} \end{aligned}$$

Per Induktion über die Tiefe[3] $T(g)$ des Gates g wird gezeigt:

$$\mathcal{C}[\mathfrak{A}](g) = \mathcal{C}[\pi\mathfrak{A}](\hat{\pi}g) \qquad \text{für alle } g \in G$$

Induktionsanfang $T(g) = 0$: Sei $g \in G$ ein Input mit $\Sigma(g) = R\bar{x}$. Per Definition von τ und $\hat{\tau}$ gilt:

$$\begin{aligned} \Sigma(\hat{\pi}g) &= R\pi\bar{x} \\ \pi\bar{x} \in \pi R^{\mathfrak{A}} &\iff \bar{x} \in \pi_2 R^{\mathfrak{A}} \end{aligned}$$

[3] Die Tiefe $T : G \to \mathbb{N}$ sei die maximale Länge eines Weges von einer Quelle zum Gate g.

Es folgt:

$$\begin{aligned} \mathcal{C}\left[\pi\mathfrak{A}\right]\left(\hat{\pi}g\right) &= \left[\pi R^{\mathfrak{A}}\right]\left(\pi\bar{x}\right) \\ &= \left[R^{\mathfrak{A}}\right]\left(\bar{x}\right) \\ &= \mathcal{C}\left[\mathfrak{A}\right]\left(g\right) \end{aligned}$$

(Falls $\Sigma\left(g\right) \in \{\mathbf{0}, \mathbf{1}\}$, folgt die Behauptung direkt aus $\Sigma\left(\hat{\pi}g\right) = \Sigma\left(g\right)$.)

Induktionsschritt $n \mapsto n+1$**:**

Annahme: Für alle Gates $g \in G$ mit Tiefe $T\left(g\right) \leqslant n$ gilt $\mathcal{C}\left[\pi\mathfrak{A}\right]\left(\hat{\pi}g\right) = \mathcal{C}\left[\mathfrak{A}\right]\left(g\right)$.

So gilt für jedes Gatter $g' \in G$ mit $T\left(g'\right) = n+1$:

1. Die Beschriftungen $\Sigma\left(\hat{\pi}g'\right) = \Sigma\left(g'\right) = \phi$ sind gleich.
2. $\mathcal{C}\left[\pi\mathfrak{A}\right]\left(\hat{\pi}g\right) = \mathcal{C}\left[\mathfrak{A}\right]\left(g\right)$ für alle $\left(g, g'\right) \in W$.

Es folgt $\mathcal{C}\left[\pi\mathfrak{A}\right]\left(\hat{\pi}g'\right) = \mathcal{C}\left[\mathfrak{A}\right]\left(g'\right)$.

Schließlich gilt für jedes Tupel $\bar{t} \in U^{\mathrm{ar}(\mathcal{C})}$:

$$\begin{aligned} \left[\!\left[\mathcal{C}\right]\!\right]\left(\pi\mathfrak{A}, \pi\bar{t}\right) &= \mathcal{C}\left[\pi\mathfrak{A}\right]\left(\Omega\left(\pi\bar{t}\right)\right) \\ &= \mathcal{C}\left[\pi\mathfrak{A}\right]\left(\hat{\pi}\Omega\left(\bar{t}\right)\right) \\ &= \mathcal{C}\left[\mathfrak{A}\right]\left(\Omega\left(\bar{t}\right)\right) = \left[\!\left[\mathcal{C}\right]\!\right]\left(\mathfrak{A}, \bar{t}\right) \end{aligned}$$

Damit ist der Schaltkreis invariant.

Um die Umkehrrichtung zu widerlegen, wird als Gegenbeispiel der folgende 0-stellige Schaltkreis $\mathcal{C}_2$ (siehe Abbildung 4.2) über $U = \{1, 2\}$ angeführt:

$$\begin{aligned} \mathcal{C} &\coloneqq \left(G, W, \Sigma, \Omega, U\right) \\ G &\coloneqq \left\{g_{i,j} \mid i, j \in U\right\} \cup \left\{g_\wedge, g'_\wedge\right\} \\ W &\coloneqq \left\{\left(g_{1,1}, g_\wedge\right), \left(g_{1,2}, g_\wedge\right), \left(g_{2,1}, g'_\wedge\right), \left(g_{2,2}, g'_\wedge\right), \left(g_\wedge, g'_\wedge\right)\right\} \\ \Sigma\left(g\right) &\coloneqq \texttt{AND} \\ \Omega &\coloneqq g'_\wedge \end{aligned}$$

□

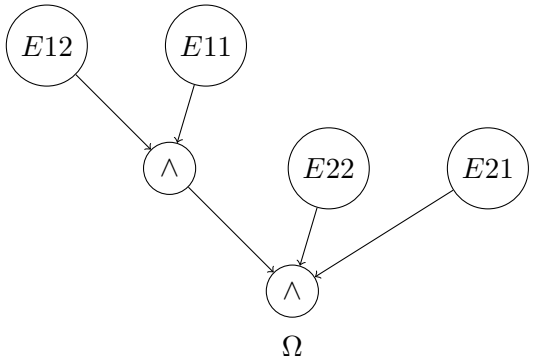

Abbildung 4.2: Schaltkreis $\mathcal{C}_2$

Der Schaltkreis ist invariant, und akzeptiert alle vollständigen K_2-Graphen. Er ist aber nicht symmetrisch: Die Permutation $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ induziert keinen Automorphismus.

Definition 4.9. Rigidität

Ein Schaltkreis $\mathcal{C} = (G, W, \Sigma, \Omega, U)$ sei rigide, wenn er keine redundanten Gates besitzt. Formal dürfen nicht $g, g' \in G$ existieren, so dass:

$$\begin{aligned} \Sigma(g) &= \Sigma(g') \\ \{u \in G \mid (u, g) \in W\} &= \{u \in G \mid (u, g') \in W\} \end{aligned}$$

Insbesondere heißt dies, das der Schaltkreis höchstens zwei Konstanten g_0, g_1 mit $\Sigma(g_0) = \mathbf{0}$ und $\Sigma(g_1) = \mathbf{1}$ enthält, und jede Input-Beschriftung $\Sigma(g) = R\bar{x}$ nur einmal vorkommt.

Die Rigidität ist hier analog zu der Arbeit von Anderson und Dawar[1] definiert, verlangt aber zusätzlich, dass zwei Gates nicht nur durch die (hier nicht injektive) Output-Markierung Ω unterschieden werden. Diese Einschränkung ist strenger, schränkt aber die Definition nicht bedeutend ein:

Für zwei Gates $g, g' \in G$ mit den gleichen Vorgängern, der gleichen Markierung $\Sigma(g) = \Sigma(g')$ und $\Omega^{-1}(g) \neq \Omega^{-1}(g')$ erlaubt die nicht-injektive Definition von Ω, dass g' entfernt wird und für alle $\bar{t} \in \Omega^{-1}(g')$ stattdessen $\Omega(\bar{t}) \coloneqq g$ gesetzt wird.

4.3 Eigenschaften von Schaltkreisfamilien

Definition 4.10. Eine $(\sigma, \mathbb{B})$-**Schaltkreisfamilie** $\bar{\mathcal{C}} = (\mathcal{C}_n)_{n \in \mathbb{N}}$ sei eine Sequenz von invarianten Schaltkreisen $\mathcal{C}_n = (G_n, W_n, \Sigma_n, \Omega_n, U_n)$ mit der gleichen Stelligkeit $\operatorname{ar}(\mathcal{C}_n) =$

k und den Universen $U_n = [1, n]$.

Die von der Schaltkreisfamilie berechnete σ-Anfrage $q_{\bar{\mathcal{C}}}$ sei wie folgt:

$$q_{\bar{\mathcal{C}}}(\mathfrak{A}) \coloneqq q_{\mathcal{C}_{|A|}}(\mathfrak{A})$$

Definition 4.11. Für eine Komplexitätsklasse $\mathcal{K}$ sei eine Schaltkreisfamilie $\bar{\mathcal{C}}$ $\mathcal{K}$-uniform, wenn die Berechnung einer Repräsentation von $\mathcal{C}_n$ bei Eingabe des Worts $\overbrace{1 \cdots 1}^{n}$ in $\mathcal{K}$ ist.

Definition 4.12. Beschränkte Größe

Für eine Funktion $f : \mathbb{N} \to \mathbb{N}$ habe eine Schaltkreisfamilie $\bar{\mathcal{C}}$ **f-Größe**, wenn für ein $n_0 \in \mathbb{N}$ und alle $n \geqslant n_0$ gilt, dass $|\mathcal{C}_n| \leqslant f(n)$. Für eine Klasse von Funktionen $\mathcal{F} \subseteq \mathrm{Abb}(\mathbb{N}, \mathbb{N})$ mit $f \in \mathcal{F}$ habe $\bar{C}$ $\mathcal{F}$-Größe.

Insbesondere sei $\mathrm{poly}(n) = n^{\mathcal{O}(1)}$ die Klasse aller polynomiell beschränkten Funktionen.

Bemerkung. Statt „poly (n)-groß“ wird in [1] der Begriff „P/poly-uniform“ verwendet:

Eine P/poly-Turingmaschine arbeitet in Polynomialzeit und erhält für eine Eingabe der Länge n eine polynomiell beschränkte Orakel-Eingabe $\Upsilon(n) \in \{0,1\}^{f(n)}$, $f(n) \in \mathrm{poly}(n)$. Unter Voraussetzung einer geeigneten Kodierung kann $\Upsilon(n)$ jede poly (n)-große Schaltkreisfamilie repräsentieren[3]. Daher sind die Begriffe „poly (n)-groß“ und „P/poly-uniform“ äquivalent.

Definition 4.13. Beschränkte Tiefe

Für eine Funktion $f : \mathbb{N} \to \mathbb{N}$ habe eine Schaltkreisfamilie $\bar{\mathcal{C}}$ **f-Tiefe**, wenn $T(\mathcal{C}_n) \leqslant f(n)$ für ein $n_0 \in \mathbb{N}$ und alle $n \geqslant n_0$. Für eine Klasse $\mathcal{F} \subseteq \mathrm{Abb}(\mathbb{N}, \mathbb{N})$ sei der Begriff „$\mathcal{F}$-tief“ analog zu „$\mathcal{F}$-groß“ definiert.

Definition 4.14. Benennung von Schaltkreisklassen

Sei σ eine beliebige relationale Signatur.

- Mit $\mathrm{SBC}[\sigma]$ bezeichnen wir die Klasse der Anfragen, die von einer symmetrischen $(\sigma, \mathbb{B}_{\mathrm{std}})$-Schaltkreisfamilie beschrieben werden.
- $(\mathrm{SBC} + \mathbf{MAJ})[\sigma]$ sei die Klasse der Anfragen, die von einer symmetrischen $(\sigma, \mathbb{B}_{\mathrm{maj}})$-Schaltkreisfamilie beschrieben werden. (Zur Erinnerung: $\mathbb{B}_{\mathrm{maj}} = \mathbb{B}_{\mathrm{std}} \uplus \{\mathtt{MAJ}\}$, wobei `MAJ` der Majority-Operator ist.)

Für eine Komplexitätsklasse $\mathcal{K}$ bezeichne $\mathrm{SBC}^{\mathcal{K}}$ (beziehungsweise $(\mathrm{SBC} + \mathbf{MAJ})^{\mathcal{K}}$ die Klasse der Anfragen, die von einer entsprechenden $\mathcal{K}$-uniformen Schaltkreisfamilie beschrieben werden.

Für jede dieser Klassen schreiben wir „SAC^0“ anstelle von „SBC“, um die Klasse auf Schaltkreisfamilien mit konstanter Tiefe und $\mathrm{poly}\,(n)$-Größe zu beschränken.

5 Von Formeln zu Schaltkreisfamilien

5.1 Logik erster Stufe

Wir weisen zunächst nach, dass die Logik der ersten Stufe durch symmetrische, LOGSPACE-uniforme Schaltkreisfamilien konstanter Tiefe beschrieben wird.

$$\mathrm{FO} \subseteq \left(\mathrm{SAC}^0\right)^{\mathrm{LOGSPACE}}$$

Lemma 5.1. *Jede* $\mathrm{FO}[\sigma]$*-Formel* $\varphi(\bar{x})$ *definiert eine* σ*-Anfrage* q*, die von einer symmetrischen* LOGSPACE*-uniformen Schaltkreis-Familie* $\mathcal{C}^{\varphi}$ *mit* $\|\varphi\|$*-Tiefe und* $\|\varphi\| \, n^{\mathtt{MF}(\varphi)}$*-Größe berechnet wird.*

Beweis. Sei σ eine relationale Signatur, und sei $\varphi(\bar{x})$ eine k-stellige $\mathrm{FO}[\sigma]$-Formel.

Per induktiver Konstruktion über den Aufbau von φ wird der k-stellige Schaltkreis $\mathcal{C}_n^{\varphi}$ über dem Universum $U \coloneqq [1,n]$ definiert, so dass $[\![\varphi]\!](\mathfrak{A},\bar{t}) \Leftrightarrow [\![\mathcal{C}_n^{\varphi}]\!](\mathfrak{A},\bar{t})$ für alle $n \in \mathbb{N}$, $\mathfrak{A} \in \mathbf{FIN}^{[1,n]}(\sigma)$ und $\bar{t} \in [1,n]^k$ gilt. Für eine beliebige Permutation $\pi \in \mathrm{Sym}_U$ wird ein Automorphismus $\hat{\pi}$ angegeben, und damit die Symmetrie nachgewiesen.

Fall 1. Falls $\varphi(\bar{x}) = R\bar{y}$ für $R/m \in \sigma$ und $\bar{y} \in \mathrm{frei}(\varphi)^m$, so besteht $\mathcal{C}_n^{\varphi}$ aus n^k Gates.

Schaltkreis:

$$\mathcal{C}_n^{\varphi} \coloneqq \left(\left\{g_{\bar{t}} \mid \bar{t} \in U^k\right\}, \emptyset, \Sigma, \Omega, U\right)$$

Für jedes Tupel $\bar{t} \in U^k$ sei $\beta_{\bar{t}} \coloneqq (\bar{x} \mapsto \bar{t})$ die Belegung der Variablen $\bar{x}$ mit $\bar{t}$:

$$\begin{aligned} \Sigma(g_{\bar{t}}) &\coloneqq R\beta_{\bar{t}}(\bar{y}) \\ \Omega(\bar{t}) &\coloneqq g_{\bar{t}} \end{aligned}$$

Korrektheit:

$$[\![R\bar{x}]\!](\mathfrak{A},\bar{t}) \;=\; \left[R^{\mathfrak{A}}\right](\beta_{\bar{t}}\bar{y}) \;=\; \mathcal{C}_n^{\varphi}[\mathfrak{A}](g_{\bar{t}}) = \; [\![\mathcal{C}_n^{\varphi}]\!](\mathfrak{A},\bar{t})$$

Symmetrie: Sei $\hat{\pi} g_{\bar{t}} \coloneqq g_{\pi\bar{t}}$ für alle Tupel $\bar{t} \in U^k$. Per Definition ist $\pi\beta_{\bar{t}}(\bar{y}) = \beta_{\pi\bar{t}}(\bar{y})$ und daher

$$\begin{aligned} \Sigma(\hat{\pi} g_{\bar{t}}) &= \pi\Sigma(g_{\bar{t}}) \\ \Omega(\pi\bar{t}) &= \hat{\pi}\Omega(\bar{t}) \end{aligned}$$

Größe: Der Schaltkreis hat die Tiefe 0 und die Größe $n^k = n^{\mathtt{MF}(\varphi)}$.

Fall 2. Falls $\varphi(\bar{x}) = y_1 \doteq y_2$, so besteht $\mathcal{C}_n^{\varphi}$ aus n^k isolierten Gates (hier ist $k \in \{1, 2\}$).

Schaltkreis:

$$\mathcal{C}_n^{\varphi} \coloneqq \left(\left\{g_{\bar{t}} \mid \bar{t} \in U^k\right\}, \emptyset, \Sigma, \Omega, U\right)$$

Für jedes Tupel $\bar{t} \in U^k$ sei $\beta_{\bar{t}} \coloneqq (\bar{x} \mapsto \bar{t})$ die entsprechende Belegung:

$$\begin{aligned} \Sigma(g_{\bar{t}}) &\coloneqq \begin{cases} \mathbf{1} & \text{falls } \beta(y_1) = \beta(y_2) \\ \mathbf{0} & \text{sonst} \end{cases} \\ \Omega(\bar{t}) &\coloneqq g_{\bar{t}} \end{aligned}$$

Korrektheit:

$$\begin{aligned} [\![y_1 \doteq y_2]\!](\mathfrak{A}, \bar{t}) = 1 &\Leftrightarrow (\beta_{\bar{t}} y_1 = \beta_{\bar{t}} y_2) \\ &\Leftrightarrow \mathcal{C}_n^{\varphi}[\mathfrak{A}](g_{\bar{t}}) = 1 \\ &\Leftrightarrow [\![\mathcal{C}_n^{\varphi}]\!](\mathfrak{A}, \bar{t}) = 1 \end{aligned}$$

Symmetrie: Sei $\hat{\pi}(g_{\bar{t}}) \coloneqq g_{\pi\bar{t}}$. Es gilt $\beta_{\bar{t}}(x) = \beta_{\bar{t}}(x')$ genau dann wenn $\beta_{\pi\bar{t}}(x) = \beta_{\pi\bar{t}}(x)$, und daher ist $\Sigma(\hat{\pi} g_{\bar{t}}) = \Sigma(g_{\pi\bar{t}})$.

Größe: Der Schaltkreis hat die Tiefe 0 und die Größe $n^k = n^{\mathtt{MF}(\varphi)}$.

Fall 3. Falls $\varphi(\bar{x}) = \varphi_1(\bar{y_1}) \wedge \cdots \wedge \varphi_m(\bar{y_m})$ mit $\mathrm{ar}(\varphi_i) = k_i$, so besteht $\mathcal{C}_n^{\varphi}$ aus der disjunkten Vereinigung aller $\mathcal{C}_n^{\varphi_i}$ für $1 \leqslant i \leqslant m$ mit der folgenden Erweiterung.

Schaltkreis:

$$\begin{aligned} \mathcal{C}_n^{\varphi_i} &= (G_i, W_i, \Sigma_i, \Omega_i, U) \\ \mathcal{C}_n^{\varphi} &\coloneqq (G, W, \Sigma, \Omega, U) \end{aligned}$$

Es werden neue Outputs für jedes k-Tupel aus U hinzugefügt:

$$G \coloneqq \biguplus_{i=1}^{m} G_i \uplus \left\{ g_{\bar{t}} \mid \bar{t} \in U^k \right\}$$

Die Outputs werden entsprechend mit denen von $\mathcal{C}_n^{\varphi_i}$ verknüpft, wobei $\rho_i : U^k \to U^{k_i}$ ein k-Tupel $\bar{t}$ wie folgt auf die in φ_i frei vorkommenden Variablen reduziere:

$$\begin{aligned} \text{Sei } \bar{j} &\in [1,k]^{k_i} \\ \text{so dass } \bar{y_i} &= \left(x_{(j_1)}, \cdots, x_{(j_{k_i})} \right) \end{aligned}$$

$$\text{dann } \rho_i \left(t_1, \cdots, t_k \right) \coloneqq \left(t_{(j_1)}, \cdots, t_{(j_{k_i})} \right)$$

$$\begin{aligned} W &\coloneqq \bigcup_{i=1}^{m} W_i \cup W_{\texttt{AND}} \\ W_{\texttt{AND}} &\coloneqq \left\{ \left(\Omega_i \left(\rho_i \bar{t} \right), g_{\bar{t}} \right) \mid 1 \leqslant i \leqslant m, \, \bar{t} \in U^k \right\} \end{aligned}$$

Die Gates werden entsprechend beschriftet:

$$\begin{aligned} \Sigma \left(g \right) &\coloneqq \begin{cases} \Sigma_i \left(g \right) & \text{für } g \in G_i \\ \texttt{AND} & \text{sonst} \end{cases} \\ \Omega \left(\bar{t} \right) &\coloneqq g_{\bar{t}} \text{ für alle } \bar{t} \in U^k \end{aligned}$$

Korrektheit: Es gilt für $\bar{t} \in U^k$:

$$\begin{aligned} \left[\!\left[\varphi_1 \wedge \cdots \wedge \varphi_m \right]\!\right] \left(\mathfrak{A}, \bar{t} \right) &= \min_{1 \leqslant i \leqslant m} \left[\!\left[\varphi_i \right]\!\right] \left(\mathfrak{A}, \bar{t} \right) \\ &= \min_{1 \leqslant i \leqslant m} \mathcal{C}_n^{\varphi_i} \left[\mathfrak{A} \right] \left(\Omega_i \left(\rho_i \bar{t} \right) \right) \\ &= \mathcal{C}_n^{\varphi} \left[\mathfrak{A} \right] \left(g_{\bar{t}} \right) \end{aligned}$$

Symmetrie: Es existieren bereits die Automorphismen $\hat{\pi}_i$ für jeden Schaltkreis $\mathcal{C}_n^{\varphi_i}$. Der Automorphismus $\hat{\pi}$ erweitert diese wie folgt:

$$\hat{\pi} \left(g \right) \coloneqq \begin{cases} \hat{\pi}_i \left(g \right) & \text{für } g \in G_i \\ g_{\pi \bar{t}} & \text{für } g = g_{\bar{t}} \end{cases}$$

Für die Gates und Kanten der Schaltkreise $\mathcal{C}_n^{\varphi_i}$ ist $\hat{\pi}$ per Annahme bereits korrekt.

1. Für jede neue Kante $(\Omega_i(\rho_i\bar{t}), g_{\bar{t}}) \in W_{\mathtt{AND}}$ gilt nach Voraussetzung:

$$\begin{aligned}(\hat{\pi}\Omega_i(\rho_i\bar{t}), \hat{\pi}g_{\bar{t}}) &= (\hat{\pi}_i\Omega_i(\rho_i\bar{t}), \hat{\pi}g_{\bar{t}}) \\ &= (\Omega_i(\rho_i\pi\bar{t}), g_{\pi\bar{t}}) \\ &\in W_{\mathtt{AND}}\end{aligned}$$

   (Die Reduktion $\rho_i : U^k \to U^{k_i}$ ist ein Homomorphismus und kommutiert mit der Permutation π.)

2. Es gilt $\Sigma(\hat{\pi}g_{\bar{t}}) = \Sigma(g_{\bar{t}}) = \mathtt{AND}$.

3. Es gilt $\hat{\pi}\Omega(\bar{t}) = \hat{\pi}g_{\bar{t}} = g_{\pi\bar{t}} = \Omega(\pi\bar{t})$.

Größe: Der Schaltkreis hat die Tiefe $T(\mathcal{C}_n^{\varphi})$ und die Größe $|\mathcal{C}_n^{\varphi}|$:

$$\begin{aligned}T(\mathcal{C}_n^{\varphi}) &= 1 + \max_{i=1}^{m} T\left(\mathcal{C}_n^{\psi_i}\right) \\ &\overset{\text{Ann.}}{\leqslant} 1 + \max_{i=1}^{m} \|\psi_i\| \\ &\leqslant 1 + \sum_{i=1}^{m} \|\psi_i\| \leqslant \|\varphi\|\end{aligned}$$

$$\begin{aligned}|\mathcal{C}_n^{\varphi}| &= n^k + \sum_{i=1}^{m} \left|\mathcal{C}_n^{\psi_i}\right| \\ &\overset{\text{Ann.}}{\leqslant} n^k + \sum_{i=1}^{m} \|\psi_i\| \, n^{\mathtt{MF}(\psi_i)} \\ &\leqslant n^{\mathtt{MF}(\varphi)} + \sum_{i=1}^{m} \|\psi_i\| \, n^{\mathtt{MF}(\varphi)} \\ &\leqslant n^{\mathtt{MF}(\varphi)} \left(1 + \sum_{i=1}^{m} \|\psi_i\|\right) \leqslant n^{\mathtt{MF}(\varphi)} \, \|\varphi\|\end{aligned}$$

Fall 4. Falls $\varphi(\bar{x}) = \varphi_1 \vee \cdots \vee \varphi_\ell$, so ist der Schaltkreis analog zu Fall 3 mit $\Sigma(g_{\bar{t}}) = \mathtt{OR}$.

Fall 5. Falls $\varphi(\bar{x}) = \neg\psi$, so wird der Schaltkreis $\mathcal{C}_n^{\psi}$ wie folgt erweitert:

Schaltkreis:

$$\begin{aligned} \mathcal{C}_n^{\psi} &= \left(G', W', \Sigma', \Omega', U\right) \\ \mathcal{C}_n^{\varphi} &:= (G, W, \Sigma, \Omega, U) \end{aligned}$$

Für jedes Tupel $\bar{t} \in U^k$ wird ein neues Gate $g_{\bar{t}}$ eingefügt. Die Gates werden mit den Outputs von $\mathcal{C}_n^{\varphi'}$ verknüpft.

$$\begin{aligned} G &:= G' \uplus \left\{ g_{\bar{t}} \mid \bar{t} \in U^k \right\} \\ W &:= W' \cup W_{\texttt{NOT}} \\ W_{\texttt{NOT}} &:= \left\{ \left(\Omega'\left(\bar{t}\right), g_{\bar{t}}\right) \mid \bar{t} \in U^k \right\} \\ \Sigma\left(g\right) &:= \begin{cases} \Sigma'\left(g\right) & \text{falls } g \in G' \\ \texttt{NOT} & \text{sonst} \end{cases} \\ \Omega\left(\bar{t}\right) &:= g_{\bar{t}} \end{aligned}$$

Korrektheit:

$$\begin{aligned} \left[\!\left[\neg\psi\right]\!\right]\left(\mathfrak{A}, \bar{t}\right) &= 1 - \left[\!\left[\psi\right]\!\right]\left(\mathfrak{A}, \bar{t}\right) \\ &= 1 - \mathcal{C}_n^{\psi}\left[\mathfrak{A}\right]\left(\Omega'\left(\bar{t}\right)\right) \\ &= \mathcal{C}_n^{\varphi}\left[\mathfrak{A}\right]\left(g_{\bar{t}}\right) \end{aligned}$$

Symmetrie: Es existiert bereits der Automorphismus $\hat{\pi'}$. Dieser wird wie folgt erweitert:

$$\hat{\pi}\left(g\right) := \begin{cases} \hat{\pi'}\left(g\right) & \text{falls } g \in G' \\ g_{\pi\bar{t}} & \text{falls } g = g_{\bar{t}} \end{cases}$$

Dann gilt:

$$\begin{aligned} \hat{\pi} W_{\texttt{NOT}} &= \left\{ \left(\hat{\pi}\Omega'\left(\bar{t}\right), \hat{\pi} g_{\bar{t}}\right) \mid \bar{t} \in U^k \right\} \\ &= \left\{ \left(\Omega'\left(\pi\bar{t}\right), g_{\pi\bar{t}}\right) \mid \bar{t} \in U^k \right\} = W_{\texttt{NOT}} \\ \Sigma\left(\hat{\pi} g_{\bar{t}}\right) &= \Sigma\left(g_{\bar{t}}\right) = \texttt{NOT} \end{aligned}$$

Größe: Der Schaltkreis hat die Tiefe $T\left(\mathcal{C}_n^{\varphi}\right)$ und die Größe $\left|\mathcal{C}_n^{\varphi}\right|$:

$$\begin{aligned} T\left(\mathcal{C}_n^{\varphi}\right) &= 1 + T\left(\mathcal{C}_n^{\psi}\right) \\ &\leqslant 1 + \|\psi\| \leqslant \|\varphi\| \end{aligned}$$

$$\begin{aligned} |\mathcal{C}_n^{\varphi}| &= n^k + \left|\mathcal{C}_n^{\psi}\right| \\ &\overset{\text{Ann.}}{\leqslant} n^k + \|\psi\|\, n^{\mathtt{MF}(\psi)} \\ &\leqslant n^{\mathtt{MF}(\varphi)} + \|\psi\|\, n^{\mathtt{MF}(\varphi)} \\ &\leqslant \|\varphi\|\, n^{\mathtt{MF}(\varphi)} \end{aligned}$$

Fall 6. Falls $\varphi(\bar{x}) = \exists y_1 \cdots \exists y_m \psi(z_1, \cdots, z_{k+m})$, so wird der Schaltkreis $\mathcal{C}_n^{\varphi'}$ wie folgt erweitert:

Schaltkreis:

$$\begin{aligned} \mathcal{C}_n^{\varphi} &:= (G, W, \Sigma, \Omega, U) \\ \mathcal{C}_n^{\varphi'} &:= \left(G', W', \Sigma', \Omega', U\right) \end{aligned}$$

Sei $\rho : U^{k+m} \to U^k$ die Abbildung, die aus $\bar{z}$ die gebundenen Variablen $\bar{y}$ entferne:

$$\begin{aligned} \text{Sei } \bar{i} &\in [1,k]^k \\ \text{so dass } \bar{x} &= \left(z_{(i_1)}, \cdots, z_{(i_k)}\right) \\ \text{dann } \rho(t_1, \cdots, t_k) &:= \left(t_{(i_1)}, \cdots, t_{(i_k)}\right) \end{aligned}$$

Es werden neue Outputs eingefügt.

$$G := G' \uplus \left\{ g_{\bar{t}} \mid \bar{t} \in U^k \right\}$$

Jedes Gate $\Omega'(\bar{u})$ mit $\bar{u} \in U^{k+m}$ wird mit dem Gate $g_{\rho\bar{u}}$ verknüpft.

$$\begin{aligned} W &:= W' \cup W_{\exists} \\ W_{\exists} &:= \left\{ \left(\Omega'(\bar{u}), g_{\rho\bar{u}}\right) \mid \bar{u} \in U^{k+m} \right\} \end{aligned}$$

Die neuen Outputs werden mit `OR` markiert.

$$\Sigma(g) := \begin{cases} \Sigma'(g) & \text{für } g \in G' \\ \mathtt{OR} & \text{sonst} \end{cases}$$

$$\Omega(\bar{t}) := g_{\bar{t}}$$

Korrektheit: Für $\bar{t} \in U^k$ gilt:

$$\begin{aligned}
[\![\varphi]\!](\mathfrak{A}, \bar{t}) &= \max_{\substack{\bar{u} \in U^{k+m} \\ \rho\bar{u} = \bar{t}}} [\![\psi]\!](\mathfrak{A}, \bar{u}) = 1 \\
&= \max_{\substack{\bar{u} \in U^{k+m} \\ \rho\bar{u} = \bar{t}}} \left(\mathcal{C}_n^{\varphi}[\mathfrak{A}]\left(\Omega'(\bar{u})\right)\right) \\
&= \mathcal{C}_n^{\varphi}[\mathfrak{A}](g_{\bar{t}})
\end{aligned}$$

Symmetrie: Es existiert bereits der Automorphismus $\hat{\pi'}$. Dieser wird wie folgt erweitert:

$$\hat{\pi}(g) \coloneqq \begin{cases} \hat{\pi'}(g) & \text{für } g \in G' \\ g_{\pi\bar{t}} & \text{für } g = g_{\bar{t}} \end{cases}$$

Auf den Gates von $\mathcal{C}_n^{\varphi'}$ ist $\hat{\pi}$ per Annahme treu zu π.

1. Für die neuen Kanten $(\Omega'(\bar{u}), g_{\rho\bar{u}}) \in W$ gilt:

$$\left(\hat{\pi}\Omega'(\bar{u}), \hat{\pi}g_{\rho\bar{u}}\right) = \left(\Omega'(\pi\bar{u}), g_{\rho\pi\bar{u}}\right) \in W$$

2. $\hat{\pi}\Sigma(g_{\bar{t}}) = \Sigma(g_{\bar{t}}) = \texttt{OR}$.
3. $\Omega(\pi\bar{t}) = g_{\pi\bar{t}} = \hat{\pi}g_{\bar{t}} = \hat{\pi}\Omega(\bar{t})$.

Größe: Der Schaltkreis hat die Tiefe $T(\mathcal{C}_n^{\varphi})$ und die Größe $|\mathcal{C}_n^{\varphi}|$:

$$\begin{aligned}
T(\mathcal{C}_n^{\varphi}) &= 1 + T\left(\mathcal{C}_n^{\psi}\right) \\
&\leqslant 1 + \|\psi\| \leqslant \|\varphi\|
\end{aligned}$$

$$\begin{aligned}
|\mathcal{C}_n^{\varphi}| &= n^k + \left|\mathcal{C}_n^{\psi}\right| \\
&\overset{\text{Ann.}}{\leqslant} n^k + \|\psi\| n^{\texttt{MF}(\psi)} \\
&\leqslant n^{\texttt{MF}(\varphi)} + \|\psi\| n^{\texttt{MF}(\varphi)} \\
&\leqslant \|\varphi\| n^{\texttt{MF}(\varphi)}
\end{aligned}$$

Fall 7. Falls $\varphi(\bar{x}) = \forall y_1 \cdots \forall y_m \psi(\bar{z})$, so sei der Schaltkreis analog zu Fall 8 mit $\Sigma(g_{\bar{t}}) \coloneqq \texttt{AND}$.

Speicherplatz Die beschriebene Konstruktion wird von dem $\|\varphi\| \, |\mathrm{var}(\varphi)| \log n$-platzbeschränkten Algorithmus 5.1 berechnet.

Algorithmus 5.1 Berechnung von $\mathcal{C}_n^\varphi$ für FO $[\sigma]$-Formeln.

```
Berechne(φ(x̄)):
    Für jedes t̄ ∈ [1,n]^ar(x̄):
        Gib Gate g_φ(t̄) und Ω_φ(t̄) := g_φ(t̄) aus.
        Gib Σ_φ(g_φ(t̄)) entsprechend der Konstruktion aus.
    Für jede direkte Teilformel ψ(ȳ):
        Berechne(ψ(ȳ)).
        Für jedes t̄ ∈ [1,n]^ar(x̄):
            Für jedes t̄' ∈ [1,n]^ar(ȳ):
                Falls t_i = t'_j für alle i ∈ [1,ar(x̄)], j ∈
                [1,ar(ȳ)] mit x_i = y_j:
                    Verknüpfe Ω_ψ(t̄') mit g_φ(t̄).
```

Jeder Aufruf von `Berechne` $(\varphi(\bar{x}))$ iteriert über Variablen $\bar{t} \in U^{\mathrm{var}(\varphi)}$, die $\mathrm{var}(\varphi) \log n$ Bits belegen. Da die maximale Tiefe der Rekursion durch $\|\varphi\|$ beschränkt ist, werden insgesamt $\|\varphi\| \, |\mathrm{var}(\varphi)| \log n$ Bits benötigt.

(Hierbei werden ohne Details eine passende Kodierung der Formel φ und ein Algorithmus zur platz-effizienten Berechnung von $\mathrm{frei}(\varphi)$ vorausgesetzt.)

□

5.2 Disjunkte numerische Erweiterungen

Wir betrachten eine beliebige numerische Erweiterung $\mathcal{L} + \Upsilon$, und weisen nach, dass eine Schaltkreis-Konstruktion für $\mathcal{L}$ angepasst werden kann, ohne die asymptotische Tiefe und Größe zu verändern.

Die neue Schaltkreisfamilie ist $\mathcal{K}$-uniform (mit $\mathcal{K} \supseteq$ LOGSPACE), wenn sowohl die Konstruktion für $\mathcal{L}$ als auch das Orakel $\mathcal{K}$-uniform sind.

Lemma 5.2. *Sei $\mathcal{L}$ eine Logik, $\mathbb{B}$ eine boolesche Basis und $\mathcal{K} \supseteq$ LOGSPACE eine Komplexitätsklasse, so dass für jede $\mathcal{L}[\sigma]$-Formel eine symmetrische $\mathcal{K}$-uniforme $(\sigma, \mathbb{B})$-Schaltkreisfamilie mit $t(n)$-Tiefe und $s(n)$-Größe (mit $s(\mathrm{n}) \in \mathrm{poly}(\mathrm{n})$) existiert, die die gleiche Anfrage beschreibt.*

Sei η eine von σ disjunkte Signatur und Υ ein $\mathcal{K}$-uniformes η-Orakel.

Dann existiert auch für jede $(\mathcal{L} + \Upsilon)[\sigma]$-Formel eine ebensolche Schaltkreisfamilie mit der Tiefe $t'(n) := t(2n+1)$ und der Größe $s'(n) := s(2n+1)$.

Insbesondere folgt dann aus der Kombination mit Lemma 5.1:

$$\begin{aligned} \mathrm{FO} + \mathbf{BIT} &\subseteq \left(\mathrm{SAC}^0\right)^{\mathrm{LOGSPACE}} \\ \mathrm{FO} + \mathbf{ARB} &\subseteq \left(\mathrm{SAC}^0\right)^{P/\mathrm{poly}} \end{aligned}$$

Beweis. Sei φ eine $(\mathcal{L} + \Upsilon)[\sigma]$-Formel. Für $n \in \mathbb{N}$ und $\mathfrak{A} \in \mathbf{FIN}^{(n)}(\sigma)$ wird φ als $\mathcal{L}[\sigma \uplus \eta \uplus \{\leqslant\}]$-Formel auf der disjunkt vereinigten $(\sigma \uplus \eta \uplus \{\leqslant\})$-Struktur $\mathfrak{A} \uplus \Upsilon(n)$ ausgewertet, wobei $\Upsilon(n) \in \mathbf{FIN}_{<}^{[0,n]}(\eta)$ das Universum $[0, n]$ hat.

Der Schaltkreis $\mathcal{C}_n$ wird aber auf einer umbenannten σ-Struktur $\mathfrak{A}' \coloneqq \pi\mathfrak{A} \in \mathbf{FIN}^{[1,n]}(\sigma)$ mit für $\pi : A \rightleftarrows [1, n]$ ausgewertet. Um $\mathfrak{A}'$ disjunkt mit $\Upsilon(n)$ zu vereinigen, werden wir zuerst das Universum $[0, n]$ durch eine Umbenennung nach $[n + 1, 2n + 1]$ „verschieben“:

$$\begin{aligned} \Upsilon'(n) &\coloneqq \rho\Upsilon(n) \\ \rho &: [0, n] \to [n + 1, 2n + 1] \\ \rho(i) &\coloneqq i + n + 1 \end{aligned}$$

Nun betrachten wir die disjunkte Vereinigung (wobei die Prädikate aus $\eta \uplus \{\leqslant\}$ nur auf $[n + 1, 2n + 1]$ definiert sind):

$$\mathfrak{A}' \uplus \Upsilon'(n) \in \mathbf{FIN}^{[1,2n+1]}(\sigma \uplus \eta \uplus \{\leqslant\})$$

Weil $\Upsilon(n) \cong \Upsilon'(n)$ und $\mathfrak{A} \cong \mathfrak{A}'$, gilt auch $\mathfrak{A} \uplus \Upsilon(n) \cong \mathfrak{A}' \uplus \Upsilon'(n)$ (denn der Isomorphismus ist unter disjunkter Vereinigung abgeschlossen):

$$[\![\varphi]\!](\mathfrak{A} \uplus \Upsilon(n), \beta) = [\![\varphi]\!](\mathfrak{A}' \uplus \Upsilon'(n), \beta)$$

Per Voraussetzung können wir in $\mathcal{K}$ einen $(\sigma \uplus \eta \uplus \{\leqslant\}, \mathbb{B})$-Schaltkreis $\mathcal{C}_{2n+1}^{\varphi}$ über $U' = [1, 2n + 1]$ berechnen. Dieser arbeitet korrekt auf $\mathfrak{A}' \uplus \Upsilon'(n)$ und hat offensichtlich die geforderte Größe $s'(n) = s(2n + 1)$ und Tiefe $t'(n) = t(2n + 1)$.

Anschließend konstruieren wir daraus den $(\sigma, \mathbb{B})$-Schaltkreis $\dot{\mathcal{C}}_n^{\varphi} \coloneqq \left(G, W, \dot{\Sigma}, \dot{\Omega}, U\right)$ über $U \coloneqq [1, n]$, indem alle Inputs $\Sigma(g) = R\bar{t}$ mit $\bar{t} \notin U^*$ oder $R \notin \sigma$ durch Konstanten $\dot{\Sigma}(g) \in \{\mathbf{0}, \mathbf{1}\}$ ersetzt werden, und die Ausgangsfunktion auf $\dot{\Omega} = \Omega_{|U}$ reduziert wird. Das ist eine einfache Iteration über die Gates G des Schaltkreises, die nur einen Zähler der Größe $\log(s'(n)) \in \log(\mathrm{poly}(n)) = \mathcal{O}(\log n)$ benötigt, und somit in LOGSPACE bleibt.

Fall 1. Für $\Sigma(g) = R\bar{t}$ mit $R/k \in \sigma$ werden die „überschüssigen“ Inputs einfach auf $\mathbf{0}$

gesetzt:

$$\dot{\Sigma}(g) \quad := \quad \begin{cases} R\bar{t} & \text{falls } \bar{t} \in U^k \\ \mathbf{0} & \text{sonst} \end{cases}$$

Fall 2. Für $\Sigma(g) = R\bar{t}$ mit $\sigma/k \in \eta \uplus \{\leqslant\}$ wird die numerische Relation $R^{\Upsilon'(n)}$ fest in den Schaltkreis eingebaut:

$$\dot{\Sigma}(g) \quad := \quad \begin{cases} \mathbf{1} & \text{falls } \bar{t} \in R^{\Upsilon'(n)} \\ \mathbf{0} & \text{sonst} \end{cases}$$

Sei nun $\pi \in \mathrm{Sym}_U$ eine beliebige Permutation.

Wir betrachten die Erweiterung $\pi' := \pi \cup \mathbf{id}_{[n+1,2n+1]}$, die die Elemente von $\Upsilon'(n)$ auf sich selbst abbildet. Offensichtlich ist $\pi' \in \mathrm{Sym}_{U'}$ eine Permutation von $U' = [1, 2n+1]$.

Aus der Symmetrie des Schaltkreises $\mathcal{C}^{\varphi}_{2n+1}$ bezüglich $\mathrm{Sym}_{U'}$ (siehe Lemma 5.1) folgt die Existenz eines von π' induzierten Automorphismus $\hat{\pi}$.

Es wird nun nachgewiesen, dass $\hat{\pi}$ auch ein von π induzierter Automorphismus in $\dot{\mathcal{C}}^{\varphi}_{n}$ ist. Dazu müssen nur $\dot{\Sigma}$ und $\dot{\Omega}$ betrachtet werden, da der Graph (G, W) unverändert bleibt. Ferner betrachten wir nur die nicht-konstanten Inputs von $\mathcal{C}^{\varphi}_{2n+1}$, denn ansonsten bleibt Σ unverändert.

Fall 1. Für $\Sigma(g) = R\bar{t}$ mit $R/k \in \sigma$ gilt:

Fall i. Falls $\bar{t} \in U^k$:

$$\dot{\Sigma}(\hat{\pi}g) = \Sigma(\hat{\pi}g) = R\pi\bar{t}$$

Fall ii. Sonst:

$$\dot{\Sigma}(\hat{\pi}g) = \mathbf{0} = \dot{\Sigma}(g)$$

Fall 2. Für $\Sigma(g) = R\bar{t}$ mit $R/k \in \eta \uplus \{\leqslant\}$ gilt:

Fall i. Falls $\bar{t} \in R^{\Upsilon'(n)} \subseteq [n+1, 2n+1]^k$, dann ist $\pi'\bar{t} = \bar{t}$:

$$\dot{\Sigma}(\hat{\pi}g) = \mathbf{1} = \dot{\Sigma}(g)$$

Fall ii. Sonst:

$$\dot{\Sigma}(\hat{\pi}g) = \mathbf{0} = \dot{\Sigma}(g)$$

Außerdem gilt ist U^k bezüglich π' abgeschlossen:

$$\hat{\pi}\dot{\Omega}\left(\bar{t}\right) = \hat{\pi}\Omega\left(\bar{t}\right) = \Omega\left(\pi'\bar{t}\right) = \dot{\Omega}\left(\pi'\bar{t}\right)$$

Damit ist $\bar{\mathcal{C}}^{\varphi}$ eine symmetrische, $\mathcal{K}$-uniforme Schaltkreisfamilie mit Tiefe $t'\left(n\right) = t\left(2n+1\right)$ und Größe $s'\left(n\right) = s\left(2n+1\right)$, die q berechnet. □

5.3 Logiken mit Zählquantoren

Wir betrachten die Logik $\mathcal{L}+\Upsilon+C$, und weisen nach, dass die Konstruktion von Lemma 5.2 angepasst werden kann, indem Majority-Gates hinzugefügt werden.

Lemma 5.3. *Sei $\mathcal{L}$ eine Logik, $\mathbb{B}$ eine boolesche Basis und $\mathcal{K} \supseteq$ LOGSPACE eine Komplexitätsklasse, so dass für jede $\mathcal{L}\left[\sigma\right]$-Formel eine symmetrische, $\mathcal{K}$-uniforme $\left(\sigma, \mathbb{B}\right)$-Schaltkreisfamilie mit $t\left(n\right)$-Tiefe und $\mathrm{poly}\left(n\right)$-Größe existiert, die die gleiche Anfrage beschreibt.*

Sei η eine von σ disjunkte Signatur und Υ ein $\mathcal{K}$-uniformes η-Orakel.

Dann existiert für jede $\left(\mathcal{L}+\Upsilon+C\right)\left[\sigma\right]$ eine ebensolche $\left(\sigma, \mathbb{B}\cup\{\mathtt{MAJ}\}\right)$-Schaltkreisfamilie mit der Tiefe $t'\left(n\right) \coloneqq t\left(2n+1\right) + \left\|\varphi\right\|$ und $\mathrm{poly}\left(n\right)$-Größe:

Insbesondere folgt aus der Kombination mit Lemma 5.1 und Lemma 5.2:

$$\begin{aligned} \mathrm{FO} + \mathbf{BIT} + C &\subseteq \left(\mathrm{SAC}^0 + \mathbf{MAJ}\right)^{\mathrm{LOGSPACE}} \\ \mathrm{FO} + \mathbf{ARB} + C &\subseteq \left(\mathrm{SAC}^0 + \mathbf{MAJ}\right)^{P/\mathrm{poly}} \end{aligned}$$

Wir werden in diesem Fall konkret mit $\exists^{\geqslant}$-Quantoren arbeiten, denn per Satz 3.26 sind diese gleich ausdrucksstark mit $\exists^{=}$-Quantoren und #-Termen.

Beweis. Sei φ eine $\left(\mathcal{L}+\Upsilon+\exists^{\geqslant}\right)\left[\sigma\right]$-Formel und $n \in \mathbb{N}$ die gewünschte Eingabegröße. Wir gehen analog zu Lemma 5.2 für $\mathcal{L}+\Upsilon$ vor und erzeugen einen $\left(\sigma \uplus \eta \uplus \{\leqslant\}, \mathbb{B}\cup\{\mathtt{MAJ}\}\right)$-Schaltkreis über $U' = [1, 2n+1]$, wobei wir aber die folgende induktive Konstruktion verwenden:

Fall 1. Falls $\varphi\left(\bar{x}\right)$ eine $\left(\mathcal{L}+\Upsilon\right)\left[\sigma\right]$-Formel ohne $\exists^{\geqslant}$-Quantor ist, so existiert der $\left(\sigma \uplus \eta \uplus \{\leqslant\}, \mathbb{B}\right)$-Schaltkreisfamilie $\mathcal{C}^{\varphi}_{2n+1}$ per Voraussetzung.

Fall 2. Falls $\varphi(\bar{x}) = \exists^{\geqslant x_i} y_j \psi(\bar{y})$ mit $\bar{x} \in \mathbf{var}^k$, so sei $\mathcal{C}^{\psi}_{2n+1}$ der Schaltkreis für die Formel ψ (dieser hat per Annahme die Tiefe $t(2n+1)+\|\psi\|$ und Größe $s(n) \in \mathrm{poly}(n)$).

$$\mathcal{C}^{\psi}_{2n+1} = \left(G_\psi, W_\psi, \Sigma_\psi, \Omega_\psi, U'\right)$$

Wir erzeugen den folgenden Schaltkreis $\mathcal{C}^{\varphi}_{2n+1}$:

$$\mathcal{C}^{\varphi}_{2n+1} \quad := \quad \left(G, W, \Sigma, \Omega, U'\right)$$

Es wird für jedes Tupel $\bar{t} \in U'^k$ ein neuer Output $g_{\bar{t}}$ eingefügt; ferner werden $2n$ Konstanten eingefügt:

$$\begin{aligned} G &= G_\psi \uplus \left\{ g_{\bar{t}} \mid \bar{t} \in U'^k \right\} \uplus \{0_j, 1_j \mid 1 \leqslant j \leqslant n\} \\ W &= W_\psi \uplus W_{\mathtt{MAJ}} \uplus W_{\mathrm{pad}} \end{aligned}$$

Die neuen Outputs werden mit `MAJ` markiert, falls t_i (der Wert der Variable x_i) einer der numerischen Werte (im Bereich $\rho[0,n] = [n+1, 2n+1]$) ist, und sonst mit $\mathbf{0}$.

$$\Sigma(0_j) = \mathbf{0}, \quad \Sigma(0_j) = \mathbf{1}, \quad \Sigma(g_{\bar{t}}) = \begin{cases} \mathtt{MAJ} & \text{falls } t_i \in \rho[0,n] \\ \mathbf{0} & \text{sonst} \end{cases}$$

$$\Omega(\bar{t}) = g_{\bar{t}}$$

Seien $\tau_1, \tau_2 : U^k \to U^{k-1}$ die folgenden Abbildungen, die den Wert t_i aus $\bar{t}$ beziehungsweise u_j aus $\bar{u}$ entfernen:

$$\begin{aligned} \tau_1(t_1, \cdots, t_k) &= (t_1, \cdots t_{i-1}, t_{i+1}, \cdots, t_k) \\ \tau_2(t_1, \cdots, t_k) &= (t_1, \cdots t_{j-1}, t_{j+1}, \cdots, t_k) \end{aligned}$$

Es gilt also $\tau_1(\bar{t}) = \tau_2(\bar{u})$ genau dann wenn $\bar{t}$ und $\bar{u}$ in den gemeinsamen freien Variablen von φ und ψ übereinstimmen. Das Majority-Gate $g_{\bar{t}}$ soll prüfen, ob $t_i \leqslant \rho f(\tau_1(\bar{t}))$, wobei $f : U^{k-1} \to [0,n]$ die Anzahl der ψ erfüllenden Belegungen von y_j bei der Belegung der übrigen freien Variablen mit $\tau_1(\bar{t})$ sei:

$$f\left(\bar{t}'\right) \quad := \quad \left| \left\{ u_j \in [1,n] \mid \text{es existiert } \bar{u} \in q_{\mathcal{C}^{\psi}_{2n+1}}\left(\mathfrak{A} \uplus \rho\Upsilon(n)\right), \tau_2(\bar{u}) = \bar{t}' \right\} \right|$$

Dazu wird jedes Gate $g_{\bar{t}}$ mit $t_i \in [n+1, 2n+1]$ zunächst mit den entsprechen-

den Outputs von $\mathcal{C}^{\psi}_{2n+1}$ verknüpft:

$$W_{\texttt{MAJ}} = \left\{ \left(\Omega_{\psi} \left(\bar{u} \right), g_{\bar{t}} \right) \mid \bar{t}, \bar{u} \in U'^{k},\, \tau_1 \left(\bar{t} \right) = \tau_2 \left(\bar{u} \right),\, u_j \in [1, n] \right\}$$

Momentan hat es genau n Eingänge (für jeden Wert $u_j \in [1, n]$). Daher gibt es 1 aus, wenn $f\left(\bar{t}\right) \geqslant \frac{n}{2}$. Es soll aber berechnen, ob $f\left(\bar{t}\right) \geqslant \rho^{-1} t_i$. Dazu fügen wir die Kanten W_{pad} ein, um die Eingänge der Majority-Gates mit Konstanten aufzufüllen. Ein Majority-Gate mit k zusätzlichen **0**-Eingängen entscheidet $f\left(\bar{t}\right) \geqslant \frac{n+k}{2}$, eines mit k' zusätzlichen **1**-Eingängen berechnet $f\left(\bar{t}\right) \geqslant \frac{n-k'}{2}$. Es folgt:

$$\begin{aligned} \rho^{-1} t_i \quad &\in \quad \left\{ \frac{n+k}{2}, \frac{n-k'}{2} \right\} \\ k = 2\rho^{-1} t_i - n \quad &\text{oder} \quad k' = n - 2\rho^{-1} t_i \end{aligned}$$

Jedes Majority-Gate $g_{\bar{t}}$ muss entweder $k = 2\rho^{-1} t_i - n$ **0**-Eingänge oder $k' = n - 2\rho^{-1} t_i$ **1**-Eingänge erhalten:

$$\begin{aligned} W_{\text{pad}} \quad &= \quad \left\{ \left(0_j, g_{\bar{t}} \right) \mid \bar{t} \in U'^{k},\, t_i \in \rho\left[0, n\right],\, 1 \leqslant j \leqslant 2\rho^{-1} t_i - n \right\} \\ &\cup \quad \left\{ \left(1_j, g_{\bar{t}} \right) \mid \bar{t} \in U'^{k},\, t_i \in \rho\left[0, n\right],\, 1 \leqslant j \leqslant n - 2\rho^{-1} t_i \right\} \end{aligned}$$

$$\overbrace{x_1 \cdots x_n \underbrace{\mathbf{00} \cdots \mathbf{0}}_{k = 2\rho^{-1} t_i - n}}^{n + k = 2\rho^{-1} t_i} \qquad \overbrace{x_1 \cdots x_n \underbrace{\mathbf{11} \cdots \mathbf{1}}_{k' = n - 2\rho^{-1} t_i}}^{n + k' = 2n - 2\rho^{-1} t_i}$$

Der neue Schaltkreis hat die Tiefe $t\left(2n+1\right) + \left\|\psi\right\| + 1 \leqslant t\left(2n+1\right) + \left\|\varphi\right\|$ und der Größe $s\left(n\right) + n^k + 2n \in \text{poly}\left(n\right)$.

Fall 3. Falls $\varphi\left(\bar{x}\right)$ eine andere $\left(\mathcal{L} + \Upsilon + \exists^{\geqslant}\right)\left[\sigma\right]$-Formel ist, so seien $\psi_1\left(\bar{y}_1\right), \cdots, \psi_m\left(\bar{y}_m\right)$ alle größten[1] Teilformeln von φ der Form $\psi_i = \exists^{\geqslant u_i} v_i \chi_i$. Wir ersetzen diese Teilformeln durch neue Atome $R_1 \bar{y}_1, \cdots, R_m \bar{y}_m$ und erhalten eine $\left(\mathcal{L} + \Upsilon\right)\left[\sigma \uplus \left\{R_1, \cdots, R_m\right\}\right]$-Formel φ', die per Voraussetzung zu einer $\left(\sigma \uplus \eta \uplus \left\{\leqslant\right\}, \mathbb{B}\right)$-Schaltkreisfamilie $\mathcal{C}^{\varphi'}_{2n+1}$ wird. (Eine solche Suche im Syntax-Baum der Formel hat LOGSPACE-Komplexität.)

Per Annahme existiert für jede der Teilformeln $\psi_1, \cdots, \psi_m$ ein Schaltkreis $\mathcal{C}^{\psi_i}_{2n+1}$. Wir erzeugen den Schaltkreis $\mathcal{C}^{\varphi}_{2n+1}$ aus der disjunkten Vereinigung wie

[1] d.h. solche, die nicht selbst in einer Teilformel der gleichen Form enthalten sind.

folgt:

$$\begin{aligned}
\mathcal{C}_{2n+1}^{\psi_i} &= (G_i, W_i, \Sigma_i, \Omega_i, [1, 2n+1]) \\
\mathcal{C}_{2n+1}^{\varphi'} &= \left(G', W', \Sigma', \Omega', [1, 2n+1]\right) \\
\mathcal{C}_{2n+1}^{\varphi} &:= \left(G, W, \Sigma, \Omega', [1, 2n+1]\right)
\end{aligned}$$

$$\begin{aligned}
G &:= G' \uplus \biguplus_{i=1}^{m} G_i \\
W &:= W' \uplus \biguplus_{i=1}^{m} W_i \uplus \\
&\quad \uplus \left\{ \left(\Omega_i\left(\bar{t}\right), g\right) \mid g \in G',\, \Sigma'\left(g\right) = R_i \bar{t} \right\}
\end{aligned}$$

Die Output-Gates der Schaltkreise $\mathcal{C}_{2n+1}^{\psi_i}$ werden mit den $R_i\bar{t}$-Inputs des Schaltkreises $\mathcal{C}_{2n+1}^{\varphi'}$ verbunden, und deren Beschriftung zu `AND` geändert.

$$\Sigma\left(g\right) := \begin{cases} \texttt{AND} & \text{falls } g \in G',\, \Sigma'\left(g\right) = R_i \bar{y}_i \\ \Sigma'\left(g\right) & \text{sonst, falls } g \in G' \\ \Sigma_i\left(g\right) & \text{sonst, falls } g \in G_i \end{cases}$$

Es gilt $\|\varphi'\| + \max \|\psi_i\| + 1 \leqslant \|\varphi\|$ (weil φ alle diese Teilformeln enthält). Daher ist die Tiefe des neuen Schaltkreises $t\left(2n+1\right) + \|\varphi\|$, und seine Größe ist in poly (n).

Symmetrie: Der neue Schaltkreis ist offensichtlich nicht symmetrisch bezüglich $\mathrm{Sym}_{U'}$, denn die Anzahl der konstanten Vorgänger jedes Majority-Gates $g_{\bar{t}}$ hängt von dem Wert t_i ab. Allerdings ist er symmetrisch bezüglich der Permutationen, die die Werte in $[n+1, 2n+1]$ fixieren, denn für alle übrigen Werte von t_i ist das Gate $g_{\bar{t}}$ eine **0**-Konstante.

Sei $\pi \in \mathrm{Sym}_U$ beliebig, und $\pi' := \pi \cup \mathbf{id}_{[n+1,2n+1]}$ deren Erweiterung auf U'. Nun erweitern wir den Automorphismus $\hat{\pi}$ von $\mathcal{C}_{2n+1}^{\psi}$ wie folgt:

$$\begin{aligned}
\hat{\pi}\left(0_i\right) &:= 0_i \\
\hat{\pi}\left(1_i\right) &:= 1_i \\
\hat{\pi}\left(g_{\bar{t}}\right) &:= g_{\pi'\bar{t}}
\end{aligned}$$

1. Nun gilt für jede Kante $(\Omega_\psi(\bar{u}), g_{\bar{t}}) \in W_{\text{maj}}$ mit $\bar{t}, \bar{u} \in U'^k$ und $\tau_1(\bar{t}) = \tau_2(\bar{u})$:

$$\begin{aligned}(\hat{\pi}\Omega_\psi(\bar{u}), \hat{\pi}g_{\bar{t}}) &\overset{\text{Ann.}}{=} \left(\Omega_\psi\left(\pi'\bar{u}\right), \hat{\pi}g_{\bar{t}}\right) \\ &= \left(\Omega_\psi\left(\pi'\bar{u}\right), g_{\pi'\bar{t}}\right)\end{aligned}$$

   Und weil $\pi'\bar{t}, \pi'\bar{u} \in U'^k$ und $\tau_1(\pi'\bar{t}) = \tau_2(\pi'\bar{u})$ gilt, folgt:

$$\left(\Omega_\psi\left(\pi'\bar{u}\right), g_{\pi'\bar{t}}\right) \in W_{\texttt{MAJ}}$$

2. Für jede Kante $(0_j, g_{\bar{t}}) \in W_{\text{pad}}$ (mit $\bar{t} \in U'^k$ und $t_i \in [n+1, 2n+1]$, und $j \in [1, 2t_i - 3n - 2]$):

$$(\hat{\pi}0_j, \hat{\pi}g_{\bar{t}}) = (0_j, g_{\pi'\bar{t}})$$

   Und weil $\pi' t_i = t_i$, gilt immer noch $j \in [1, 2\pi' t_i - 3n - 2]$, und daher $(\hat{\pi}0_j, \hat{\pi}g_{\bar{t}}) \in W_{\text{pad}}$. Das gleiche gilt analog für die Kanten $(\hat{\pi}1_j, \hat{\pi}g_{\bar{t}})$.

3. Für Σ:

$$\begin{aligned}\Sigma(\hat{\pi}0_j) &= \Sigma(0_j) \\ \Sigma(\hat{\pi}1_j) &= \Sigma(1_j) \\ \Sigma(\hat{\pi}g_{\bar{t}}) &= \Sigma(g_{\pi'\bar{t}}) \\ &= \begin{cases} \texttt{MAJ} & \text{falls } \pi' t_i \in [n+1, 2n+1] \\ \mathbf{0} & \text{sonst} \end{cases} \\ &= \Sigma(g_{\bar{t}})\end{aligned}$$

4. Für Ω ist $\hat{\pi}\Omega(\bar{t}) = \hat{\pi}g_{\bar{t}} = g_{\pi'\bar{t}} = \Omega(\pi'\bar{t})$ per Definition gegeben.

Nach der Erzeugung von $\mathcal{C}^{\varphi}_{2n+1}$ wird der Schaltkreis auf die bereits beschriebene Weise zu $\dot{\mathcal{C}}^{\varphi}_{n}$ umgewandelt, in dem die nicht-konstanten Inputs mit Elementen aus $[n+1, 2n+1]$ zu Konstanten werden. Der neue Schritt fügt keine nicht-konstanten Inputs hinzu, so dass sich hierbei nichts ändert.

Da der Schaltkreis $\mathcal{C}^{\varphi}_{2n+1}$ für jede Permutation $\pi \cup \mathbf{id}_{[n+1,2n+1]}$ mit $\pi \in \text{Sym}_{[1,n]}$ einen Automorphismus besitzt, ist der Schaltkreis $\dot{\mathcal{C}}^{\varphi}_{n}$ symmetrisch (siehe Lemma 5.2). □

5.4 Fixpunktlogik

Die Fixpunktlogik LFP $[\sigma]$ ist echt ausdrucksstärker als die Logik FO $[\sigma]$. Beispielsweise ist die Erreichbarkeit über einen Pfad beliebiger Länge nicht erststufig definierbar [14, 22]. In LFP $[\{E\}]$ wird diese Klasse durch die folgende Formel definiert:

$$\varphi(u,v) \coloneqq \Big[\mathrm{lfp}_{R,(x,y)}\ (\exists z\ (E(x,z) \wedge R(z,y)) \vee x = y)\Big]\ (u,v)$$

Jede LFP $[\sigma]$-Formel φ ist aber äquivalent zu einer Familie von FO $[\sigma]$-Formeln $(\varphi_n)_{n\in\mathbb{N}}$ mit einer konstanten Anzahl Variablen, so dass φ_n auf allen Strukturen der Größe n äquivalent zu φ ist. (Dies ist vergleichbar zum k-Variablen-Fragment der infinitären Logik $L^k_{\infty\omega}$, welches die Fixpunktlogik einschließt[7, 19, 20]. In unserer Definition hat jedoch jede einzelne Formel φ_n eine endliche Länge.)

Leider sind diese Formeln noch zu lang: Wenn das Symbol R mehr als einmal in ψ vorkommt, ist $\|\psi_{i+1}\| \geqslant 2\,\|\psi_i\|$, und daher wächst die Formellänge mit $\|\varphi\| \geqslant 2^{n^k}$ exponentiell für $k = \mathrm{ar}(R)$. Mit $\mathcal{C}^{\varphi}_n = \mathcal{C}^{\varphi_n}_n$ könnten wir nicht die gewünschte poly (n)-Größe ableiten.

Die booleschen Schaltkreise haben jedoch nicht dieselbe Einschränkung wie FO $[\sigma]$: Die Berechnung einer Teilformel $\psi_i(\bar{z})$ kann mehrfach verwendet werden, ohne den Schaltkreis $\mathcal{C}^{\psi_i}_n$ zu vervielfältigen.

5.4.1 Von Fixpunkt-Formeln zu Schaltkreisfamilien

Im folgenden möchten wir uns gerne auf Formeln beschränken, die nur einen einzigen Fixpunktoperator enthalten. Diese Normalform schränkt die Allgemeinheit nicht ein, was in [10] (Abschnitt 8.2) für LFP (FO) gezeigt wird.

Lemma 5.4. *(Lemma 8.2.4 aus [10])*

Jede LFP (FO) $[\sigma]$*-Formel* φ *ist äquivalent zu einer* LFP (FO) $[\sigma]$*-Formel* $\hat{\varphi}$ *der folgenden Form, wobei* $X/k \in \mathbf{var}_2$*, und* ψ *eine* FO $[\sigma \uplus \{X/k\}]$*-Formel mit* frei $(\psi) = \{x_1, \cdots, x_k\}$ *ist:*

$$(Q_i z_i)_{\substack{i\in[1,m]\\ Q_i\in\{\exists,\forall\}}}\ \left[\mathrm{lfp}_{X,\bar{x}}\psi\right](\bar{y})$$

Das Lemma für LFP (FO) gilt automatisch auch für jede numerische Erweiterung LFP $(\mathrm{FO} + \Upsilon)$ für ein η-Orakel Υ, denn eine LFP $(\mathrm{FO} + \Upsilon)$ $[\sigma]$-Formel φ gleicht syntaktisch einer LFP (FO) $[\sigma \uplus \eta]$-Formel φ'. Wenn dann φ' per Lemma 5.4 auf jeder endlichen $(\sigma \uplus \eta)$-Struktur äquivalent zu einer Formel $\hat{\varphi}'$ der obigen Form ist, dann gilt diese Äquivalenz insbesondere auch für

die Auswertung von φ auf einer σ-Struktur $\mathfrak{A}$, die disjunkt mit der η-Struktur $\Upsilon(|A|)$ vereinigt wird.

Lemma 5.5. *Sei $\mathcal{L}$ eine Logik, σ eine relationale Signatur und $\mathbb{B}$ eine boolesche Basis, so dass jede $\mathcal{L}[\sigma]$-Formel φ eine Anfrage beschreibt, die auch durch eine $\mathcal{K}$-uniforme (mit $P \subseteq \mathcal{K}$), symmetrische $(\sigma, \mathbb{B})$-Schaltkreisfamilie mit konstanter t-Tiefe und polynomiell beschränkter $s(n)$-Größe beschreibbar ist.*

Sei φ eine beliebige $\mathrm{LFP}(\mathcal{L})[\sigma]$-Formel der in Lemma 5.4 beschriebenen Normalform:

$$\varphi = (Q_i z_i)_{\substack{i \in [1,m] \\ Q_i \in \{\exists, \forall\}}} \left[\mathrm{lfp}_{X,\bar{x}} \psi\right](\bar{y})$$

Dann existiert eine $\mathcal{K}$-uniforme symmetrische $(\sigma, \mathbb{B})$-Schaltkreisfamilie $\mathcal{C}^{\varphi}$ mit $m + n^k(t+1)$-Tiefe und $1 + n^k(s(n) + m)$-Größe, so dass $q_{\mathcal{C}^{\varphi}}(\mathfrak{A}) = q_{\varphi}(\mathfrak{A})$ für alle $\mathfrak{A} \in \mathbf{FIN}(\sigma)$ gilt.

In Kombination mit dem Rest dieses Kapitels folgt dann:

$$\begin{aligned} \mathrm{LFP} + \mathbf{ORD} &\subseteq \mathrm{SBC}^{P} \\ \mathrm{LFP} + \mathbf{ARB} &\subseteq \mathrm{SBC}^{P/\mathrm{poly}} \end{aligned}$$

$$\begin{aligned} \mathrm{LFP} + C &\subseteq (\mathrm{SBC} + \mathbf{MAJ})^{P} \\ \mathrm{LFP} + \mathbf{ARB} + C &\subseteq (\mathrm{SBC} + \mathbf{MAJ})^{P/\mathrm{poly}} \end{aligned}$$

Beweis. Per Definition existiert bereits eine $(\sigma, \mathbb{B})$-Schaltkreisfamilie für jede $\mathcal{L}[\sigma]$-Formel.

Sei nun $\varphi = (Q_i z_i)_{i \in [1,m]} \varphi'$ und $\varphi' = \left[\mathrm{lfp}_{X,\bar{x}} \psi\right](\bar{y})$ für eine Relationsvariable $X/k \in \mathbf{var}_2$, eine k-stellige parameterfreie $\mathcal{L}[\sigma \uplus \{X\}]$-Formel $\psi(\bar{x})$ und ein Tupel von $\mathrm{LFP}(\mathcal{L})[\sigma]$-Termen $\bar{y} \in \mathbf{var}^k$.

Per Voraussetzung existiert eine $\mathcal{K}$-uniforme, k-stellige, symmetrische $(\sigma \cup \{X\})$-Schaltkreisfamilie $\left(\mathcal{C}_n^{\psi}\right)_{n \in \mathbb{N}}$, die auf einer $(\sigma \cup \{X\})$-Struktur $\mathfrak{A}' := \mathfrak{A} \cup (A, (X \mapsto Y))$ die Anfrage $q_{\mathcal{C}_n^{\psi}}(\mathfrak{A}') = q_{\psi(X \mapsto Y)}(\mathfrak{A})$ berechnet. (Hier wird die Relationsvariable X als neues Symbol in die Signatur mit aufgenommen.)

$$\mathcal{C}_n^{\psi} = (G_{\psi}, W_{\psi}, \Sigma_{\psi}, \Omega_{\psi}, U)$$

Wir werden für jede Eingabegröße $n \in \mathbb{N}$ einen neuen Schaltkreis für $\mathcal{C}_n^{\varphi'}$ bauen, der den Schaltkreis $\mathcal{C}_n^{\psi}$ genau n^k-mal iteriert.

Schaltkreis: Es wird eine Sequenz $\left(\mathcal{D}^i\right)_{i \in \mathbb{N}}$ von k-stelligen $(\sigma, \mathbb{B})$-Schaltkreisen definiert.

$$\mathcal{D}^i := (G_i, W_i, \Sigma_i, \Omega_i, U)$$

Für $i = 0$ nehmen wir nur eine **0**-Konstante:

$$\begin{aligned} \mathcal{D}^0 &:= (\{g_0\}, \emptyset, \Sigma_0, \Omega_0, U) \\ \Sigma_0(g_0) = \mathbf{0} \qquad & \Omega(\bar{t}) = g_0 \end{aligned}$$

Für $i \in \mathbb{N}_{\geqslant 1}$ fügen wir eine neue Kopie von $\mathcal{C}_n^\psi$ in $\mathcal{D}^i$ ein:

$$\begin{aligned} G_{i+1} &:= G_i \uplus G_\psi \\ W_{i+1} &:= W_i \uplus W_\psi \uplus W' \end{aligned}$$

$\mathcal{D}^i$ verbindet alle mit $X\bar{u}$ markierten Inputs mit dem Output $\Omega_i(\bar{u})$, und markiert sie mit „`AND`“. (Hier wäre „`OR`“ äquivalent, da jedes dieser Gates nur einen Vorgänger bekommt.)

$$\Sigma_{i+1}(g) := \begin{cases} \Sigma_i(g) & \text{falls } g \in G_i \\ \texttt{AND} & \text{falls } g \in G_\psi,\ \Sigma_\psi(g) = X\bar{u} \\ \Sigma_\psi(g) & \text{sonst} \end{cases}$$

$$W' := \{(\Omega_i(\bar{u}), g) \mid g \in G_\psi,\ \Sigma_\psi(g) = X\bar{u}\}$$

Die Outputs von $\mathcal{C}_n^\psi$ werden zu den Outputs von $\mathcal{D}^{i+1}$:

$$\Omega_{i+1} = \Omega_\psi$$

Schließlich sei $\mathcal{C}_n^\varphi := \mathcal{D}^{n^k}$.

Korrektheit: Es wird induktiv bewiesen, dass $\mathcal{D}^i$ auf $\mathfrak{A} \in \mathbf{FIN}(\sigma)$ die σ-Anfrage $q_{\mathcal{D}^i}(\mathfrak{A}) = F^i(\emptyset)$ berechnet.

$$q_{\mathcal{D}^0}(\mathfrak{A}) = F^0(\emptyset) = \emptyset$$

$$\begin{aligned} q_{\mathcal{D}^{i+1}}(\mathfrak{A}) &= q_{\mathcal{C}_n^\psi}(\mathfrak{A} \cup (A, (X \mapsto q_{\mathcal{D}^i}(\mathfrak{A})))) \\ &\overset{\text{Ann.}}{=} q_{\mathcal{C}_n^\psi}(\mathfrak{A} \cup (A, (X \mapsto F^i(\emptyset)))) \\ &= q_{\psi(X \mapsto F^i(\emptyset))}(\mathfrak{A}) \\ &\overset{\text{Def.3.12}}{=} F^{i+1}(\emptyset) \end{aligned}$$

Daher berechnet $\mathcal{C}_n^\varphi = \mathcal{D}^{n^k}$ die Anfrage $q_{\mathcal{C}_n^\varphi}(\mathfrak{A}) = F^{n^k}(\emptyset) = F^\infty(\emptyset)$.

Symmetrie: Sei $\pi \in \mathrm{Sym}_U$ beliebig. Per Annahme ist $\mathcal{C}_n^\psi$ symmetrisch, also existiert der Automorphismus $\hat{\pi}$.

Sei $\hat{\pi}_0 := \mathbf{id}_{\{g_0\}}$. Per Annahme existiere für $i \in \mathbb{N}$ ein von π induzierter Automor-

phismus $\hat{\pi}_i$ in $\mathcal{D}^i$. Sei dann $\hat{\pi}_{i+1}$ die folgende Abbildung in $\mathcal{D}^{i+1}$:

$$\hat{\pi}_{i+1}(g) \quad := \quad \begin{cases} \hat{\pi}_i(g) & \text{falls } g \in G_i \\ \hat{\pi}(g) & \text{sonst} \end{cases}$$

1. Es gilt $(\hat{\pi}_{i+1})_{|G_i} = \hat{\pi}_i$, und $(\hat{\pi}_{i+1})_{|G_\psi} = \hat{\pi}$; damit sind die Bedingungen für $W_i \cup W_\psi$, Σ_i, $\Omega_{i+1} = \Omega_\psi$ und alle internen Gates $g \in G_\psi$ mit $\Sigma_\psi \notin \{X\bar{u} \mid \bar{u} \in U^m\}$ bereits erfüllt.
2. Für die ehemaligen Inputs mit $\Sigma(g) = X\bar{u}$ gilt $\Sigma_{i+1}(\hat{\pi}g) = \Sigma_{i+1}(g) = \texttt{AND}$.
3. Für jede neue Kante $(\Omega_i(\bar{u}), g) \in W'$ mit $g \in G_\psi$ und $\Sigma_\psi(g) = X\bar{u}$:

$$\begin{aligned} (\hat{\pi}_{i+1}\Omega_i(\bar{u}), \hat{\pi}_{i+1}g) &= (\hat{\pi}_i\Omega_i(\bar{u}), \hat{\pi}g) \\ &= (\Omega_i(\pi\bar{u}), \hat{\pi}g) \end{aligned}$$

   Per Definition ist $\Sigma_\psi(\hat{\pi}g) = X\pi\bar{u}$, und daher:

$$(\Omega_i(\pi\bar{u}), \hat{\pi}g) \in W'$$

Daher ist $\mathcal{D}^{i+1}$ ebenfalls symmetrisch, und es folgt die Symmetrie von $\mathcal{C}_n^\varphi = \mathcal{D}^{n^k}$.

Größe: Es wird induktiv bewiesen, dass $T(\mathcal{D}^i) \leqslant i(t+1)$, und $|\mathcal{D}^i| \leqslant 1 + i \cdot s(n)$

$$\begin{aligned} T(\mathcal{D}^0) &= 0 \\ T(\mathcal{D}^{i+1}) &= T(\mathcal{D}^i) + T\left(\mathcal{C}_n^\psi\right) + 1 \\ &\leqslant T(\mathcal{D}^i) + t + 1 \\ &\overset{\text{Ann.}}{\leqslant} i(t+1) + t + 1 = (i+1)(t+1) \end{aligned}$$

$$\begin{aligned} |\mathcal{D}^0| &= 1 \\ |\mathcal{D}^{i+1}| &= |\mathcal{D}^i| + \left|\mathcal{C}_n^\psi\right| \\ &\leqslant |\mathcal{D}^i| + s(n) \\ &\overset{\text{Ann.}}{\leqslant} 1 + i \cdot s(n) + s(n) = 1 + (i+1)s(n) \end{aligned}$$

Damit gilt $T\left(\mathcal{C}_n^{\varphi'}\right) = T\left(\mathcal{D}^{n^k}\right) \leqslant n^k(t+1)$ und $\left|\mathcal{C}_n^{\varphi'}\right| = \left|\mathcal{D}^{n^k}\right| = 1 + n^k s(n)$.

Um jetzt noch aus $\mathcal{C}_n^{\varphi'}$ den Schaltkreis $\mathcal{C}_n^\varphi$ zu erzeugen, muss nur für jeden Quantor $Q_i z_i$ Fall 6 oder 7 aus dem Beweis von Lemma 5.1 angewendet werden. Dieser erzeugt in

jedem Schritt höchstens n^k neue Gates und vergrößert die Tiefe um 1, so dass wir die Tiefe $n^k (t+1) + m$ und Größe $n^k (s(n) + m) + 1$ erhalten. □

6 Partitionen und Träger

Unsere Konstruktion der logischen Formel aus einer Schaltkreisfamilie wird voraussetzen, dass jedes Gate g unter allen Bijektionen $\pi : A \rightleftarrows U$ ausgewertet wird. Wir stehen zunächst vor dem Problem, dass es $|\mathrm{Bij}(A, U)| = n! \in \Omega(2^n)$ solche Bijektionen gibt. Um sie für jedes Gate auf eine $\mathrm{poly}(n)$-beschränkte Zahl zu reduzieren, möchten wir gerne nachweisen, dass die $n!$ Bijektionen bezüglich jedem Gate in $\frac{n!}{(n-k)!}$ verschiedene Äquivalenzklassen der Größe $(n-k)!$ (mit $k \in \mathcal{O}(1)$) fallen (und einen effizienten Algorithmus finden, der die Repräsentanten dieser Äquivalenzklassen erzeugt).

In dem Ergebnis von Martin Otto in 1997[26] setzt er eine lokale polynomielle Beschränkung der Orbits jedes Gates voraus, und leitet für diese Schaltkreisfamilien eine Charakterisierung durch das variablen-beschränkte Fragment der infinitären Logik $L^{\omega}_{\infty\omega}$ her.

Das Ergebnis von Anderson und Dawar 2014[1] beschränkt sich auf symmetrische Schaltkreisfamilien mit polynomieller Größe (und daher automatisch polynomiell beschränkten Orbits). Hier wird für jedes Gate nachgewiesen, dass sein Wert nur von $\mathcal{O}(1)$ vielen Elementen des Universums U abhängt, und daraus eine Charakterisierung durch die Fixpunktlogik abgeleitet.

Hierfür werden zunächst die Begriffe der Partition, des Stabilisators und des Trägers eingeführt.

6.1 Partitionen einer Menge

Sei U ein beliebiges Universum. Wir führen die **Partition** als Zerlegung von U in disjunkte Teilmengen ein.

Definition 6.1. Sei $\mathcal{P} \coloneqq \{P_1, \cdots, P_k\}$ eine Menge von disjunkten nicht-leeren Mengen. Wir nennen $\mathcal{P}$ eine Partition von U, wenn $\biguplus_{i=1}^{k} P_i = U$. Sei Part_U die Menge aller Partitionen von U. Sei $\sim_{\mathcal{P}}$ eine Äquivalenzrelation auf U, deren Äquivalenzklassen von $\mathcal{P}$ repräsentiert werden.

Die Permutationen Sym_U werden auf natürliche Weise auf $\mathcal{P} \in \mathrm{Part}_U$ erweitert:

$$\pi\mathcal{P} \quad := \quad \{\pi P_i \mid P_i \in \mathcal{P}\} \in \mathrm{Part}_U$$

Als nächstes wird die **Feinheit** als Relation auf Part_U eingeführt.

Definition 6.2. Sei $\mathcal{P} \preceq \mathcal{P}'$ („$\mathcal{P}$ ist mindestens so fein wie $\mathcal{P}'$“) genau dann wenn jedes $P_i \in \mathcal{P}$ eine Teilmenge eines $P'_j \in \mathcal{P}'$ ist.

Dies ist äquivalent zu der Teilmengenbeziehung von $\sim_{\mathcal{P}}$ und $\sim_{\mathcal{P}'}$:

$$\begin{aligned}
\mathcal{P} \preceq \mathcal{P}' \quad &\Leftrightarrow \quad \text{f.a. } P \in \mathcal{P} \,\text{ex. } P' \in \mathcal{P}' \,\text{s.d. } P \subseteq P' \\
&\Leftrightarrow \quad \text{f.a. } u, u' \in U \,\text{gilt } u \sim_{\mathcal{P}} u' \Rightarrow u \sim_{\mathcal{P}'} u' \\
&\Leftrightarrow \quad (\sim_{\mathcal{P}}) \subseteq (\sim_{\mathcal{P}'})
\end{aligned}$$

Genau wie die Teilmengenbeziehung der Äquivalenzrelation bildet $\preceq$ eine Halbordnung auf Part_U.

Daher bildet Part_U einen vollständigen Verband (siehe [18]) mit den folgenden Infimum- und Supremum-Operationen $\sqcap$ und $\sqcup$:

$$\begin{aligned}
\mathcal{A} \sqcap \mathcal{B} \quad &:= \quad \max_{\preceq} \{\mathcal{P} \in \mathrm{Part}_U \mid \mathcal{P} \preceq \mathcal{A} \,\text{und}\, \mathcal{P} \preceq \mathcal{B}\} \\
\mathcal{A} \sqcup \mathcal{B} \quad &:= \quad \min_{\preceq} \{\mathcal{P} \in \mathrm{Part}_U \mid \mathcal{A} \preceq \mathcal{P} \,\text{und}\, \mathcal{B} \preceq \mathcal{P}\}
\end{aligned}$$

($\mathcal{A} \sqcap \mathcal{B}$ sei die gröbste feinere Partition als $\mathcal{A}$ und $\mathcal{B}$, und $\mathcal{A} \sqcup \mathcal{B}$ die feinste gröbere Partition als $\mathcal{A}$ und $\mathcal{B}$.)

Satz 6.3. *Wenn $[x]_\sim$ die Äquivalenzklasse $\{y \mid x \sim y\}$ ist, und $\mathcal{P}_1, \mathcal{P}_2 \in \mathrm{Part}_U$ wie folgt sind,*

$$\begin{aligned}
\mathcal{P}_1 \quad &:= \quad \left\{[x]_{\sim_{\mathcal{A}} \cap \sim_{\mathcal{B}}} \mid x \in U\right\} \\
\mathcal{P}_2 \quad &:= \quad \{[x]_{\sim^*} \mid x \in U\} \\
&\qquad\quad \text{wobei } \sim := (\sim_{\mathcal{A}}) \cup (\sim_{\mathcal{B}})
\end{aligned}$$

dann ist $\mathcal{P}_1 = \mathcal{A} \sqcap \mathcal{B}$ und $\mathcal{P}_2 = \mathcal{A} \sqcup \mathcal{B}$.

Beweis. Die Eigenschaft $\mathcal{P}_1 \preceq \mathcal{A}, \mathcal{B} \preceq \mathcal{P}_2$ folgt offensichtlich aus $(\sim_{\mathcal{A}} \cap \sim_{\mathcal{B}}) \subseteq \sim_{\mathcal{A}}, \sim_{\mathcal{B}} \subseteq (\sim_{\mathcal{A}} \cup \sim_{\mathcal{B}})^*$. Ferner muss jede Relation $\sim_{\mathcal{P}}$ mit $(\sim_{\mathcal{P}}) \subseteq (\sim_{\mathcal{A}})$ und $(\sim_{\mathcal{A}}) \subseteq (\sim_{\mathcal{B}})$ auch in $(\sim_{\mathcal{A}}) \cap (\sim_{\mathcal{B}})$ enthalten sein, und jede mit $(\sim_{\mathcal{P}}) \supseteq (\sim_{\mathcal{A}})$, $(\sim_{\mathcal{P}}) \supseteq (\sim_{\mathcal{B}})$ muss auch $(\sim_{\mathcal{A}}) \cup (\sim_{\mathcal{B}})$ (und dessen Abschluss) enthalten. □

Definition 6.4. Die feinste und gröbste Partition von U seien $\mathcal{P}_{\min}(U) \coloneqq \{\{u_1\}, \cdots, \{u_n\}\}$ und $\mathcal{P}_{\max}(U) \coloneqq \{U\}$.

6.2 Stabilisatoren einer Partition

Wir führen die Stabilisatoren von Elementen, Teilmengen und Partitionen eines Universums U ein.

Definition 6.5. Der Stabilisator eines Elements $u \in U$ in U sei die Untergruppe $\mathrm{Stab}_U(u) \subseteq \mathrm{Sym}_U$ aller Permutationen, die u fixieren:

$$\mathrm{Stab}_U(u) \coloneqq \{\pi \in \mathrm{Sym}_U \mid \pi u = u\}$$

Der Punktstabilisator einer Teilmenge $X \subseteq U$ in U sei die Untergruppe $\mathrm{Stab}_U(X) \subseteq \mathrm{Sym}_U$ der Permutationen, die jedes Element $x \in X$ fixieren:

$$\begin{aligned} \mathrm{Stab}_U(X) &\coloneqq \{\pi \in \mathrm{Sym}_U \mid \pi x = x \text{ f.a. } x \in X\} \\ &= \bigcap_{x \in X} \mathrm{Stab}_U(x) \end{aligned}$$

Der Mengenstabilisator von X in U sei die Untergruppe $\mathrm{Stab}_U\{X\} \subseteq \mathrm{Sym}_U$ der Permutationen, die die Menge X als ganzes fixieren.

$$\begin{aligned} \mathrm{Stab}_U\{X\} &\coloneqq \{\pi \in \mathrm{Sym}_U \mid \pi X = X\} \\ &= \bigcup_{\pi \in \mathrm{Sym}_X} \left(\pi \cup \mathbf{id}_{U \setminus X}\right)(\mathrm{Stab}_U(X)) \end{aligned}$$

Definition 6.6. Die obige Definition wird auf Partitionen $\mathcal{P} \in \mathrm{Part}_U$ erweitert:

Der Punktstabilisator von $\mathcal{P}$ in U sei die Untergruppe $\mathrm{Stab}_U(\mathcal{P}) \subseteq \mathrm{Sym}_U$ aller Permutationen, die jede Menge $P_i \in \mathcal{P}$ fixieren:

$$\begin{aligned} \mathrm{Stab}_U(\mathcal{P}) &\coloneqq \{\pi \in \mathrm{Sym}_U \mid \pi P_i = P_i \,\text{für alle}\, P_i \in \mathcal{P}\} \\ &= \bigcap_{P_i \in \mathcal{P}} \mathrm{Stab}_U\{P_i\} \end{aligned}$$

Der Mengenstabilisator von $\mathcal{P}$ in U sei die Untergruppe $\mathrm{Stab}_U\{\mathcal{P}\} \subseteq \mathrm{Sym}_U$ aller Permutationen, die die Partition als ganzes fixieren:

$$\mathrm{Stab}_U\{\mathcal{P}\} \coloneqq \{\pi \in \mathrm{Sym}_U \mid \pi \mathcal{P} = \mathcal{P}\}$$

Diese Gruppe wird durch $\mathrm{Stab}_U(\mathcal{P})$ und alle Permutationen von gleich-mächtigen Elementen von $\mathcal{P}$ erzeugt: Sei $\mathcal{P}_{|i} \coloneqq \{P_j \in \mathcal{P} \mid |P_j| = i\}$ für $i \in [1, |U|]$, dann gilt:

$$\mathrm{Stab}_U\{\mathcal{P}\} = \bigcup_{\substack{i \in [1,|U|] \\ \pi \in \mathrm{Sym}_{\mathcal{P}_{|i}}}} \pi \mathrm{Stab}_U(\mathcal{P})$$

Die Feinheit von Partitionen ist äquivalent zu der Teilmengenbeziehung ihrer Stabilisatoren.

Satz 6.7. *Für zwei Partitionen $\mathcal{P}, \mathcal{P}' \in \mathrm{Part}_U$ gilt $\mathcal{P} \preceq \mathcal{P}'$ genau dann wenn* $\mathrm{Stab}_U(\mathcal{P}) \subseteq \mathrm{Stab}_U(\mathcal{P}')$.

Beweis. Sei $\pi \in \mathrm{Stab}_U(\mathcal{P})$ beliebig, so besteht π aus einer Folge von Transpositionen:

$$\pi = (u_1 v_1) \circ \cdots \circ (u_k v_k)$$

Jede Transposition $(u_i v_i)$ vertauscht Elemente einer Menge $P_i \in \mathcal{P}$; daher gilt $u_i \sim_{\mathcal{P}} v_i$. Per Definition 6.2 gilt $(\sim_{\mathcal{P}}) \subseteq (\sim_{\mathcal{P}'})$, und daher $u_i \sim_{\mathcal{P}'} v_i$ und $(u_i v_i) \in \mathrm{Stab}_U(\mathcal{P}')$ für alle $i \in [1, k]$. Aus der Abgeschlossenheit des Stabilisators folgt $\pi \in \mathrm{Stab}_U(\mathcal{P}')$.

Umgekehrt impliziert auch $\mathrm{Stab}_U(\mathcal{P}) \subseteq \mathrm{Stab}_U(\mathcal{P}')$, dass für jedes Paar $u \sim_{\mathcal{P}} v$ die Transposition $(uv) \in \mathrm{Stab}_U(\mathcal{P})$ auch in $\mathrm{Stab}_U(\mathcal{P}')$ enthalten ist, und daher $u \sim_{\mathcal{P}'} v$ gilt. Aus $(\sim_{\mathcal{P}}) \subseteq (\sim_{\mathcal{P}'})$ folgt $\mathcal{P} \preceq \mathcal{P}'$. □

6.3 Träger

6.3.1 Trägerpartitionen einer Permutationsgruppe

Definition 6.8. Sei $G \subseteq \mathrm{Sym}_U$ eine Untergruppe und $\mathcal{P}$ eine Partition von U. $\mathcal{P}$ sei eine **Trägerpartition** von G genau dann wenn $\mathrm{Stab}_U(\mathcal{P}) \subseteq G$.

Wenn die Partition $\mathcal{P}$ eine Trägerpartition von G ist, dann ist sie es auch von jeder Obermenge $G' \supseteq G$. Außerdem sind per Satz 6.7 alle feineren $\mathcal{P}' \preceq \mathcal{P}$ Trägerpartitionen von G. Somit ist $\mathcal{P}_{\min} = \{\{u_1\}, \cdots, \{u_n\}\}$ mit $\mathrm{Stab}_U(\mathcal{P}_{\min}) = \{\mathbf{id}\}$ eine triviale Trägerpartition jeder Untergruppe $G \subseteq \mathrm{Sym}_U$, und alle $\mathcal{P} \in \mathrm{Part}_U$ sind Trägerpartitionen der Gruppe $\mathrm{Sym}_U = \mathrm{Stab}_U(\mathcal{P}_{\max})$.

Satz 6.9. *Wenn $\mathcal{A}$ und $\mathcal{B}$ Trägerpartitionen von G sind, so sind es auch $\mathcal{A} \sqcap \mathcal{B}$ und $\mathcal{A} \sqcup \mathcal{B}$.*

Beweis. Per Definition ist $\mathcal{A} \sqcap \mathcal{B} \preceq \mathcal{A}$ und $\mathcal{A} \sqcap \mathcal{B} \preceq \mathcal{B}$, und daher folgt die Tatsache direkt aus Satz 6.7.

Für $\mathcal{P} \coloneqq \mathcal{A} \sqcup \mathcal{B}$ gilt:

1. Jede Permutation $\pi \in \mathrm{Stab}_U(\mathcal{P})$ ist eine Folge von Transpositionen $\pi = (u_1 v_1) \circ \cdots \circ (u_k v_k)$, so dass wir nur Transpositionen betrachten müssen.
2. Die Äquivalenzrelation $\sim_{\mathcal{P}}$ ist per Satz 6.3 die transitive Hülle von $\sim \coloneqq (\sim_{\mathcal{A}} \cup \sim_{\mathcal{B}})$. Daher existiert für alle $u \sim_{\mathcal{P}} v$ eine Folge von $\ell \leqslant |U|$ Elementen $\bar{w} \in U^\ell$ mit

$$u \sim w_1 \sim \cdots \sim w_\ell \sim v$$

Sei nun $(uv) \in \mathrm{Stab}_U(\mathcal{P})$ eine beliebige Transposition. (uv) lässt sich mit dem entsprechenden $\bar{w} \in (U \setminus \{u, v\})^*$ in die folgenden Transpositionen zerlegen:

$$\begin{aligned}
(uv) &= \begin{pmatrix} u & \begin{pmatrix} w_i \\ w_i \end{pmatrix}_{1 \leqslant i \leqslant \ell} & v \\ v & & u \end{pmatrix} \\
&= \begin{pmatrix} w_1 & \begin{pmatrix} w_i \\ w_{i-1} \end{pmatrix}_{1 < i \leqslant \ell} & v \\ v & & w_\ell \end{pmatrix} \circ \begin{pmatrix} u & \begin{pmatrix} w_i \\ w_{i+1} \end{pmatrix}_{1 \leqslant i < \ell} & w_\ell & v \\ w_1 & & v & u \end{pmatrix} \\
&\quad (v w_\ell)\,(w_\ell w_{\ell-1}) \cdots (w_2 w_1) \circ (u w_1)\,(w_1 w_2) \cdots (w_{\ell-1} w_\ell)\,(w_\ell v)
\end{aligned}$$

Weil $\sim = (\sim_{\mathcal{A}} \cup \sim_{\mathcal{B}})$, ist jede der Transpositionen entweder in $\mathrm{Stab}_U(\mathcal{A})$ oder in $\mathrm{Stab}_U(\mathcal{B})$ enthalten, und beide sind Teilmengen von G. Also ist $(uv) \in G$, und es folgt $\mathrm{Stab}_U(\mathcal{P}) \subseteq G$. □

Korollar 6.10. *Jede Gruppe $G \subseteq \mathrm{Sym}_U$ besitzt eine eindeutige gröbste Trägerpartition.*

Beweis. Angenommen, $\mathcal{P}$ und $\mathcal{P}'$ seien zwei gröbste Trägerpartitionen von G. Nun ist $\mathcal{P} \sqcup \mathcal{P}'$ nach Lemma 6.9 ebenfalls eine Trägerpartition von G, und es gilt $\mathcal{P}, \mathcal{P}' \preceq \mathcal{P} \sqcup \mathcal{P}'$.

Da aber per Definition $\mathcal{P}$ und $\mathcal{P}'$ aber per Definition gröbste Träger von G sind, muss $\mathcal{P} = \mathcal{P} \sqcup \mathcal{P}' = \mathcal{P}'$ gelten. □

Definition 6.11. Für jede Gruppe $G \subseteq \mathrm{Sym}_U$ sei $\mathrm{SP}(G)$ der gröbste Träger von G.

Wir betrachten nun die Konjugations-Operation $\pi G \pi^{-1}$ einer Permutation π auf einer Untergruppe $G \subseteq \mathrm{Sym}_U$, und weisen nach, dass $\pi \mathrm{SP}(G) = \mathrm{SP}\left(\pi G \pi^{-1}\right)$.

Satz 6.12. *Wenn eine Partition $\mathcal{P}$ ein Träger einer Gruppe $G \subseteq \mathrm{Sym}_U$ ist, dann ist $\pi\mathcal{P}$ ein Träger von $\pi G \pi^{-1}$ für alle $\pi \in \mathrm{Sym}_U$.*

Beweis. Seien $\rho \in \mathrm{Stab}_U(\pi\mathcal{P})$ und $P_i \in \mathcal{P}$ beliebig. $\pi^{-1}\rho\pi$ fixiert P_i:

$$\begin{aligned}\left(\pi^{-1}\rho\pi\right) P_i &= \pi^{-1}\left(\rho\left(\pi P_i\right)\right) \\ &= \pi^{-1}\pi P_i \\ &= P_i\end{aligned}$$

Daraus folgt $\left(\pi^{-1}\rho\pi\right) \in \mathrm{Stab}_U(\mathcal{P}) \subseteq G$, und schließlich gilt:

$$\begin{aligned}\rho &= \left(\pi\pi^{-1}\right)\rho\left(\pi\pi^{-1}\right) \\ &= \pi\left(\pi^{-1}\rho\pi\right)\pi^{-1} \\ &\in \pi G\pi^{-1}\end{aligned}$$

Damit $\pi\mathcal{P}$ ein Träger der konjugierten Gruppe $\pi G\pi^{-1}$. □

Korollar 6.13. *Für jede Gruppe $G \subseteq \mathrm{Sym}_U$ und jede Permutation $\pi \in \mathrm{Sym}_U$ ist* $\pi\mathrm{SP}(G) = \mathrm{SP}\left(\pi G\pi^{-1}\right)$.

Beweis. Nach Lemma 6.12 ist $\pi\mathrm{SP}(G)$ eine Trägerpartition von $\pi G\pi^{-1}$, und daher gilt $\pi\mathrm{SP}(G) \preceq \mathrm{SP}\left(\pi G\pi^{-1}\right)$.

Umgekehrt ist auch $\pi^{-1}\mathrm{SP}\left(\pi G\pi^{-1}\right)$ eine Trägerpartition von $\pi^{-1}\pi G\pi\pi^{-1} = G$. Es folgt $\pi^{-1}\mathrm{SP}\left(\pi G\pi^{-1}\right) \preceq \mathrm{SP}(G)$ und daher $\mathrm{SP}\left(\pi G\pi^{-1}\right) \preceq \pi\mathrm{SP}(G)$. □

Satz 6.14. *Jede Gruppe G ist Obermenge des Punkt- und Teilmenge des Mengenstabilisators von* $\mathrm{SP}(G)$*:*

$$\mathrm{Stab}_U(\mathrm{SP}(G)) \subseteq G \subseteq \mathrm{Stab}_U\{\mathrm{SP}(G)\}$$

Beweis. Per Definition 6.8 gilt bereits $\mathrm{Stab}_U(\mathrm{SP}(G)) \subseteq G$.

Sei nun $\pi \in G$ beliebig. Weil $\pi G\pi^{-1} = G$, folgt nach Korollar 6.13:

$$\pi\mathrm{SP}(G) = \mathrm{SP}\left(\pi G\pi^{-1}\right) = \mathrm{SP}(G)$$

Weil π die Partition $\mathrm{SP}(G)$ auf sich selbst abbildet, gilt per Definition $\pi \in \mathrm{Stab}_U\{\mathrm{SP}(G)\}$. □

6.3.2 Trägermengen im Schaltkreis

Wir erweitern die Begriffe „Stabilisator“ und „Träger“ auf die Gates eines rigiden (Definition 4.9), symmetrischen Schaltkreises. $\mathcal{C} = (G, W, \Sigma, \Omega, U)$.

Definition 6.15. Für jedes Gate $g \in G$ sei der Stabilisator von g wie folgt definiert:

$$\mathrm{Stab}_{\mathcal{C}}(g) \coloneqq \{\pi \in \mathrm{Sym}_U \mid \hat{\pi} g = g\}$$

Eine Menge $X \subseteq U$ sei eine Trägermenge von g, wenn jede Permutation, die die Elemente von X fixiert, einen Automorphismus in $\mathcal{C}$ induziert, der g fixiert:

$$\mathrm{Stab}_U(X) \subseteq \mathrm{Stab}_{\mathcal{C}}(g)$$

Da für $X \subseteq X'$ offensichtlich $\mathrm{Stab}_U(X') \subseteq \mathrm{Stab}_U(X)$ gilt (je mehr Elemente fixiert werden, um so weniger Permutationen lassen wir zu), ist hier vor allem die kleinste Trägermenge des Gates interessant.

Satz 6.16. *Wenn $X, X' \subseteq U$ zwei Trägermengen von $g \in G$ sind, dann ist $X \cap X'$ ebenfalls eine Trägermenge von g.*

Beweis. Sei $\mathcal{P} \coloneqq \{\{x\} \mid x \in X\} \cup \{U \backslash X\}$ und $\mathcal{P}' \coloneqq \{\{x\} \mid x \in X'\} \cup \{U \backslash X'\}$. Offensichtlich gilt $\mathrm{Stab}_U(\mathcal{P}) = \mathrm{Stab}_U(X) \subseteq \mathrm{Stab}_{\mathcal{C}}(g)$ und $\mathrm{Stab}_U(\mathcal{P}') = \mathrm{Stab}_U(X') \subseteq \mathrm{Stab}_{\mathcal{C}}(g)$.

Daher sind $\mathcal{P}$ und $\mathcal{P}'$ beide Trägerpartitionen von $\mathrm{Stab}_{\mathcal{C}}(g)$. Per Satz 6.9 ist auch $\mathcal{P} \sqcup \mathcal{P}' = \{\{x\} \mid x \in X \cap X'\} \cup \{U \setminus (X \cap X')\}$ eine Trägerpartition, und per $\mathrm{Stab}_U(\mathcal{P} \sqcup \mathcal{P}') = \mathrm{Stab}_U(X \cap X')$ ist auch $X \cap X'$ eine Trägermenge von g. □

Korollar 6.17. *Jedes Gate $g \in G$ besitzt eine eindeutige kleinste Trägermenge.*

Satz 6.18. *Sei $\mathcal{P} \coloneqq \mathrm{SP}(\mathrm{Stab}_{\mathcal{C}}(g))$ die gröbste Trägerpartition des Stabilisators eines Gates g, und sei $\mathcal{P} = \{P_1, \cdots, P_k\}$ mit $|P_1| \leqslant \cdots \leqslant |P_k|$. Dann ist $X \coloneqq \bigcup_{i=1}^{k-1} P_i$ die kleinste Trägermenge von g.*

Beweis. Sei X' mit $|X'| < |X|$ eine kleinere Trägermenge von g. Per Definition ist $\mathcal{P}' \coloneqq \{\{x\} \mid x \in X'\} \cup \{U \backslash X'\}$ eine Trägerpartition von $\mathrm{Stab}_{\mathcal{C}}(g)$, denn $\mathrm{Stab}_U(\mathcal{P}') = \mathrm{Stab}_U(X') \subseteq \mathrm{Stab}_{\mathcal{C}}(g)$.

Per Definition ist $U \backslash X = P_k$ eine größte Menge in $\mathrm{SP}(\mathrm{Stab}_{\mathcal{C}}(g))$. Per Annahme ist $|X'| < |X|$ und daher $|U \backslash X'| > |U \backslash X|$. Weil aber $\mathcal{P}' \preceq \mathrm{SP}(\mathrm{Stab}_{\mathcal{C}}(g))$ ist, muss $\mathrm{SP}(\mathrm{Stab}_{\mathcal{C}}(g))$ eine Obermenge von $U \backslash X'$ als Element enthalten, und deren Größe ist mindestens $|U \backslash X'| > |U \backslash X|$; es entsteht ein Widerspruch. □

Definition 6.19. Sei $\mathrm{S}(g)$ die kleinste Trägermenge von g, und sei $\mathrm{S}(\mathcal{C}) = \max_{g \in G} |\mathrm{S}(g)|$ die maximale Größe aller Trägermengen.

6.4 Obere Schranken für die Größe von Trägern

Das Ergebnis von Anderson und Dawar beruht auf einem Theorem, das eine konstante obere Schranke $\mathrm{S}(\mathcal{C}_n) \in \mathcal{O}(1)$ für jede symmetrischen Schaltkreisfamilie $(\mathcal{C}_n)_{n\in\mathbb{N}}$ polynomieller Größe nachweist. Diese konstante Größe führt zu einer polynomiell beschränkten Anzahl von Permutationen $\left|\mathrm{Sym}_{\mathrm{S}(g)}\right| = |\mathrm{S}(g)|! \leqslant n^{|S(g)|}$ jeder Trägermenge eines Gates.

Wir stellen hierfür das sogenannte Support-Theorem vor:

Theorem 6.20. ***Support-Theorem*** *(Theorem 21 aus [1])*

Für $\epsilon \in \mathbb{R}_{\left[\frac{2}{3},1\right]}$ *und einen rigiden symmetrischen Schaltkreis* $\mathcal{C} = (G, W, \Sigma, \Omega, U)$ *mit* $|U| > 2^{\frac{56}{\epsilon^2}}$*, gilt: Wenn die maximalen Orbit-Größe mit* $s \coloneqq \max_{g\in G} \mathrm{Orb}_{\mathcal{C}}(g) \leqslant 2^{n^{1-\epsilon}}$ *subexponentiell ist, dann ist* $\mathrm{S}(\mathcal{C}) \leqslant \frac{33}{\epsilon}\frac{\log s}{\log n}$.

Korollar 6.21. *(Korollar 23 aus [1])*

Für jede symmetrische, rigide $(\sigma, \mathbb{B})$*-Schaltkreisfamilie mit* $\mathrm{poly}(n)$*-Größe gilt* $\mathrm{SP}(\mathcal{C}_n) \in \mathcal{O}(1)$.

Beweis. Die $\mathrm{poly}(n)$-Größe des Schaltkreises $\mathcal{C}_n = (G, W, \Sigma, \Omega, U)$ impliziert für jedes $\epsilon < 1$ und hinreichend große $n \in \mathbb{N}$ offensichtlich:

$$s \coloneqq \max_{g\in G} \mathrm{Orb}_{\mathcal{C}}(g) \leqslant |\mathcal{C}_n| \leqslant n^c < 2^{n^{1-\epsilon}}$$

Damit ist $\mathrm{S}(\mathcal{C}) \leqslant \frac{33}{\epsilon}\frac{\log s}{\log n} \leqslant \frac{33}{\epsilon}\frac{k\log n}{\log n} = \frac{33k}{\epsilon} \in \mathcal{O}(1)$. □

7 Von Schaltkreisfamilien zu Formeln

7.1 Berechnung von rigiden Schaltkreisen

Um die Eindeutigkeit der im symmetrischen Schaltkreis induzierten Automorphismen zu gewährleisten, wird nun gefordert, dass der Schaltkreis *rigide* gemäß Definition 4.9 ist.

Die Rigidität kann nicht in jeder booleschen Basis $\mathbb{B}$ problemlos hergestellt werden, ohne die Tiefe zu verändern - während redundante Vorgänger von `AND`- und `OR`-Gates ohne Beschränkung der Annahme entfernt werden können, ist dies zum Beispiel bei `MAJ`- und `XOR`-Gates nicht möglich.

In [1] werden redundante Gates $H = (g_1, \cdots, g_k)$ „in Reihe“ geschaltet, so dass jedes Gate $g_i \in H \setminus \{g_1\}$ durch ein `AND`-Gate mit dem Vorgänger g_{i-1} ersetzt wird. Dies vergrößert jedoch die Tiefe des Schaltkreises unbeschränkt.

Um die Tiefe als Parameter zu erhalten, werden wir stattdessen die Definition des Schaltkreises auf Multigraphen erweitern:

Definition 7.1. Multimenge

Eine Multimenge $\mathcal{W} : W \to \mathbb{N}$ sei eine Abbildung einer Menge auf $\mathbb{N}$, wobei $\mathcal{W}(x)$ die Vielfachheit von x in $\mathcal{W}$ angibt.

Nach der in Definition 2.3 eingeführten Notation entspricht für eine gewöhnliche Relation $W \subseteq G^2$ die Funktion $[W] : G^2 \to \{0, 1\}$ gerade der äquivalenten Multimenge. Die Größe der Multimenge $|\mathcal{W}| \coloneqq \sum_{w \in \mathcal{W}} \mathcal{W}(x)$ sei die Summe der Vielfachheiten aller Elemente.

Definition 7.2. Multischaltkreis

Ein $(\sigma, \mathbb{B}_{\text{std}})$-Multischaltkreis $\mathcal{C} = (G, \mathcal{W}, \Sigma, \Omega, U)$ ist analog zum $(\sigma, \mathbb{B})$-Schaltkreis definiert, aber $(G, \mathcal{W})$ bildet einen azyklischen Multigraphen:

$$\mathcal{W} : G \times G \to \mathbb{N}$$

Formal beschreiben wir den Multischaltkreis durch eine $\tau_{\sigma,\mathbb{B},k}$-Struktur $\mathcal{C}$ über einem Universum $G \uplus U \uplus [0, |\mathcal{W}|]$ ausgewertet:

$$\begin{aligned} \tau'_{\sigma,\mathbb{B},k} &:= \left\{ W/3, (\Sigma_s/1)_{s \in \mathbb{B} \uplus \{\mathbf{0},\mathbf{1},\mathtt{NOT}\}}, (\Sigma_R/1+k)_{R/k \in \sigma}, \Omega/k+1 \right\} \\ \operatorname{ar}(W) &:= 3 \\ W^{\mathcal{C}} &= \left\{ (g, g', n) \in G^2 \times [0, |\mathcal{W}|] \mid \mathcal{W}(g, g') = n \right\} \end{aligned}$$

Für die Auswertung eines internen Gates gilt analog zu 4.4:

$$\begin{aligned} j_1 &:= \sum_{h \in G} (\mathcal{C}[\mathfrak{A}](h) \cdot \mathcal{W}(h, g)) \\ j_0 &:= \sum_{h \in G} \mathcal{W}(h, g) - j_1 \\ \mathcal{C}[\mathfrak{A}](g) &:= [\Sigma(g)](j_0, j_1) \end{aligned}$$

Die Größe $|\mathcal{C}|$ eines Multischaltkreises $\mathcal{C}$ sei die Summe seiner Gates und Kanten:

$$|\mathcal{C}| := |G| + \sum_{g,g' \in G^2} \mathcal{W}(g, g')$$

Die Symmetrie wird auf natürliche Weise angepasst: Der von π induzierte Automorphismus $\hat{\pi} \in \operatorname{Aut}_{\mathcal{C}}$ bildet $(G, \mathcal{W})$ auf den isomorphen Multigraphen $(\hat{\pi}G, \hat{\pi}\mathcal{W})$ mit $\mathcal{W}(\hat{\pi}g, \hat{\pi}g') = \mathcal{W}(g, g')$ ab.

Die Rigidität wird ebenfalls angepasst: Ein rigider Schaltkreis enthält keine Gates g, g' mit $\Sigma(g) = \Sigma(g')$ und $\mathcal{W}(h, g) = \mathcal{W}(h, g')$ für alle $h \in G$.

Lemma 7.3. *(nach Lemma 24 aus [1])*

Es existiert ein Algorithmus, der einen beliebigen $(\sigma, \mathbb{B})$-Schaltkreis $\mathcal{C}$ in einen rigiden Multischaltkreis $\hat{\mathcal{C}}$ umwandelt, wobei $T\left(\hat{\mathcal{C}}\right) = T(\mathcal{C})$ und $\left|\hat{\mathcal{C}}\right| \leqslant |\mathcal{C}| + |\mathcal{C}|^2$. Der Algorithmus ist $\operatorname{poly}(|G| + |U|)$*-zeitbeschränkt.*

Beweis. Sei $\mathcal{C}'' = (G, W, \Sigma, \Omega, U)$ ein beliebiger k-stelliger Schaltkreis. Wir erzeugen zunächst den äquivalenten Multischaltkreis $\mathcal{C} := (G, \mathcal{W}, \Sigma, \Omega, U)$ mit $\mathcal{W} := [W]$, wobei die Tiefe unverändert bleibt und die Größe zu $|\mathcal{C}| = |G| + |W| \leqslant |\mathcal{C}''| + |\mathcal{C}''|^2$ wird.

Der Multischaltkreis $\mathcal{C}$ wird nun wiederholt reduziert, bis er rigide ist: Berechne dazu die Äquivalenzrelation $\sim_{\mathcal{C}} \subseteq G \times G$, so dass $g \sim_{\mathcal{C}} g'$ genau dann wenn

1. $\Sigma(g) = \Sigma(g')$, und

2. für alle $h \in W$ gilt $\mathcal{W}(h, g) = \mathcal{W}(h, g')$.

Wenn keine Gates $g, g' \in G$ mit $g \sim_{\mathcal{C}} g'$ mehr existieren, so ist der Schaltkreis rigide, und der Algorithmus ist fertig.

Ansonsten sei $E \subseteq G$ eine Äquivalenzklasse von $\sim_{\mathcal{C}}$ mit mindestens zwei Gates und minimaler Tiefe $T(E)$.

Wir berechnen die Funktion $c : G \to [0, |E|]$, die für jedes Gate $h \in G$ die Vorgänger in E zählt:

$$c(h) \coloneqq \sum_{g' \in E} \mathcal{W}(g', h)$$

Sei $g \in E$ beliebig, und sei $f_{g,E}(\mathcal{C}) \coloneqq (G', \mathcal{W}', \Sigma', \Omega', U)$ der folgende Multischaltkreis:

$$\begin{aligned} G' &\coloneqq G \setminus (E \setminus \{g\}) \\ \Sigma' &\coloneqq \Sigma_{\setminus E \setminus \{g\}} \end{aligned}$$

1. Es werden die eingehenden Kanten der Gates $E \setminus \{g\}$ entfernt. Außerdem werden die von E ausgehenden Kanten entfernt und durch Kanten von g ersetzt:

$$\mathcal{W}'(h, i) \coloneqq \begin{cases} c(i) & \text{falls } h = g \\ 0 & \text{falls } h \in E \setminus \{g\} \\ 0 & \text{falls } i \in E \setminus \{g\} \\ \mathcal{W}(h, i) & \text{sonst} \end{cases}$$

2. Die Output-Funktion wird wie folgt angepasst:

$$\Omega'(\bar{t}) \coloneqq \begin{cases} g & \text{falls } \Omega(t) \in E \setminus \{g\} \\ \Omega(t) & \text{sonst} \end{cases}$$

Der Schaltkreis $\mathcal{C}' \coloneqq f_{g,E}(\mathcal{C})$ ist äquivalent zu dem Schaltkreis $\mathcal{C}$ über jeder Struktur $\mathfrak{A} \in \mathbf{FIN}^U(\sigma)$, was induktiv über die Tiefe (ausgehend von g) nachgewiesen wird:

1. Offensichtlich gilt $\mathcal{C}'[\mathfrak{A}](g) = \mathcal{C}[\mathfrak{A}](g) = \mathcal{C}[\mathfrak{A}](g')$ für alle $g' \in E$, da die Gates die gleichen Vorgänger und die gleiche Beschriftung $\Sigma'(g) = \Sigma(g) = \Sigma(g')$ besitzen.

2. Für jeden direkten Nachfolger $h \in G$ eines Gates $g' \in E$ gilt:

$$\begin{aligned} j_1 &:= \sum_{i \in G'} \mathcal{W}(i,h) \cdot \mathcal{C}[\mathfrak{A}] \\ j_0 &:= \sum_{i \in G'} \mathcal{W}(i,h) - j_1 \\ j_1' &:= \sum_{i \in G'} \mathcal{W}'(i,h) \cdot \mathcal{C}'[\mathfrak{A}] \\ j_0' &:= \sum_{i \in G'} \mathcal{W}'(i,h) - j_1' \end{aligned}$$

   Aus der Definition von $\mathcal{W}'$ folgt $j_1 = j_1'$ und $j_0 = j_0'$, da die $c(h) - 1$ entfernten Vorgänger $g' \in E \setminus \{g\}$ durch $c(h) - 1$ zusätzliche (g,h)-Kanten ersetzt wurden, und $\mathcal{C}[\mathfrak{A}](g) = \mathcal{C}[\mathfrak{A}](g')$. Daher gilt:

$$\begin{aligned} \mathcal{C}'[\mathfrak{A}](g) &:= \left[\Sigma'(g)\right](j_0', j_1') \\ &= [\Sigma(g)](j_0, j_1) \\ &= \mathcal{C}[\mathfrak{A}] \end{aligned}$$

3. Für jedes übrige Gate $h \in G$ folgt die Äquivalenz aus der Induktionsannahme und der Tatsache, dass die Vorgänger von h unverändert bleiben.

Für jedes Tupel $\bar{t} \in U^k$ mit $\Omega(\bar{t}) = g' \in E$ gilt nun:

$$\begin{aligned} [\![\mathcal{C}']\!](\mathfrak{A}, \bar{t}) &= \mathcal{C}'[\mathfrak{A}]\left(\Omega'(\bar{t})\right) \\ &= \mathcal{C}'[\mathfrak{A}](g) \\ &= \mathcal{C}[\mathfrak{A}](g) \\ &= \mathcal{C}[\mathfrak{A}]\left(g'\right) \\ &= \mathcal{C}[\mathfrak{A}](\Omega(\bar{t})) = [\![\mathcal{C}]\!](\mathfrak{A}, \bar{t}) \end{aligned}$$

Größe: Die Umrechnung von $\mathcal{C}$ zu $f_{g,E}(\mathcal{C})$ lässt die Tiefe unverändert, und vergrößert den Schaltkreis nicht: Es werden $\sum_{h \in G} c(h)$ Kanten eingefügt und mindestens $\sum_{g',h' \in E \times G}$ Kanten entfernt, wobei gilt:

$$\sum_{h \in G} c(h) = \sum_{h \in G} \sum_{g' \in E} \mathcal{W}(g', h) = \sum_{g',h' \in E \times G}$$

Symmetrie: Wenn alle Äquivalenzklassen $\bar{E} = (E_1, \cdots, E_m)$ der gleichen Tiefe reduziert werden, dann bewahrt der neue Schaltkreis $f_{g_1,E_1} \cdots f_{g_m,E_m}(\mathcal{C}) = \mathcal{C}'$ die Symmetrie

von $\mathcal{C}$:

Sei $\pi \in \mathrm{Sym}_U$ eine beliebige Permutation, und $\hat{\pi}$ ein induzierter Automorphismus. Offensichtlich muss $\hat{\pi}$ die Äquivalenzklassen $\bar{E}$ aufeinander abbilden, da $\hat{\pi} g \sim_{\mathcal{C}} \hat{\pi} g'$ für alle $g \sim_{\mathcal{C}} g'$ gilt.

Der Automorphismus $\hat{\pi}$ auf $\mathcal{C}$ wird wie folgt zu einem auf $\mathcal{C}'$ angepasst:

$$\hat{\pi}' g \coloneqq \begin{cases} g_i & \text{falls } \hat{\pi} g \in E_i \\ \hat{\pi} g & \text{sonst} \end{cases}$$

Da $\mathcal{W}(\hat{\pi} g, \hat{\pi} g') = \mathcal{W}(g, g')$, folgt $\mathcal{W}'(\hat{\pi} g, \hat{\pi} g')$.

Die Umrechnung von $\mathcal{C}$ zu $\mathcal{C}'$ verkleinert die Äquivalenzklasse des Gates g zu $\{g\}$, da alle äquivalenten Gates entfernt werden, und lässt alle anderen Äquivalenzklassen der Tiefe $i \leqslant T(g)$ unverändert.

Daher haben nach höchstens $|G|$ Wiederholungen alle Äquivalenzklassen der Tiefe $i \leqslant T(g)$ die Größe 1, und nach höchstens $T(\mathcal{C}) \cdot |G|$ Wiederholungen wird ein äquivalenter, rigider Schaltkreis erzeugt. □

Satz 7.4. *Die beschriebene Konstruktion kann mit $\mathcal{O}(T(\mathcal{C}) \log n)$ Speicherplatz berechnet werden, und ist für Schaltkreisfamilien konstanter Tiefe daher in* LOGSPACE.

Beweis. Der Algorithmus 7.1 gibt die Kanten und Markierungen des rigiden Multischaltkreises aus, wobei eine natürliche Ordnung der Gates G vorausgesetzt wird.

Sei $\sim^*$ eine rekursive Erweiterung von $\sim$, die alle Paare von Gates g, g' enthält, die aus jeder Äquivalenzklasse bezüglich $\sim^*$ die gleiche Anzahl Vorgänger besitzen. Ferner sei $\leqslant$ eine implizite Ordnung der Gates G. Ein Gate $g \in G$, für das $g \not\sim^* g'$ für alle $g' < g$ gilt, nennen wir den Repräsentanten seiner Äquivalenzklasse.

Der beschriebene Algorithmus wird `Rigid`(g) für jeden Repräsentanten $g \in G$ aufrufen. `Rigid`(g) gibt dann g mit seinen Markierungen aus, findet dann jeden Repräsentanten $h \in G$, zählt die zu h äquivalenten Vorgänger von g und gibt die entsprechende Multikante $\mathcal{W}(h, g) \in \mathbb{N}$ aus.

Da die Funktionen `Rigid` und `Equiv` jeweils nur konstant viele lokale Variablen der Größe $\mathcal{O}(\log n)$ verwenden, ist der Algorithmus platzbeschränkt durch $T \cdot \mathcal{O}(\log n)$, wobei T die maximale Rekursionstiefe von `Equiv` ist. Weil jeder Aufruf `Equiv`(g) nur Aufrufe `Equiv`(h, h') für Vorgänger h, h' von g auslöst, ist $T = T(\mathcal{C})$ die Tiefe des Schaltkreises $\mathcal{C}$. □

Algorithmus 7.1 Rigider Schaltkreis in LOGSPACE

```
Input: (G, W, Σ, Ω, U).
Main:
    Für jedes Gate g ∈ G:
        Falls kein Gate g' < g mit Equiv(g, g') existiert:
            Rigid(g).
Rigid(g):
    Gib g und Σ(g) aus.
    Für alle t̄ ∈ U^k mit Ω(t̄) = g:
        Gib Ω(t̄) = g aus.
    Für jedes Gate h ∈ G:
        Falls kein Gate h' < h mit Equiv(h, h') existiert:
            i ← 0.
            Für alle Vorgänger h'' von g mit Equiv(h, h'').
              i ← i + 1.
            Gib W(h, g) = i aus.
Equiv(g, g'):
    Falls nicht Σ(g) = Σ(g'): FALSE
    Für jeden Vorgänger h von g:
        i ← 0
        Für jeden Vorgänger h' von g mit Equiv(h, h'):
            i ← i + 1.
        Für jeden Vorgänger h' von g' mit Equiv(h, h'):
            i ← i − 1
        Falls i ≠ 0: FALSE.
    TRUE
```

7.2 Berechnung der Orbits und Träger

Satz 7.5. *(nach Satz 9 aus [1])*

Sei $\mathcal{C}$ ein rigider $(\sigma, \mathbb{B})$-Multischaltkreis über U. Sei $\pi \in \mathrm{Sym}_U$ beliebig.

Falls π einen Automorphismus in $\mathcal{C}$ induziert, dann ist dieser eindeutig.

Beweis. Sei $\mathcal{C} = (G, \mathcal{W}, \Sigma, \Omega, U)$ und $\pi \in \mathrm{Sym}_U$ beliebig. Seien $\hat{\pi}_1, \hat{\pi}_2 : \mathcal{C} \tilde{\to} \mathcal{C}$ zwei von π induzierte Automorphismen.

Durch Induktion über die Tiefe wird bewiesen, dass $\hat{\pi}_1 g = \hat{\pi}_2 g$ für jedes Gate $g \in G$ gilt.

Anfang: Wenn g eine Konstante mit $\Sigma(g) \in \{\mathbf{0}, \mathbf{1}\}$ ist, dann ist g das einzige Gate mit der Beschriftung $\Sigma(g)$:

$$\hat{\pi}_1 g = g = \hat{\pi}_2$$

Wenn g ein relationales Input mit $\Sigma(g) = R\bar{t}$, $R/k \in \sigma$ und $\bar{t} \in U^k$ ist, dann existiert auf Grund der Rigidität nur ein Gate $g' \in G$ mit $\Sigma(g') = R\pi\bar{t}$:

$$\hat{\pi}_1 g = g' = \hat{\pi}_2 g$$

Schritt: Wenn g ein internes Gate mit $\Sigma(g) \in \mathbb{B}$ ist, dann muss gelten:

$$\begin{aligned} \Sigma(\hat{\pi}_1 g) &= \Sigma(\hat{\pi}_2 g) = \Sigma(g) \\ \mathcal{W}(\hat{\pi}_1 h, \hat{\pi}_1 g) &= \mathcal{W}(\hat{\pi}_2 h, \hat{\pi}_2 g) = \mathcal{W}(h, g) \\ &\quad \text{f.a. } h \in G \end{aligned}$$

Auf Grund der Rigidität von $\mathcal{C}$ muss $\hat{\pi}_1 g = \hat{\pi}_2 g$ gelten.

□

Lemma 7.6. *(nach Lemma 25 aus [1])*

Es existiert ein deterministischer Algorithmus, der bei Eingabe eines rigiden $(\sigma, \mathbb{B})$-Multischaltkreises $\mathcal{C} = (G, \mathcal{W}, \Sigma, \Omega, U)$ und einer Permutation $\pi \in \mathrm{Sym}_U$ in $\mathrm{poly}(|\mathcal{C}|)$-Zeit für jedes Gate $g \in G$ das Gate $\hat{\pi}g$ ausgibt, falls π einen Automorphismus $\hat{\pi}$ induziert.

Beweis. Analog zu dem Beweis von Lemma 7.5 wird gezeigt, dass der eindeutige Automorphismus in Polynomialzeit bestimmt wird:

1. Zunächst sei für jedes konstante Gate $\hat{\pi}g := g$. Für jedes relationale Input $g \in G$ mit $\Sigma(g) = R\bar{t}$ finde das einzige Gate $g' \in G$ mit $\Sigma(g) = R\pi\bar{t}$ und gib $\hat{\pi}g := g'$ aus.

Algorithmus 7.2 Automorphismus in LOGSPACE

```
Input: (G, W, Σ, Ω, U), k, π.
Main:
    Für g, g' ∈ G:
        Falls Aut(g, g'):
            Gib π̂(g) = g' aus.
Aut(g, g'):
    Falls Σ(g) ≠ Σ(g') ∈ 𝔹 ⊎ {0, 1, NOT}: False
    Falls Σ(g) = Rt̄, Σ(g') ≠ Rπt̄: False
    Für t̄ ∈ U^k:
        Falls Ω(t̄) = g und Ω(πt̄) ≠ g': False
    Für jeden Vorgänger h von g:

        Falls kein Vorgänger h' von g' mit Aut(h, h') existiert:
            False
    True
```

2. Finde ein beliebiges Gate $g \in G$, für dessen Vorgänger $h \in G$ mit $\mathcal{W}(h,g) > 0$ bereits $\hat{\pi}h = h'$ ausgegeben wurde.
3. Finde ein Gate $g' \in G$ mit $\Sigma(g) = \Sigma(g')$ und $\mathcal{W}(\hat{\pi}h, g') = \mathcal{W}(h,g)$ für die Vorgänger $h \in G$, so dass g' sonst keine Vorgänger hat. (Wegen der Rigidität gibt es höchstens eines.) Gib $\hat{\pi}g = g'$ aus.
4. Wiederhole die Schritte 2 bis 3 solange bis $\hat{\pi}$ für jedes Gate $g \in G$ berechnet wurde. (Wenn zu irgendeinem g kein Gate gefunden wird, ist der Schaltkreis nicht symmetrisch und der Algorithmus bricht ab.)

Die Schritte 2 bis 3 werden höchstens $|G|$-mal wiederholt, und jeder Schritt erfordert $|G|^2$-Zeit, so dass der Algorithmus in $|G|^3$-Zeit arbeitet. □

Satz 7.7. *Die obige Konstruktion ist mit $\mathcal{O}(T(\mathcal{C}) \log n)$ Speicherplatz berechenbar, und ist für Schaltkreisfamilien konstanter Tiefe daher in* LOGSPACE.

Beweis. Der Algorithmus 7.2 berechnet den Automorphismus $\hat{\pi}$, in dem für jedes Paar von Gates g, g' rekursiv geprüft wird, ob $\hat{\pi}g = \hat{\pi}g'$.

Da jede Funktion nur konstant viele lokale Variablen der Größe $\mathcal{O}(\log n)$ verwendet, ist der Speicherplatz durch die Funktion $T \cdot \mathcal{O}(\log n)$ beschränkt.

□

Lemma 7.8. *(nach Lemma 26 aus [1])*

Es existiert ein deterministischer Algorithmus, der bei Eingabe eines rigiden $(\sigma, \mathbb{B})$-Multischaltkreises $\mathcal{C} = (G, \mathcal{W}, \Sigma, \Omega, U)$ in $\mathrm{poly}(|\mathcal{C}|)$ entscheidet, ob dieser symmetrisch ist, und gegebenenfalls die Orbits $\mathrm{Orb}_{\mathcal{C}}(g)$ und Träger $\mathrm{SP}(g)$ jedes Gates $g \in G$ ausgibt.

Beweis. Um die Symmetrie nachzuweisen, genügt es, den Algorithmus aus Lemma 7.6 für jede Transposition $(uv) \in \mathrm{Sym}_U$ durchzuführen. Diese Transpositionen erzeugen die gesamte Symmetriegruppe Sym_U, und daher ist für jede Permutation $\pi = (u_1 v_1) \cdots (u_k v_k) \in \mathrm{Sym}_U$ die Abbildung $\hat{\pi} = \hat{\pi}_{(u_1 v_1)} \cdots \hat{\pi}_{(u_k v_k)}$ ein von π induzierter Automorphismus.

1. Berechne den von $(uv) \in \mathrm{Sym}_U$ induzierten Automorphismus $\hat{\pi}_{(uv)}$ für jedes Paar $u, v \in U$ mit $u \neq v$. Wenn nicht alle Automorphismen existieren, ist der Schaltkreis nicht symmetrisch; es wird abgebrochen.
2. Für jedes Gate $g \in G$ wird der Träger $\mathrm{SP}(g)$ aufgebaut, in dem für jede Transposition $(uv) \in \mathrm{Sym}_U$ geprüft wird, ob $\hat{\pi}_{(uv)}$ das Gate g fixiert. In diesem Fall werden die Elemente u, v in der Partition kombiniert:

$$\begin{aligned} \mathcal{P}_{(uv)} &:= \{\{u, v\}\} \cup \{\{w\} \mid w \in U \setminus \{u, v\}\} \\ \mathcal{P}_g &:= \bigsqcup_{\substack{(uv) \in \mathrm{Sym}_U \\ \hat{\pi}_{(uv)} g = g}} \mathcal{P}_{(uv)} \end{aligned}$$

3. Für jedes Gate $g \in G$ sei $S_0 := \{g\}$. Iterativ wird der Orbit von g wie folgt aufgebaut, bis mit $S_{i+1} = S_i$ ein Fixpunkt erreicht wird (spätestens bei $S_{|U|}$):

$$S_{i+1} := S_i \cup \bigcup_{(uv) \in \mathrm{Sym}_U} \hat{\pi}_{(uv)} S_i$$

Nach den Definitionen aus Kapitel 7 ist jede Partition $\mathcal{P}_{(uv)}$ Träger von g, wenn $\hat{\pi}_{(uv)} g = g$, und daher ist $\mathcal{P}_g$ ebenfalls ein Träger von g. Wenn es einen gröberen Träger $\mathcal{P}'$ gäbe, dann müsste dieser zwei Elemente $u, v \in U$ kombinieren, die in $\mathcal{P}_g$ getrennt sind, und für die $\hat{\pi}_{(uv)} g = g$ gilt. In diesem Fall ist aber die Partition $\mathcal{P}_{(uv)}$ mit in $\mathcal{P}_g$ aufgenommen worden, und es gilt $\mathcal{P}_{(uv)} \preceq \mathcal{P}_g = \mathrm{SP}(g)$.

Für die Mengen $(S_i)_{i \in \mathbb{N}}$ gilt $S_i \subseteq \mathrm{Orb}_{\mathcal{C}}(g)$, denn per Induktion existiert für jedes Gate $g' \in S_i$ eine Folge von i Transpositionen $\pi_1 \cdots \pi_i$, so dass $\hat{\pi}_1 \cdots \hat{\pi}_i$ das Gate g auf g' abbildet. Ferner besteht jede Permutation π aus einer Folge von höchstens $|U|$ Transpositionen, so dass $S_{|U|} \supseteq \mathrm{Orb}_{\mathcal{C}}(g)$ den gesamten Orbit von g enthält.

Es existieren weniger als $|U|^2$ Transpositionen, so dass der Schritt 1 in $|G|^3 |U|^2$-Zeit abgeschlossen wird. Ebenso wird Schritt 2 in $|U|^3$-Zeit abgeschlossen (die Operation $\mathcal{P} \sqcup \mathcal{P}'$

für Partitionen ist durch eine Union-Find-Datenstruktur effektiv in $|U|$-Zeit berechenbar). Schritt 3 erfordert eine Iteration bis $S_{|U|}$, wobei jeder Durchlauf $|U|^2$-Zeit benötigt. Insgesamt läuft der Algorithmus in $|G|^3\,|U|^3$-Zeit. □

7.3 Rekursive Auswertung der Schaltkreise

Für eine rigide, symmetrische k-stellige $(\sigma, \mathbb{B})$-Multischaltkreisfamilie $(\mathcal{C}_n)_{n\in\mathbb{N}}$ gilt nach Korollar 6.21 $\mathrm{SP}(\mathcal{C}_n) \in \mathcal{O}(1)$. Seien also $n_0, c \in \mathbb{N}$ so gewählt, dass $\mathrm{SP}(\mathcal{C}_n) \leqslant c$ für $n \geqslant n_0$.

Zur Erinnerung: $\mathrm{SP}(\mathcal{C})$ misst die maximale Größe der Vereinigung aller nicht-größten Teile $U\backslash P_m$ des gröbsten Trägers $\mathrm{SP}(g) = \{P_1, \cdots, P_m\}$, $|P_1| \leqslant \cdots \leqslant |P_m|$ jedes Gates g von $\mathcal{C}$.

Per Definition ist $\mathcal{P}_{U\backslash P_m} = \{\{u\} \mid u \in U\backslash P_m\} \cup \{P_m\} \preceq \mathrm{SP}(g)$ ein Träger von g, und $\left|\mathcal{P}_{U\backslash P_m}\right| := 1 + |U\backslash P_m| \leqslant 1 + c$.

Es sei $\mathrm{sp}(g) := U\backslash P_m$ die Menge der in $\mathcal{P}_{U\backslash P_m}$ getrennten Elemente; diese Menge nennen wir den **kanonischen Träger** des Gates g.

Wir möchten $\mathcal{C}_n$ auf beliebigen Strukturen $\mathfrak{A} \in \mathbf{FIN}^{(n)}(\sigma)$ (nicht nur $\mathfrak{A} \in \mathbf{FIN}^{[1,n]}(\sigma)$) auswerten, wofür eine beliebige Einbettung $\pi : A \to [1, n]$ definiert werden muss. Es wird nun gezeigt, dass die Auswertung des Gates g nur von dem Teil der Abbildung π abhängt, der Elemente auf $\mathrm{sp}(g)$ abbildet. Die Abbildung auf die übrigen Elemente $U\backslash\mathrm{sp}(g)$ ist für g unbedeutend.

Die Folgerung in diesem Abschnitt passt den Abschnitt 4.3 aus [1] für Multischaltkreise an.

Definition 7.9. Konsistenz

Zwei bijektive Abbildungen $f, f' : A \to B$ seien konsistent in $A' \subseteq A$ (kurz $f \sim_{A'} f'$), wenn sie im Teilbereich A' identisch sind.

$$f \sim_{A'} f' \Leftrightarrow f_{|A'} = f'_{|A'}$$

Für $B' \subseteq B$ heißen sie bildkonsistent in B', wenn $f^{-1} \sim_{B'} f^{-1}$ beziehungsweise wenn $f = \tau f'$ mit einer Permutation $\tau \in \mathrm{Stab}_B(B')$, die die Elemente von B' fixiert.

Satz 7.10. *Sei $\mathcal{C} = (G, \mathcal{W}, \Sigma, \Omega, U)$ ein rigider, symmetrischer Multischaltkreis mit $n = |U|$, und sei $g \in G$ ein beliebiges Gate mit den Vorgängern $H := \{h \in G \mid \mathcal{W}(h, g) > 0\}$. Sei $\mathfrak{A} \in \mathbf{FIN}^{(n)}(\sigma)$ eine beliebige Struktur. Seien $\pi_1, \pi_2 : A \to U$ zwei beliebige Einbettungen von $\mathfrak{A}$ in U, die bildkonsistent in $\mathrm{sp}(g)$ sind. So gilt:*

$$\mathcal{C}[\pi_1\mathfrak{A}](g) = \mathcal{C}[\pi_2\mathfrak{A}](g) \tag{7.1}$$

$$\sum_{h\in H} \mathcal{W}(h, g) \cdot \mathcal{C}[\pi_1\mathfrak{A}](h) = \sum_{h\in H} \mathcal{W}(h, g) \cdot \mathcal{C}[\pi_2\mathfrak{A}](h) \tag{7.2}$$

Beweis. Sei $\tau \in \mathrm{Sym}_U$ die Permutation $\tau \coloneqq \pi_1 \pi_2^{-1}$, so dass $\pi_1 = \tau\pi_2$.
Weil π_1 und π_2 bildkonsistent in $\mathrm{sp}(g)$ sind, gilt $\pi_1^{-1}u = \pi_2^{-1}u$ für $u \in \mathrm{sp}(g)$.

$$\begin{aligned} \tau u &= \pi_1 \pi_2^{-1} u \\ &= \pi_1 \pi_1^{-1} u = u \end{aligned}$$

Wegen der Symmetrie und Rigidität induziert τ einen eindeutigen Automorphismus $\hat{\tau}$ im Schaltkreis $\mathcal{C}$. Weil τ die Elemente von $\mathrm{sp}(g)$ fixiert, fixiert $\hat{\tau}$ auch das Gate g:

$$\begin{aligned} \tau &\in \mathrm{Stab}_U(\mathrm{sp}(g)) \\ &\subseteq \mathrm{Stab}_{\mathcal{C}}(g) \end{aligned}$$

Damit ist Gleichung 7.1 bewiesen:

$$\begin{aligned} \mathcal{C}[\pi_2 \mathfrak{A}](g) &= \mathcal{C}[\tau\pi_2 \mathfrak{A}](\hat{\tau} g) \\ &= \mathcal{C}[\tau\pi_2 \mathfrak{A}](g) \\ &= \mathcal{C}[\pi_1 \mathfrak{A}](g) \end{aligned}$$

Da $\hat{\tau} g = g$, muss auch $\hat{\tau} H = H$ auch für die Vorgänger gelten. Außerdem hat $\hat{\tau} h$ die gleiche Anzahl von Kanten zu g wie τ:

$$\begin{aligned} \mathcal{C}[\pi_2](h) &= \mathcal{C}[\tau\pi_2](\hat{\tau} g) \\ \mathcal{W}(h, g) &= \mathcal{W}(\hat{\tau}, g) \end{aligned}$$

Es folgt die Gleichung 7.2 für das Gewicht der mit 1 belegten Vorgänger von g:

$$\sum_{h \in H} \mathcal{W}(h, g) \cdot \mathcal{C}[\pi_1 \mathfrak{A}](h) = \sum_{h \in H} \mathcal{W}(h, g) \cdot \mathcal{C}[\pi_2 \mathfrak{A}](h)$$

□

Definition 7.11. Für jedes Gate g des Schaltkreises $\mathcal{C}$ über dem Universum U beschreiben wir die Menge der verschiedenen Bijektionen $\pi \in \mathrm{Bij}(U, A)$, für die $\mathcal{C}\left[\pi^{-1}\mathfrak{A}\right](g) = 1$. Per Satz 7.10 müssen nur deren Reduktionen auf $\mathrm{sp}(g)$ betrachtet werden. Sei $\mathrm{EV}(g)$ die Menge dieser Belegungen von $\mathrm{sp}(g)$:

$$\mathrm{EV}(g) \coloneqq \left\{ \pi_{|\mathrm{sp}(g)} \mid \pi : \mathrm{Bij}(U, A), \mathcal{C}\left[\pi^{-1}\mathfrak{A}\right](g) = 1 \right\}$$

Für jede injektive Funktion $\rho : \mathrm{sp}(g) \to A$ sei M_ρ die Menge der zu ρ konsistenten

Bijektionen $\pi : U \to A$:

$$M_\rho \coloneqq \left\{\pi \in \mathrm{Bij}\,(U, A) \mid \pi_{|\mathrm{sp}(g)} = \rho\right\}$$

Zusätzlich beschreiben wir für jeden Vorgänger $h \in H$ von g und jede injektive Funktion $\rho : \mathrm{sp}\,(g) \to A$ die Menge $\Pi_\rho\,(h)$ der unterschiedlichen $\mathrm{sp}\,(h)$-Reduktionen von Bijektionen $\pi : U \to A$, die auf $\mathrm{sp}\,(g)$ konsistent zu π sind:

$$\Pi_\rho\,(h) \coloneqq \left\{\pi_{|\mathrm{sp}(h)} \mid \pi \in M_\rho\right\}$$

Behauptung 7.12. (nach Behauptung 28 aus [1])

Sei $\pi : U \to A$ eine beliebige Bijektion, und $\rho \coloneqq \pi_{|\mathrm{sp}(g)}$. Das Gesamtgewicht der unter $\pi^{-1}\mathfrak{A}$ erfüllten Vorgänger $h \in H$ gleicht der gewichteten Summe von $\frac{|\Pi_\rho(h) \cap \mathrm{EV}(h)|}{|\Pi_\rho(h)|}$, dem Anteil der erfüllenden Bijektionen in $\Pi_\rho\,(h)$:

$$r \coloneqq \sum_{h \in H} \mathcal{W}\,(h, g)\, \mathcal{C}\left[\pi^{-1}\mathfrak{A}\right](h) = \sum_{h \in H} \mathcal{W}\,(h, g)\, \frac{|\Pi_\rho\,(h) \cap \mathrm{EV}\,(h)|}{|\Pi_\rho\,(h)|} \tag{7.3}$$

Beweis. Nach Gleichung 7.2 ist das Gesamtgewicht der unter $\pi'^{-1}\mathfrak{A}$ erfüllten Gates $h \in G$ für alle $\pi' \in M_\rho$ gleich, so dass $|M_\rho|\, r$ die Summe der Gesamtgewichte für jede Belegung $\pi' \in M_\rho$ ist.

Weiterhin können wir für jeden Vorgänger $h \in H$ die Belegungen M_ρ in Äquivalenzklassen bezüglich der Konsistenz zu einer Belegung $\rho' \in \Pi_\rho\,(h)$ von $\mathrm{sp}\,(h)$ partitionieren:

$$\begin{aligned} |M_\rho|\, r &= \sum_{h \in H} \mathcal{W}\,(h, g) \sum_{\pi' \in M_\rho} \mathcal{C}\left[\pi'^{-1}\mathfrak{A}\right](h) \\ &= \sum_{h \in H} \mathcal{W}\,(h, g) \sum_{\rho' \in \Pi_\rho(h)} \sum_{\substack{\pi' \in M_\rho \\ \pi'_{|\mathrm{sp}(h)} = \rho'}} \mathcal{C}\left[\pi'^{-1}\mathfrak{A}\right](h) \end{aligned}$$

Nach der Definition der Menge $\mathrm{EV}\,(h)$ gilt für alle Belegungen $\pi' : U \to A$, dass $\mathcal{C}\left[\pi'^{-1}\mathfrak{A}\right](h) = 1$ genau dann wenn $\pi'_{|\mathrm{sp}(h)} \in \mathrm{EV}\,(h)$. Daher können wir $[\mathrm{EV}\,(h)]\,(\rho') \in \{0, 1\}$ einfach mit der Größe von $\left\{\pi' \in M_\rho \mid \pi'_{|\mathrm{sp}(h)} = \rho'\right\}$ multiplizieren:

$$\begin{aligned} |M_\rho|\, r &= \sum_{h \in H} \mathcal{W}\,(h, g) \sum_{\rho' \in \Pi_\rho(h)} \sum_{\substack{\pi' \in M_\rho \\ \pi'_{|\mathrm{sp}(h)} = \rho'}} [\mathrm{EV}\,(h)]\,(\rho') \\ &= \sum_{h \in H} \mathcal{W}\,(h, g) \sum_{\rho' \in \Pi_\rho(h)} [\mathrm{EV}\,(h)]\,(\rho') \left|\left\{\pi' \in M_\rho,\, \pi'_{|\mathrm{sp}(h)} = \rho'\right\}\right| \end{aligned}$$

Weil die Partitionierung $M_\rho = \biguplus_{\rho' \in \Pi_\pi(h)} \left\{\pi' \in M_\rho,\, \pi'_{|\mathrm{sp}(h)} = \rho'\right\}$ die Menge M_ρ in isomorphe Klassen teilt, gilt $\left|\left\{\pi' \in M_\rho,\, \pi'_{|\mathrm{sp}(h)} = \rho'\right\}\right| = \frac{|M_\rho|}{|\Pi_\rho(h)|}$ für $\rho' \in \Pi_\rho(h)$.

$$\begin{aligned}
|M_\rho|\, r &= \sum_{h \in H} \mathcal{W}(h,g) \sum_{\rho' \in \Pi_\rho(h)} [\mathrm{EV}(h)]\left(\rho'\right) \frac{|M_\rho|}{|\Pi_\rho(h)|} \\
&= \sum_{h \in H} \mathcal{W}(h,g) \sum_{\rho' \in \Pi_\rho(h) \cap \mathrm{EV}(h)} \frac{|M_\rho|}{|\Pi_\rho(h)|} \\
&= \sum_{h \in H} \mathcal{W}(h,g) \frac{|\Pi_\rho(h) \cap \mathrm{EV}(h)|\, |M_\rho|}{|\Pi_\rho(h)|}
\end{aligned}$$

Durch das Kürzen von $|M_\rho|$ entsteht die Gleichung 7.3 aus der Behauptung. □

Sei nach Definition 2.1 $\bar{U}$ das geordnete Tupel aller Elemente des Universums, und $\bar{\mathrm{sp}}(g)$ das Tupel der Elemente von $\mathrm{sp}(g)$.

Sei $\bar{M}_\rho \subseteq A^n$ die Relation der n-Tupel $\pi\bar{U}$ für $\pi \in M_\rho$, sei $\bar{\Pi}_\rho(h) \subseteq A^{|\mathrm{sp}(h)|}$ die Relation der Tupel $\rho\bar{\mathrm{sp}}(h)$ für $\rho \in \Pi_\rho(h)$, und sei $\bar{\mathrm{EV}}(g) \subseteq A^{|\mathrm{sp}(g)|}$ die Relation der Tupel $\rho\bar{\mathrm{sp}}(g)$ für $\rho \in \mathrm{EV}(g)$.

$$\begin{aligned}
\bar{M}_\rho &:= \left\{\pi\bar{U} \mid \pi \in M_\rho\right\} \\
\bar{\mathrm{EV}}(g) &:= \left\{\rho\bar{\mathrm{sp}}(g) \mid \rho \in \mathrm{EV}(g)\right\}
\end{aligned}$$

Wir werden nun für jedes Gate $g \in G$ mit den Vorgängern $H \subseteq G$ die Menge $\bar{\mathrm{EV}}(g)$ rekursiv durch $\left(\bar{\mathrm{EV}}(h)\right)_{h \in H}$ und $\mathfrak{A}$ definieren, wobei $\rho_{\bar{a}} : \mathrm{sp}(g) \to A$ für $\bar{a} \in A^{|\mathrm{sp}(g)|}$ die Abbildung $\rho_{\bar{a}} = (\bar{\mathrm{sp}}(g) \mapsto \bar{a})$ bezeichne.

Fall 1. Falls g eine Konstante mit $\Sigma(g) \in \{\mathbf{0}, \mathbf{1}\}$ ist, dann ist $\mathrm{sp}(g) = \emptyset$, da g ein Fixpunkt aller Automorphismen ist. In diesem Fall gilt:

$$\bar{\mathrm{EV}}(g) = \begin{cases} \emptyset & \text{falls } \Sigma(g) = \mathbf{0} \\ \{\langle\rangle\} & \text{falls } \Sigma(g) = \mathbf{1} \end{cases}$$

Fall 2. Falls g ein relationales Input mit $\Sigma(g) = R\bar{t}$, $R/k \in \sigma$ und $\bar{t} \in \mathrm{sp}(g)^k$ ist, dann gilt:

$$\bar{\mathrm{EV}}(g) = R^{\mathfrak{A}} \cap \left\{\rho_{\bar{a}}\bar{t} \mid \bar{a} \in A^{|\mathrm{sp}(g)|}\right\}$$

Fall 3. Falls $\Sigma(g) = \texttt{AND}$ ist, dann gilt für jedes Tupel $\bar{a} \in A^{|\mathrm{sp}(g)|}$, dass $\rho_{\bar{a}} \in \mathrm{EV}(g)$ genau dann wenn jede zu $\rho_{\bar{a}}$ konsistente Bijektion $\pi \in M_{\rho_{\bar{a}}}$ alle Vorgänger

$h \in H$ erfüllt:

$$\sum_{h \in H} \mathcal{W}(h,g)\, \mathcal{C}\left[\pi^{-1}\mathfrak{A}\right](h) \quad = \quad \sum_{h \in H} \mathcal{W}(h,g)$$

Beziehungsweise nach Behauptung 7.12:

$$\sum_{h \in H} \mathcal{W}(h,g)\, \frac{|\Pi_{\rho_{\bar{a}}}(h) \cap \mathrm{EV}(h)|}{|\Pi_{\rho_{\bar{a}}}(h)|} = \sum_{h \in H} \mathcal{W}(h,g)$$

Dies ist gleichbedeutend mit $\Pi_{\rho_{\bar{a}}}(h) \subseteq \mathrm{EV}(h)$. Demnach gilt:

$$\bar{\mathrm{EV}}(g) = \left\{ \bar{a} \in A^{|\mathrm{sp}(g)|} \mid \bigwedge_{h \in H} \bar{\Pi}_{\rho_{\bar{a}}}(h) \subseteq \bar{\mathrm{EV}}(h) \right\}$$

Fall 4. Falls $\Sigma(g) = \texttt{OR}$ ist, dann ist $\rho_{\bar{a}} \in \mathrm{EV}(g)$ genau dann wenn mindestens eine Bijektion $\pi \in M_\rho$ mindestens einen Vorgänger $h \in H$ erfüllt:

$$\sum_{h \in H} \mathcal{W}(h,g)\, \frac{|\Pi_{\rho_{\bar{a}}}(h) \cap \mathrm{EV}(h)|}{|\Pi_{\rho_{\bar{a}}}(h)|} > 0$$

$$\bar{\mathrm{EV}}(g) = \left\{ \bar{a} \in A^{|\mathrm{sp}(g)|} \mid \bigvee_{h \in H} \left(\bar{\Pi}_{\rho_{\bar{a}}}(h) \cap \bar{\mathrm{EV}}(h) \neq \emptyset\right) \right\}$$

Fall 5. Falls $\Sigma(g) = \texttt{MAJ}$ ist, dann ist $\rho_{\bar{a}} \in \mathrm{EV}(g)$ genau dann wenn mindestens die Hälfte der Vorgänger erfüllt sind:

$$\sum_{h \in H} \mathcal{W}(h,g)\, \frac{|\Pi_{\rho\bar{a}}(h) \cap \mathrm{EV}(h)|}{|\Pi_{\rho_{\bar{a}}}(h)|} \geqslant \frac{1}{2} \sum_{h \in H} \mathcal{W}(h,g)$$

Fall 6. Falls $\Sigma(g) = \texttt{NOT}$, dann hat g per Definition des Schaltkreises genau einen Vorgänger h, es gilt $\mathrm{sp}(g) = \mathrm{sp}(h)$ und $\mathcal{C}\left[\pi^{-1}\mathfrak{A}\right](g) = 1 - \mathcal{C}\left[\pi^{-1}\mathfrak{A}\right](h)$. Also:

$$\bar{\mathrm{EV}}(g) = A^{|\mathrm{sp}(g)|} \backslash \bar{\mathrm{EV}}(h)$$

Die vom Schaltkreis $\mathcal{C}$ berechnete Anfrage $q_{\mathcal{C}}$ ist äquivalent zu der folgenden Relation:

$$q_{\mathcal{C}}(\mathfrak{A}) \coloneqq \left\{ \bar{a} \in A^k \mid \text{ex. } \bar{t} \in U^k \text{ mit } \bar{a} \in \mathrm{EV}(\Omega(\bar{t})) \right\}$$

7.4 Kodierung durch Fixpunktlogik

Die beschriebenen Klassen Relationen EV werden nun verwendet, um die Klasse SBC auf die Fixpunktlogik LFP zu reduzieren.

Lemma 7.13. *Sei $(\mathcal{C}_n)_{n\in\mathbb{N}}$ eine k-stellige, rigide, symmetrische, P-uniforme $(\sigma, \mathbb{B}_{\text{std}})$-Multischaltkreisfamilie. Es existiert eine $(\text{LFP} + \mathbf{ORD})[\sigma]$-Formel φ aufbauen, so dass für $n \in \mathbb{N}$ und $\mathfrak{A} \in \mathbf{FIN}^{(n)}(\sigma)$ die Formel $\varphi(\bar{x})$ die gleiche Anfrage definiert wie $\mathcal{C}_n$:*

$$q_{\mathcal{C}_n}(\mathfrak{A}) = q_\varphi(\mathfrak{A})$$

Beweis. Da die Schaltkreisfamilie von einer P-Turingmaschine berechnet wird, existiert nach dem Immerman-Vardi-Theorem[30, 15] und Lemma 7.3 eine Sammlung von LFP $[\{\leqslant\}]$-Formeln Φ, die auf der Struktur $\mathbf{ORD}(n)$ ausgewertet den Schaltkreis $\mathcal{C}_n$ beschreiben:

$$\Phi := \left(\varphi_G, \varphi_{\mathcal{W}}, \varphi_\Omega, (\varphi_\phi)_{\phi\in\mathbb{B}\uplus\{\mathbf{0},\mathbf{1},\texttt{NOT}\}}, (\varphi_R)_{R\in\sigma}\right)$$

Hierbei sei $f_G : G \to [1,n]^c$ eine geeignete Kodierung der höchstens n^c Gates von $\mathcal{C}_n$, und $f_W : [1,n^c] \to [1,n]^c$ eine Kodierung von Zahlen, so dass für $\bar{g}, \bar{h}, \bar{w} \in [0,n]^c$:

$$\begin{aligned}
\mathbf{ORD}(n) \models \varphi_G[\bar{g}] &\Leftrightarrow f_G^{-1}(\bar{g}) \in G \\
\mathbf{ORD}(n) \models \varphi_W[\bar{h}\bar{g}\bar{w}] &\Leftrightarrow \mathcal{W}\left(f_G^{-1}(\bar{h}), f_G^{-1}(\bar{g})\right) = f_W^{-1}(\bar{w}) \\
\mathbf{ORD}(n) \models \varphi_\Omega[\bar{t}\bar{g}] &\Leftrightarrow \Omega(\bar{t}) = f_G^{-1}(\bar{g}) \\
&\quad \text{für } \bar{t} \in [1,n]^k \\
\mathbf{ORD}(n) \models \varphi_\phi[\bar{g}] &\Leftrightarrow \Sigma\left(f_G^{-1}(\bar{g})\right) = \phi \\
&\quad \text{für } \phi \in \mathbb{B} \uplus \{\mathbf{0},\mathbf{1},\texttt{NOT}\} \\
\mathbf{ORD}(n) \models \varphi_R[\bar{g}\bar{x}] &\Leftrightarrow \Sigma\left(f_G^{-1}(\bar{g})\right) = R\bar{x} \\
&\quad \text{für } R/m \in \sigma,\ \bar{x} \in [1,n]^m
\end{aligned}$$

Für $n < n_0$ gibt es nur eine endliche Anzahl von festen Schaltkreisen $\mathcal{C}_n$. Jeder dieser Schaltkreise ist durch eine FO $[\sigma]$-Formel kodierbar: Sei $\psi_n(\bar{x})$ eine Formel, die prüft, ob $|A| = n$, und dann prüft, ob für alle $n!$ Bijektionen $\pi : A \to U$ gilt, dass $\mathcal{C}[\pi\mathfrak{A}](\Omega(\pi\beta\bar{x}))$ mit $\beta : \text{frei}(\psi_n) \to A$.

[...] □

7.5 Schaltkreise konstanter Tiefe

Das Resultat von Anderson und Dawar werden wir nun auf Schaltkreise konstanter Tiefe ausweiten, die auf $\mathrm{FO} + \mathbf{BIT}$ reduzierbar sind.

Lemma 7.14. *Sei $(\mathcal{C}_n)_{n\in\mathbb{N}}$ eine k-stellige, rigide, symmetrische,* LOGSPACE*-uniforme $(\sigma, \mathbb{B})$-Multischaltkreisfamilie mit konstanter c-Tiefe und n^d-Größe. Es existiert eine $(\mathrm{FO} + \mathbf{BIT})[\sigma]$-Formel φ, so dass für $n \in \mathbb{N}$ und $\mathfrak{A} \in \mathbf{FIN}^{(n)}(\sigma)$ die Formel $\varphi(\bar{x})$ die gleiche Anfrage definiert wie $\mathcal{C}_n$.*

Beweis. Weil die Schaltkreisfamilie von einer LOGSPACE-Turingmaschine berechnet wird, existiert nach Immerman[17] eine Sammlung von $\mathrm{FO}[\{\mathtt{BIT}\}]$-Formeln Φ, die auf der Struktur $\mathbf{BIT}(n)$ ausgewertet den Schaltkreis $\mathcal{C}_n$ beschreiben:

$$\Phi := \left(\varphi_G, \varphi_{\mathcal{W}}, \varphi_\Omega, (\varphi_\phi)_{\phi\in\mathbb{B}\uplus\{\mathbf{0},\mathbf{1},\mathtt{NOT}\}}, (\varphi_R)_{R\in\sigma}\right)$$

Hierbei sei $f_G : G \to [1,n]^d$ eine geeignete Kodierung der höchstens n^d Gates von $\mathcal{C}_n$, und $f_W : \left[1, n^d\right] \to [1,n]^d$ eine Kodierung von Zahlen, so dass für $\bar{g}, \bar{h}, \bar{w} \in [0,n]^d$:

$$\begin{aligned}
\mathbf{BIT}(n) \models \varphi_G[\bar{g}] &\Leftrightarrow f_G^{-1}(\bar{g}) \in G \\
\mathbf{BIT}(n) \models \varphi_W[\bar{h}\bar{g}\bar{w}] &\Leftrightarrow \mathcal{W}\left(f_G^{-1}(\bar{h}), f_G^{-1}(\bar{g})\right) = f_W^{-1}(\bar{w}) \\
\mathbf{BIT}(n) \models \varphi_\Omega[\bar{t}\bar{g}] &\Leftrightarrow \Omega(\bar{t}) = f_G^{-1}(\bar{g}) \\
&\quad \text{für } \bar{t} \in [1,n]^k \\
\mathbf{BIT}(n) \models \varphi_\phi[\bar{g}] &\Leftrightarrow \Sigma\left(f_G^{-1}(\bar{g})\right) = \phi \\
&\quad \text{für } \phi \in \mathbb{B} \uplus \{\mathbf{0}, \mathbf{1}, \mathtt{NOT}\} \\
\mathbf{BIT}(n) \models \varphi_R[\bar{g}\bar{x}] &\Leftrightarrow \Sigma\left(f_G^{-1}(\bar{g})\right) = R\bar{x} \\
&\quad \text{für } R/m \in \sigma,\ \bar{x} \in [1,n]^m
\end{aligned}$$

[...] □

8 Grenzen der symmetrischen Schaltkreisklassen

Wir weisen nach, dass die symmetrischen AC^0-Schaltkreisfamilien eine echte Teilmenge der Anfragen beschreiben, die durch AC^0 definierbar sind.

Hierfür verwenden wir die Charakterisierung aus Theorem 1.2 von symmetrischem AC^0 durch die Logik FO + **ARB**, die Charakterisierung von AC^0 durch die arb-invariante FO (arb)-Logik, und ein Problem, dass die Ausdrucksstärke dieser beiden Logiken voneinander trennt.

Theorem 8.1. ***Neil Immerman (1987)****[16]*

Die Klasse AC^0 *ist äquivalent zu der Klasse der durch* inv (FO $\oplus$ **ARB**)*-Formeln definierbaren Anfragen.*

Der verwendete Teil des Beweises (hier nur skizziert) ist die Konstruktion einer Formel für eine beliebige AC^0-Schaltkreisfamilie. Dazu wird jeder Schaltkreis in eine alternierende Normalform der Tiefe d gebracht, in der jedes Gate n^k Vorgänger hat. Die n^{kd} Wege von einem Input zu einem Output werden durch numerische Tupel kodiert (die Relation dieser Wege ist ein numerisches Prädikat und daher in inv (FO $\oplus$ **ARB**)-Logik verwendbar). Die Formel muss dann über jede der alternierenden Ebenen des Schaltkreises quantifizieren (mit $\exists$ für `OR`, und $\forall$ für `AND`), und berechnet so die Auswertung von $\mathcal{C}$.

Da per Definition offensichtlich $SAC^0 \subseteq AC^0$ gilt, können wir mit FO + **ARB** $\subseteq SAC^0$ direkt ablesen, dass FO + **ARB** in inv (FO $\oplus$ **ARB**) enthalten ist (und beweisen somit Teil 1 des Theorems 1.3): Die Logik erster Stufe mit disjunktem **ARB**-Orakel ist verständlicherweise nicht stärker als die mit nicht-disjunktem Orakel.

Für den echten Einschluss (Teil 2 des Theorems 1.3) benötigen wir eine Anfrage, die in inv (FO $\oplus$ **ARB**) beschreibbar ist, jedoch nicht in FO+**ARB** beschreibbar ist. Per Lemma 8.1 ist diese Anfrage dann in AC^0, aber per Theorem 1.2 nicht in SAC^0 beschreibbar.

Lemma 8.2. *Es existiert eine Graph-Anfrage q, die in* inv (FO $\oplus$ **ARB**)*-definierbar ist, aber nicht in* FO + **ARB** *beschreibbar ist.*

Sei $S \subseteq \mathbf{FIN}(\{E\})$ die Klasse der Graphen $\mathfrak{A} = \left(A, E^{\mathfrak{A}}\right)$ für die gilt: A enthält mindestens $\lceil \log |A| \rceil$ viele nicht-isolierte Knoten.

Behauptung 8.3. Es existiert eine $\mathrm{inv}(\mathrm{FO} \oplus \mathbf{ARB})$-Formel, die S definiert.

Literaturverzeichnis

[1] Matthew Anderson and Anuj Dawar. On Symmetric Circuits and Fixed-Point Logics. In Ernst W Mayr and Natacha Portier, editors, *31st International Symposium on Theoretical Aspects of Computer Science (STACS'14)*, volume 25 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 1–22, Dagstuhl, Germany, 2014. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[2] Matthew Anderson, Dieter van Melkebeek, Nicole Schweikardt, and Luc Segoufin. Locality from Circuit Lower Bounds. *SIAM Journal on Computing*, 41(6):1481–1523, 2012.

[3] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009.

[4] Jin Y Cai, Martin Fürer, and Neil Immerman. An optimal lower bound on the number of variables for graph identification. *Combinatorica*, 12(4):389–410, 1992.

[5] Anuj Dawar. A restricted second order logic for finite structures. *Logic and Computational Complexity*, 174:393–413, 1995.

[6] Anuj Dawar and Yuri Gurevich. Fixed Point Logics. *Bulletin of Symbolic Logic*, 8(1):65–88, 2002.

[7] Anuj Dawar, Steven Lindell, and Scott Weinstein. Infinitary Logic and Inductive Definability over Finite Structures. *Information and Computation*, 119(2):160–175, jun 1995.

[8] Anuj Dawar, David Richerby, and Benjamin Rossman. Choiceless Polynomial Time, Counting and the Cai–Fürer–Immerman Graphs. *Electronic Notes in Theoretical Computer Science*, 143(August 2007):13–26, jan 2006.

[9] Stefan Dziembowski. Bounded-Variable Fixpoint Queries are PSPACE-complete. In Dirk van Dalen and Marc Bezem, editors, *In Proc. CSL'96, LNCS 1258*, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pages 89–105, Berlin, Heidelberg, 1996. Springer.

[10] Heinz-Dieter Ebbinghaus and Jörg Flum. *Finite Model Theory*. Number February in Perspectives in Mathematical Logic. Springer Verlag, 1999.

[11] Heinz-Dieter Ebbinghaus, Jörg Flum, and Wolfgang Thomas. *Einführung in die mathematische Logik*. Spektrum Akademischer Verlag, 1996.

[12] Martin Grohe, Stefan Kreutzer, and Nicole Schweikardt. The expressive power of two-variable least fixed-point logics. *Mathematical Foundations of Computer Science 2005, Proceedings*, 3618:422–434, 2005.

[13] Yuri Gurevich and Saharon Shelah. Fixed-Point Extensions of First-Order Logic. *Annals of Pure and Applied Logic*, 32:265–280, 1986.

[14] Neil Immerman. Upper and lower bounds for first order expressibility. *Journal of Computer and System Sciences*, 25(1):76–98, 1982.

[15] Neil Immerman. Relational queries computable in polynomial time. *Information and Control*, 68(1):86–104, 1986.

[16] Neil Immerman. Languages that Capture Complexity Classes. *SIAM Journal on Computing*, 16(4):760–778, 1987.

[17] Neil Immerman. *Descriptive Complexity*, volume 7 of *Texts in Computer Science*. Springer New York, 2012.

[18] Fritz Klein-Barmen. Grundzüge der Theorie der Verbände. *Mathematische Annalen*, 111(1):596–621, 1935.

[19] Phokion G Kolaitis and Moshe Y Vardi. Fixpoint Logic vs. Infinitary Logic in Finite-Model Theory. In *7th Symposium on Logic in Computer Science (LICS'92)*, pages 46–57, 1992.

[20] Phokion G Kolaitis and Moshe Y Vardi. Infinitary logics and 0–1 laws. *Information and Computation*, 98(2):258–294, jun 1992.

[21] Leonid Libkin. Logics with Counting, Auxiliary Relations, and Lower Bounds for Invariant Queries. In *14th Symposium on Logic in Computer Science (LICS'99)*, 1999.

[22] Leonid Libkin. *Elements of Finite Model Theory*. Texts in Theoretical Computer Science. An EATCS Series. Springer Berlin Heidelberg, 2013.

[23] Eugene M Luks. lsomorphism of Graphs of Bounded Valence Can Be Tested in Polynomial Time. *Journal of Computer and System Sciences*, 25(1):42–65, aug 1982.

[24] Johann A Makowsky. Invariant Definability (Extended Abstract). In *Proceedings of the 5th Kurt Gödel Colloquium on Computational Logic and Proof Theory (KGC'97)*, KGC '97, pages 186–202, London, UK, UK, 1997. Springer-Verlag.

[25] Johann A Makowsky. *Invariant definability and P/poly*, chapter Invariant, pages 142–158. Springer Berlin Heidelberg, Berlin, Heidelberg, 1998.

[26] Martin Otto. The logic of explicitly presentation-invariant circuits. In *Computer Science Logic: 10th International Workshop*, volume 1258, pages 369–384, 1997.

[27] Nicole Schweikardt. Arithmetic, First-Order Logic, and Counting Quantifiers. *ACM Transactions on Computational Logic*, 6(3):634–671, 2005.

[28] Nicole Schweikardt. A short tutorial on order-invariant first-order logic. In *8th International Computer Science Symposium in Russia (CSR'13)*, pages 112–126, 2013.

[29] Jouko Väänänen. A Short Course on Finite Model Theory. *Language*, 94(8):1–44, 1999.

[30] Moshe Y Vardi. The Complexity of Relational Query Languages. In *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing (STOC'82)*, STOC '82, pages 137–146, New York, NY, USA, 1982. ACM.

[31] Faried Abu Zaid, Erich Grädel, and Stephan Jaax. Bisimulation Safe Fixed Point Logic. In *Tenth conference on Advances in Modal Logic (AiML'14)*, pages 1–15, 2014.

Erklärung

Gemäß der Ordnung für den Masterstudiengang Informatik, § 24 Abs. 12 bestätige ich hiermit, dass ich die vorliegende Arbeit selbständig ohne fremde Hilfe angefertigt und nur die angegebenen Hilfsmittel verwendet habe.

Frankfurt, den 15. Mai 2016

Christoph Burschka