**Bachelor-Arbeit**

# Die Nutzung von Schaltkreisschranken zum Nachweis von Lokalitätseigenschaften von Logiken

Christoph Burschka
christoph@burschka.de

10. Dezember 2012

Betreuerin: Prof. Dr. Nicole Schweikardt
Goethe-Universität Frankfurt am Main
Wintersemester 2012 / 2013

# Inhaltsverzeichnis

# 1 Einleitung

Eine relationale Anfrage an einen Graphen ist lokal, falls ihr Ergebnis nur von einer eingeschränkten Umgebung der Eingabe abhängt. Bei der Auswertung einer Anfrage mit geringem Lokalitätsradius muss nur ein kleiner Teil des Graphen betrachtet werden. Daher ist die Lokalität einer Anfrage relevant für die Komplexität ihrer Auswertung.

In der Logik ist die Lokalität ein nützliches Werkzeug zur Bestimmung der Ausdruckstärke. Die Existenz einer allgemeinen Schranke für den Lokalitätsradius aller in einem Logiksystem beschreibbaren Anfragen ist ein Resultat von erheblicher Bedeutung: Anfragen können in einer lokalen Logik als nicht ausdrückbar klassifiziert werden, wenn gezeigt wird, dass sie die Schranke nicht einhalten.

Der Lokalitätsbegriff wurde 1982 von Gaifman geprägt. Er wies nach, dass jede Formel der Prädikatenlogik der ersten Stufe (FO) eine Anfrage mit einem konstanten Lokalitätsradius bezüglich der Größe von Strukturen beschreibt [6]. Daraus folgt die Nicht-Ausdrückbarkeit aller Anfragen, die keinen konstanten Lokalitätsradius besitzen, wie zum Beispiel die Erreichbarkeit durch Wege beliebiger Länge.

Grohe und Schwentick wiesen 2000 die gleiche Schranke für die ordnungsinvariante Logik der ersten Stufe nach [7]. Dieses Logiksystem erlaubt die Verwendung eines Ordnungsprädikats in Formeln, wobei die Auswertung der Formel invariant bezüglich der gewählten Ordnung ist. Obwohl das Logiksystem ausdrucksstärker als FO ist, ist es also ebenfalls auf Anfragen mit konstanter Lokalität eingeschränkt.

In dieser Arbeit wird die invariante Logik der ersten Stufe unter Verwendung beliebiger numerischer Prädikate (FO [**arb**]) betrachtet, darunter arithmetische Operationen wie Addition und Multiplikation. Ein neues Lokalitätsergebnis für dieses Logiksystem folgt aus einem Ansatz der deskriptiven Komplexitätstheorie: FO [**arb**] charakterisiert die Komplexitätsklasse $AC^0$ aller Probleme, die durch parallele boolesche Schaltkreise in konstanter Zeit berechnet werden können [9]. Daher kann eine bereits bekannte untere Schranke für die Tiefe und Größe boolescher Schaltkreise genutzt werden, um eine obere Schranke für die Lokalität von FO [**arb**] zu erhalten [2].

## Ergebnisse

In Kapitel 2 werden zunächst Grundbegriffe der Logik, Lokalität und der booleschen Schaltkreise eingeführt, und die verwendeten Notationen und Abkürzungen festgelegt. Unter anderem wird eine Kodierung definiert, die relationale Strukturen als Bitstrings repräsentiert, damit relationale Anfragen als binäre Sprachen modelliert werden können.

Kapitel 3 charakterisiert die Schaltkreisklasse $\mathrm{AC}^0$ durch das Logiksystem $\mathrm{FO}\,[\mathbf{arb}]$. Die Berechenbarkeit einer Graph-Anfrage in $\mathrm{AC}^0$ folgt direkt aus ihrer Ausdrückbarkeit als arb-invariante $\mathrm{FO}\,[\mathbf{arb}]$-Formel [9]. Dies wird bewiesen, indem aus jeder $\mathrm{FO}\,[\mathbf{arb}]$-Formel eine äquivalente Schaltkreisfamilie konstanter Tiefe und polynomieller Größe konstruiert wird. Zusätzlich wird als Teil der Umkehrrichtung gezeigt, dass jede in $\mathrm{AC}^0$ berechenbare binäre Sprache durch einen $\mathrm{FO}\,[\mathbf{arb}]$-Satz beschrieben werden kann.

Für Anfragen in $\mathrm{FO}\,[\mathbf{arb}]$ und $\mathrm{AC}^0$ wird in Kapitel 4 und 5 ein polylogarithmischer Lokalitätsradius nachgewiesen [2]. Eine Reduktion von Parity zeigt nämlich, dass jede einstellige Formel $\varphi$ Gaifman-lokal mit $(\log n)^c$ für ein $c \in \mathbb{N}$ sein muss, um die Verletzung einer unteren Schranke für das Parity-Problem zu vermeiden. Für mehrstellige Formeln wird analog die schwache Gaifman-Lokalität gezeigt.

Die Behandlung der starken Gaifman-Lokalität mehrstelliger Formeln erfolgt durch eine Fallunterscheidung, die in dieser Arbeit zusammengefasst, aber nicht durch einen Beweis formalisiert wird.

Ferner wird erklärt, warum die nachgewiesene Schranke optimal ist: Für jede spezifische polylogarithmische Schranke $(\log n)^c$ existiert eine Formel, die nicht $(\log n)^c$-lokal ist. Die Konstruktion dieser Formel wird informell beschrieben.

In Kapitel 6 wird eine Erweiterung von $\mathrm{FO}\,[\mathbf{arb}]$ um zählende Quantoren betrachtet. Die Schaltkreisklasse $\mathrm{ACC}\,[p]$, die über ein Zählgatter modulo einer Primzahl $p$ verfügt, wird durch das Logiksystem $(\mathrm{FO}{+}\mathrm{MOD}_p)\,[\mathbf{arb}]$ charakterisiert [15, 16].

Diese Charakterisierung wird verwendet, um für einen speziellen Fall, $(\mathrm{FO} + \mathrm{MOD}_p)$-Formeln mit $p > 2$, eine schwache polylogarithmische Gaifman-Lokalität nachzuweisen. Viele allgemeinere Fälle sind noch immer offene Forschungsfragen.

# 2 Grundlagen

## 2.1 Notationen

**Definition 2.1.** Eine relationale **Signatur** sei eine Menge von Prädikaten beliebiger Stelligkeit. Eine **Struktur** über einer Signatur $\sigma$ (eine $\sigma$-Struktur) bestehe aus einer Menge (dem Universum) und einer Interpretation, die jedem Prädikat von $\sigma$ eine Relation auf dem Universum zuordnet [4].

Strukturen werden hier allgemein durch $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \cdots$ bezeichnet. Implizit wird für eine $\sigma$-Struktur $\mathfrak{A}$ das Universum mit $A$, und die Interpretation jedes Prädikats $\dot{R} \in \sigma$ mit $\dot{R}^{\mathfrak{A}}$ bezeichnet. Eine $\{E\}$-Struktur $\mathfrak{A}$ wird auch durch das Tupel $\left(A, E^{\mathfrak{A}}\right)$ abgekürzt.

Im Kontext dieser Arbeit werden nur Strukturen mit endlicher Größe betrachtet.

**Definition 2.2.** Ein **Isomorphismus** $\pi$ von einer $\sigma$-Struktur $\mathfrak{A}$ auf eine $\sigma$-Struktur $\mathfrak{B}$ sei eine Abbildung $\pi : A \to B$, so dass $\pi\left(\dot{R}^{\mathfrak{A}}\right) = \dot{R}^{\mathfrak{B}}$ für alle Prädikate erfüllt sei. Eine solche Abbildung wird auch durch $\pi : \mathfrak{A} \cong \mathfrak{B}$ definiert.

Für zwei Tupel $\bar{a} \in A^k$ und $\bar{b} \in B^k$ gelte $(\mathfrak{A}, \bar{a}) \cong \left(\mathfrak{B}, \bar{b}\right)$, falls ein Isomorphismus $\pi : \mathfrak{A} \cong \mathfrak{B}$ mit $\pi(\bar{a}) = \bar{b}$ existiert.

**Notation.** Ein endlicher Bereich der natürlichen Zahlen wird durch $[\cdot]$ abgekürzt. Für jede natürliche Zahl $n \in \mathbb{N}$ sei $[n] = \{m \in \mathbb{N} \ : \ 1 \leqslant m \leqslant n\} = \{1, \cdots, n\}$.

**Notation.** Ist $\bar{s} \in X^k$ ein Tupel, so sei $\bar{s} = (s_1, \cdots, s_k)$. Für zwei Tupel $\bar{s} \in X^k$ und $\bar{t} \in Y^\ell$ sei $\bar{s} \cdot \bar{t} \in (X \cup Y)^{k+\ell}$ das Tupel $(s_1, \cdots, s_k, t_1, \cdots, t_\ell)$. Für $\bar{s} \in X^k$ und $y \in Y$ bezeichnen $\bar{s} \cdot y$ und $y \cdot \bar{s}$ respektive die Tupel $(s_1, \cdots, s_k, y)$ und $(y, s_1, \cdots, s_k)$.

**Definition 2.3.** Eine **Aufzählung** einer endlichen Menge $X$ sei eine Bijektion $f : X \to [|X|]$. Die zu $f$ passende **Ordnung** $\dot{\leqslant}_f \subseteq X^2$ sei wie folgt:

$$\dot{\leqslant}_f := \left\{(x, y) \in X^2 \ : \ f(x) \leqslant f(y)\right\}$$

Umgekehrt sei für jede lineare Ordnung $\dot{\leqslant} \subseteq X^2$ die zu $\dot{\leqslant}$ passende Aufzählung $f_{\dot{\leqslant}} : X \to [|X|]$ wie folgt:

$$f_{\dot{\leqslant}}(x) := \left|\left\{y \in X \ : \ y \dot{\leqslant} x\right\}\right|$$

**Definition 2.4.** Für eine Signatur $\sigma$ mit einem Ordnungsprädikat $\dot{\leqslant}$ sei eine $\sigma$-Struktur $\mathfrak{A}$ **geordnet**, falls $\dot{\leqslant}^{\mathfrak{A}}$ eine lineare Ordnung auf der Struktur $\mathfrak{A}$ ist.

**Notation.** Ein Wort $\bar{w} = w_1 \cdots w_n \in \{0,1\}^n$ für $n \in \mathbb{N}$ wird als **Bitstring** bezeichnet. Durch $|\bar{w}|_1 \in \mathbb{N}$ wird die Anzahl der Einsen $\sum_{i=1}^{n} w_i$ abgekürzt.

**Definition 2.5.** Für jede Funktion $f : \mathbb{N} \to \mathbb{N}$ bezeichnen $\mathcal{O}(f)$ und $\Omega(f)$ die Klassen aller Funktionen, deren asymptotisches Wachstum jeweils von oben oder von unten durch $f$ beschränkt sind. Für $f, g : \mathbb{N} \to \mathbb{N}$ bezeichnen $f(\mathcal{O}(g))$ und $f(\Omega(g))$ die Klassen $\bigcup_{g' \in \mathcal{O}(g)} \mathcal{O}(f(g'))$ und $\bigcup_{g' \in \Omega(g)} \Omega(f(g'))$.

## 2.2 Graphen

**Definition 2.6.** Sei GRAPH eine Signatur mit einem zweistelligen Relationssymbol $E$. Ein gerichteter **Graph** $\mathfrak{A}$ sei eine GRAPH-Struktur $\left(V, E^{\mathfrak{A}}\right)$, wobei $V$ die Knotenmenge und $E^{\mathfrak{A}}$ die Kantenrelation des Graphen sind.

**Definition 2.7.** Eine $k$-stellige **Graph-Anfrage** $q$ sei die Zuordnung einer Relation $q(\mathfrak{A}) \subseteq A^k$ zu jedem Graphen $\mathfrak{A}$, die unter Isomorphismen abgeschlossen ist: Es gelte $\pi(q(\mathfrak{A})) = q(\pi(\mathfrak{A}))$ für jeden Isomorphismus $\pi$ auf $\mathfrak{A}$.

**Definition 2.8.** Der **Gaifman-Graph** $\mathcal{G}(\mathfrak{A})$ eines gerichteten Graphen $\mathfrak{A} = \left(V, E^{\mathfrak{A}}\right)$ sei ein ungerichteter Graph, in dem zwei Knoten $x, y \in V$ genau dann durch eine ungerichtete Kante $\{x, y\}$ verbunden sind, falls $(x, y) \in E^{\mathfrak{A}}$ oder $(y, x) \in E^{\mathfrak{A}}$.

Die **Distanzfunktion** $\operatorname{dist} : V \times V \to \mathbb{N}$ sei eine partielle Funktion, die jedem durch Wege verbundenen Knotenpaar $x, y \in V$ die Länge des kürzesten Weges zwischen $x$ und $y$ im Gaifman-Graph zuordnet. Die Funktion wird auf $\operatorname{dist} : V^* \times V \to \mathbb{N}$ erweitert, wobei $\operatorname{dist}(\bar{x}, y) := \min\{\operatorname{dist}(x_i, y) \ : \ 1 \leqslant i \leqslant |\bar{x}|\}$ sei.

Für jeden Radius $r \in \mathbb{N}$, jeden Knoten $x \in V$ und jedes Tupel $\bar{x} \in V^*$ wird festgelegt:

- Die $r$-**Kugel** von $x$ oder $\bar{x}$ in $\mathfrak{A}$ sei die Menge aller Knoten, die höchstens die Distanz $r$ von $x$ oder $\bar{x}$ haben.

$$N_r^{\mathfrak{A}}(x) = \{y \in V \ : \ \operatorname{dist}(x, y) \leqslant r\}$$

- Die $r$-**Schale** von $x$ oder $\bar{x}$ in $\mathfrak{A}$ sei die Menge der Knoten, die genau die Distanz $r$ von $x$ oder $\bar{x}$ haben.

$$S_r^{\mathfrak{A}}(x) = \{y \in V \ : \ \operatorname{dist}(\bar{x}, y) = r\} = N_r^{\mathfrak{A}}(x) \setminus N_{r-1}^{\mathfrak{A}}(x)$$

- Die $r$-**Umgebung** von $x$ oder $\bar{x}$ in $\mathfrak{A}$ sei der durch die $r$-Kugel von $x$ oder $\bar{x}$ induzierte Teilgraph von $\mathfrak{A}$.

$$\mathcal{N}_r^{\mathfrak{A}}(x) \quad = \quad \mathfrak{A}_{|N_r^{\mathfrak{A}}(x)}$$

**Definition 2.9.** Eine k-stellige Graph-Anfrage $q$ sei auf einem Graphen $\mathfrak{A}$ **(stark) Gaifman-lokal** mit Radius $r \in \mathbb{N}$, oder (**stark**) **$r$-lokal**, falls für alle Tupel $\bar{a}, \bar{b} \in A^k$ mit $\left(\mathcal{N}_r^{\mathfrak{A}}(\bar{a}), \bar{a}\right) \cong \left(\mathcal{N}_r^{\mathfrak{A}}\left(\bar{b}\right), \bar{b}\right)$ gilt:

$$\bar{a} \in q(\mathfrak{A}) \Longleftrightarrow \bar{b} \in q(\mathfrak{A})$$

Eine $k$-stellige Anfrage $q$ ist $f$-lokal (für $f : \mathbb{N} \to \mathbb{N}$), falls eine Schranke $n_0 \in \mathbb{N}$ existiert, so dass sie auf allen Graphen $\mathfrak{A}$ der Größe $n \geqslant n_0$ Gaifman-lokal mit Radius $f(n)$ ist. Ist $\mathcal{F} \subseteq \operatorname{Abb}(\mathbb{N}, \mathbb{N})$ eine Klasse von Funktionen, so ist die Anfrage $\mathcal{F}$-lokal, falls sie $f$-lokal für eine beliebige Funktion $f \in \mathcal{F}$ ist[1] [11, 2].

**Definition 2.10.** Eine $k$-stellige Graph-Anfrage $q$ sei auf einem gerichteten Graphen $\mathfrak{A}$ **schwach Gaifman-lokal** mit Radius $r \in \mathbb{N}$, oder **schwach $r$-lokal**, falls für alle Tupel $\bar{a}, \bar{b} \in A^k$ mit $\left(\mathcal{N}_r^{\mathfrak{A}}(\bar{a}), \bar{a}\right) \cong \left(\mathcal{N}_r^{\mathfrak{A}}\left(\bar{b}\right), \bar{b}\right)$ und $\mathcal{N}_r^{\mathfrak{A}}(\bar{a}) \cap \mathcal{N}_r^{\mathfrak{A}}\left(\bar{b}\right) = \emptyset$ gilt:

$$\bar{a} \in q(\mathfrak{A}) \Longleftrightarrow \bar{b} \in q(\mathfrak{A})$$

Die schwache $f$-Lokalität und $\mathcal{F}$-Lokalität seien analog definiert.

## 2.3 Logik

**Definition 2.11.** Die Syntax und Semantik der Logik der ersten Stufe (FO) entspreche der allgemeinen Definition [4].

Zur besseren Lesbarkeit wird das Ordnungsprädikat $\dot{\leqslant}$ mit Infixnotation verwendet, so dass die atomare Formel "$x \dot{\leqslant} y$" für "$\dot{\leqslant}(x, y)$" stehe.

**Definition 2.12.** Die relationale Signatur $\sigma_{arb}$ sei wie folgt definiert:

$$\sigma_{arb} = \left\{ \dot{R} \ : \ R \subseteq \mathbb{N}^k, \ k \in \mathbb{N} \right\}$$

Für jede Stelligkeit $k \in \mathbb{N}_{>0}$ und jede Relation $R \subseteq \mathbb{N}^k$ ist $\dot{R} \in \sigma_{arb}$ ein Prädikat, das eindeutig $R$ zugeordnet sei. (Dazu gehört insbesondere die lineare Ordnung auf den natürlichen Zahlen.)

**Definition 2.13.** Alle FO $[\textsc{Graph} \cup \sigma_{arb}]$-Formeln bilden die Logik erster Stufe mit Arb-Erweiterung über GRAPH. Von nun an werde **arb** als Abkürzung für $\textsc{Graph} \cup \sigma_{arb}$ verwendet.

**Notation.** Für jede $k$-stellige Formel $\varphi$ wird eine feste Folge von freien Variablen $\bar{x} \in \mathbf{var}^k$ vorgegeben (kurz $\varphi(\bar{x})$). Für jeden Graphen $\mathfrak{A}$ und jedes Tupel $\bar{t} \in A^k$ bezeichne $[\![\varphi(\bar{t})]\!]^{\mathfrak{A}}$ die Auswertung von $\varphi$ auf $\mathfrak{A}$ mit der Belegung $\beta : \bar{x} \mapsto \bar{t}$ (auch als die Belegung "$\bar{t}$" abzukürzen). Außerdem gelte $\mathfrak{A} \models \varphi(\bar{t})$ genau dann wenn $[\![\varphi(\bar{t})]\!]^{\mathfrak{A}} = 1$.

[1] Insbesondere wird so die Lokalität durch asymptotische Klassen wie $\mathcal{O}(\log n^c)$ oder $\mathcal{O}(1)$ klassifiziert.

**Definition 2.14.** Für jeden Graphen $\mathfrak{A}$ mit endlicher Größe $n$, und jede Aufzählung $f : A \to [n]$ sei die **Ordnungs-Erweiterung** $\mathfrak{A}_f$ eine geordnete **arb**-Struktur, wobei $\dot{S}^{\mathfrak{A}_f} := f^{-1}\left(S \cap [n]^k\right)$ für alle Relationen $S \subseteq \mathbb{N}^k$ der Stelligkeit $k$ sei.

Jede *geordnete* $\sigma$-Struktur $\mathfrak{A}$ sei implizit ihre eigene Ordnungs-Erweiterung $\mathfrak{A}_f$, wobei $f$ die zu $\dot{\leqslant}^{\mathfrak{A}}$ passende Aufzählung von $A$ sei.

**Definition 2.15.** Eine FO [**arb**]-Formel $\varphi$, die in allen Ordnungs-Erweiterungen eines Graphen $\mathfrak{A}$ von den gleichen Belegungen erfüllt wird, heiße **arb-invariant** bezüglich $\mathfrak{A}$. Eine Formel, die bezüglich allen endlichen Graphen arb-invariant ist, heiße arb-invariant. Die Auswertung einer arb-invarianten Formel $\varphi$ über einer beliebigen Ordnungs-Erweiterung $\mathfrak{A}_f$ von $\mathfrak{A}$ werde im folgenden durch $[\![\varphi]\!]^{\mathfrak{A}}$ abgekürzt.

**Beispiel.** Die folgende arb-invariante FO $\left[\dot{\leqslant}, \dot{\times}\right]$-Formel drückt aus, dass die Anzahl der Knoten eines Graphen eine Primzahl ist:

$$\exists x_n \left(\forall x\ x \dot{\leqslant} x_n \wedge \exists x_1\ \neg x_1 = x_n \wedge \forall y_a \forall y_b \left(\dot{\times}\left(y_a, y_b, x_n\right) \to \left(y_a = y_n \vee y_b = x_n\right)\right)\right)$$

Die folgende nicht arb-invariante FO $\left[\dot{\leqslant}\right]$-Formel drückt aus, dass der bezüglich der Ordnung minimale Knoten eine ausgehende Kante hat.

$$\exists x_1 \left(\forall x\ x_1 \dot{\leqslant} x \wedge \exists y\ E\left(x_1, y\right)\right)$$

**Definition 2.16.** Für jede FO [**arb**]-Formel sei $\|\varphi\| \in \mathbb{N}$ die Anzahl der Symbole, aus denen die Formel besteht.

**Definition 2.17.** Die Alternierungstiefe $T\left(\varphi\right) = \max\left\{T_\exists\left(\varphi\right), T_\forall\left(\varphi\right)\right\}$ einer Formel in Pränexnormalform sei die Anzahl der alternierenden geschachtelten Quantoren. Es gelte:

- Für alle quantorenfreien Formeln sei $T_\exists\left(\varphi\right) = T_\forall\left(\varphi\right) = 0$.
- Es sei $T_\exists\left(\exists x \varphi\right) = T_\exists\left(\varphi\right)$ und $T_\forall\left(\exists x \varphi\right) = 1 + T_\exists\left(\varphi\right)$.
- Es sei $T_\exists\left(\forall x \varphi\right) = 1 + T_\forall\left(\varphi\right)$ und $T_\forall\left(\forall x \varphi\right) = T_\forall\left(\varphi\right)$.

**Definition 2.18.** Sei $p \in \mathbb{N}$ eine Primzahl. Es wird für $0 \leqslant i < p$ ein zusätzlicher Quantor $\exists^{(p,i)}$ eingeführt und die Logik $(\mathrm{FO} + \mathrm{MOD}_p)$ definiert, die zusätzlich zu der Syntax von FO eine neue Regel enthält:

- Ist $\varphi$ eine $(\mathrm{FO} + \mathrm{MOD}_p)$-Formel, $x \in$ **var** eine Variable und $0 \leqslant i < p$, so sei $\exists^{(p,i)} x\ \varphi$ eine $(\mathrm{FO} + \mathrm{MOD}_p)$-Formel.

Die Semantik von $(\mathrm{FO} + \mathrm{MOD}_p)$ sei die folgende Erweiterung der Semantik von FO:

- Ist eine $(\mathrm{FO} + \mathrm{MOD}_p)$-Formel $\varphi(\bar{x})$ von der Form $\exists^{(p,i)} y\ \psi(\bar{x})$ mit $\bar{x} \in \mathbf{var}^k$, $\mathfrak{A}$ eine $\sigma$-Struktur, und $\beta : \{x_1, \cdots, x_k, y\} \to A$ eine Belegung, so gelte:

$$\mathfrak{A} \models \varphi(\bar{a}) \quad \Leftrightarrow \quad \left| \left\{ b \in A \ : \ \mathfrak{A} \models \psi \frac{b, \ \bar{a}}{y, \ \bar{x}} \right\} \right| \equiv i \mod p$$

## 2.4 Schaltkreise

**Definition 2.19.** Ein **Schaltkreis** $\mathcal{C}_n = (G, f, x)$ mit der Eingabelänge $n$ besteht aus einem azyklischen Graphen $G = \left(V, E^G\right)$ mit genau einer Senke $x \in V$ und einer Knotenmarkierung $f : V \to \left\{\wedge, \vee, \mathbf{0}, \mathbf{1}, I_i, \overline{I_i} \ : \ i \in [n]\right\}$. Alle mit $f(v) \in \{\wedge, \vee\}$ beschrifteten Knoten haben in dieser Definition einen unbeschränkten Eingangsgrad. Die übrigen Knoten sind Quellen und haben keine eingehenden Kanten.

Eine **Schaltkreisfamilie** oder Schaltkreissequenz $(\mathcal{C}_i)_{i \in \mathbb{N}}$ sei eine Folge von Schaltkreisen $\mathcal{C}_i$ mit Eingabelänge $i \in \mathbb{N}$.

**Notation.** Die Knoten eines Schaltkreises werden im folgenden als „Gatter“ bezeichnet. Als „innere Gatter“ werden alle Gatter mit Vorgängern bezeichnet.

Mit der Notation „$v \in \mathcal{C}_n$“ wird abgekürzt, dass $v \in V$ ein Gatter im Schaltkreis $\mathcal{C}_n = (G, f, x)$ mit $G = \left(V, E^G\right)$ sei. Mit $x = \mathrm{Out}(\mathcal{C}_n)$ wird abgekürzt, dass $x \in \mathcal{C}_n$ die Senke (*Output*) des Schaltkreises $\mathcal{C}_n = (G, f, x)$ sei.

Die Kantenrelation $E^G$ des Schaltkreises $\mathcal{C}_n = (G, f, x)$ wird auch als $E^{\mathcal{C}_n}$ abgekürzt.

Für jedes Gatter $v \in \mathcal{C}_n$ sei $\mathrm{In}(\mathcal{C}_n, v) = \left\{u \in \mathcal{C}_n \ : \ (u, v) \in E^{\mathcal{C}_n}\right\}$ die Menge der direkten Vorgänger von $v$, und $\mathrm{Pre}(\mathcal{C}_n, v)$ die Menge der Knoten, von denen aus $v$ über einen Weg beliebiger Länge erreichbar ist.

Für $\mathcal{C}_n = (G, f, x)$ und $v \in \mathcal{C}_n$ bezeichne $\mathcal{C}_{n,v}$ den Teilschaltkreis, dessen Ausgang $v$ ist. Daher ist $\mathcal{C}_n$ gleichbedeutend mit $\mathcal{C}_{n,\mathrm{Out}(\mathcal{C}_n)}$.

$$\mathcal{C}_{n,v} := \left(G_{|\mathrm{Pre}(\mathcal{C}_n,v)}, f, v\right)$$

**Definition 2.20.** Die Auswertung $[\![\mathcal{C}_n]\!]^w$ eines Schaltkreises $\mathcal{C}_n$ über einem Ein-

gabewort $w \in \{0,1\}^n$ sei rekursiv wie folgt definiert:

$$\begin{aligned}
[\![\mathcal{C}_n]\!]^w &:= \left[\!\!\left[\mathcal{C}_{n,\mathrm{Out}(\mathcal{C}_n)}\right]\!\!\right]^w \\
[\![\mathcal{C}_{n,v}]\!]^w &:= \begin{cases}
0 & \text{falls } f(v) = \mathbf{0} \\
1 & \text{falls } f(v) = \mathbf{1} \\
w_i & \text{falls } f(v) = I_i \\
\neg w_i & \text{falls } f(v) = \overline{I_i} \\
\bigwedge_{u \in \mathrm{In}(\mathcal{C}_n,v)} [\![\mathcal{C}_{n,u}]\!]^w & \text{falls } f(v) = \wedge \\
\bigvee_{u \in \mathrm{In}(\mathcal{C}_n,v)} [\![\mathcal{C}_{n,u}]\!]^w & \text{falls } f(v) = \vee
\end{cases}
\end{aligned}$$

Eine Schaltkreisfamilie $(\mathcal{C}_i)_{i\in\mathbb{N}}$ berechnet eine boolesche Funktion $\mathcal{C} : \{0,1\}^* \to \{0,1\}$ mit $\mathcal{C}(w) = \left[\!\!\left[\mathcal{C}_{|w|}\right]\!\!\right]^w$ für $w \in \{0,1\}^*$.

**Notation.** Die Aussage "$w \models \mathcal{C}_n$" sei gleichbedeutend mit $[\![\mathcal{C}_n]\!]^w = 1$.

**Definition 2.21.** Die **Tiefe** eines Schaltkreises $T(\mathcal{C}_n)$ sei die Länge des längsten Wegs von einer Quelle zur Senke. Die Größe eines Schaltkreises $|\mathcal{C}_n|$ sei die Anzahl seiner Gatter. Eine Schaltkreisfamilie hat die Tiefe $f : \mathbb{N} \to \mathbb{N}$ und Größe $g : \mathbb{N} \to \mathbb{N}$, wenn sie $T(\mathcal{C}_n) \leqslant f(n)$ und $|\mathcal{C}_n| \leqslant g(n)$ für alle $n \in \mathbb{N}$ einhält.

Die Tiefe eines Gatters $v \in \mathcal{C}_n$ sei die Tiefe $T(\mathcal{C}_{n,v})$.

**Beispiel.** Der folgende Schaltkreis berechnet die Parity-Funktion $\textsc{Parity} : \{0,1\}^2 \to \{0,1\}$ mit $\textsc{Parity}(ab) = \begin{cases} 1 & a = b \\ 0 & a \neq b \end{cases}$.

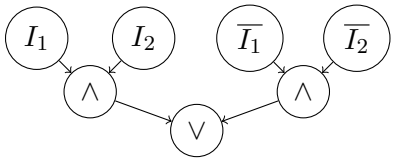


Abbildung 2.1: Schaltkreis $\mathcal{C}_2$.

**Notation.** Ist der Schaltkreis $\mathcal{C}_n$ ein Baum, so kann er eindeutig durch eine aussagenlogische Formel in Negationsnormalform über den Variablen $w_1, \cdots, w_n$ beschrieben werden. Dabei steht ein atomarer Ausdruck „0“, „1“, „$w_i$“ oder „$\neg w_i$“ für einen jeweils mit „$\mathbf{0}$“, „$\mathbf{1}$“, „$I_i$“ oder „$\bar{I}_i$“ markierten Knoten. Die Operatoren für Disjunktion und Konjunktion stehen für entsprechende Gatter, deren Vorgänger jeweils die durch die Operanden definierten Schaltkreise sind.

Da die Herstellung der Negationsnormalform eine triviale Umformung ist, werden auch allgemeine aussagenlogische Formeln zur Notation verwendet.

**Beispiel.** Die allgemeine Parity-Funktion $\textsc{Parity} : \{0,1\}^* \to \{0,1\}$, wobei $\textsc{Parity}\,(w_1 \cdots w_n) = 1$ genau dann wenn $|w|_1$ gerade ist, kann durch eine Schaltkreissequenz der folgenden Form berechnet werden:

$$\begin{aligned}
\mathcal{C}_1 &:= \neg w_1 \\
\mathcal{C}_2 &:= (w_1 \wedge w_2) \vee (\neg w_1 \wedge \neg w_2) \\
\mathcal{C}_n &:= \left(\mathcal{C}_{\lfloor \frac{n}{2} \rfloor}\left(w_1 \cdots w_{\lfloor \frac{n}{2} \rfloor}\right) \wedge \mathcal{C}_{\lceil \frac{n}{2} \rceil}\left(w_{\lfloor \frac{n}{2} \rfloor + 1} \cdots w_n\right)\right) \vee \\
&\quad \left(\neg\mathcal{C}_{\lfloor \frac{n}{2} \rfloor}\left(w_1 \cdots w_{\lfloor \frac{n}{2} \rfloor}\right) \wedge \neg\mathcal{C}_{\lceil \frac{n}{2} \rceil}\left(w_{\lfloor \frac{n}{2} \rfloor + 1} \cdots w_n\right)\right)
\end{aligned}$$

Diese Schaltkreissequenz hat die Tiefe $\Theta(\log n)$ und Größe $\Theta(n)$.

**Definition 2.22.** Sei $p \in \mathbb{N}$ eine natürliche Zahl. Ein $\oplus^p$-Schaltkreis $\mathcal{C}_n = (G, f, x)$ (ein Schaltkreis mit "$p$-Zählgatter") sei analog zu einem gewöhnlichen Schaltkreis definiert, wobei die Markierung wie folgt erweitert wird:

$$f : V \to \left\{\mathbf{0}, \mathbf{1}, I_i, \overline{I_i}, \wedge, \vee, \oplus^p \;:\; i \in [n]\right\}$$

Für ein Gatter $v \in \mathcal{C}_n$ mit $f(v) = \oplus^p$ sei die Auswertung wie folgt:

$$[\![\mathcal{C}_{n,v}]\!]^w = \begin{cases} 1 & \text{falls } \sum_{u \in \mathrm{In}(\mathcal{C}_n, v)} [\![\mathcal{C}_{n,u}]\!]^w \equiv 0 \mod p \\ 0 & \text{sonst} \end{cases}$$

Das $p$-Zählgatter prüft also, ob die Anzahl der aktiven Eingänge ein Vielfaches von $p$ ist.

Schaltkreisfamilien, Tiefe und Größe seien analog zu den gewöhnlichen Schaltkreisen definiert.

**Notation.** Das $p$-Zählgatter wird in der aussagenlogischen Formel durch einen zusätzlichen Junktor $\oplus^p$ repräsentiert.

**Beispiel.** Eine triviale $\oplus^2$-Schaltkreisfamilie mit der Tiefe 1 kann das Parity-Problem lösen:

$$\mathcal{C}_n = \bigoplus_{i \in [n]}^{2} w_i$$

**Definition 2.23.** Die Klasse $\mathrm{ACC}^0[p]$ enthalte alle Probleme, die von einer $\oplus^p$-Schaltkreissequenz mit konstanter Tiefe und polynomieller Größe berechnet werden können [15].

## 2.5 Binäre Kodierung von Graphen

Die Schaltkreisklasse $\mathrm{AC}^0$ soll logisch charakterisiert werden. Logische Formeln werden über Graphen ausgewertet, und Schaltkreise über binären Worten. Um

diese Begriffe in Bezug zu bringen, wird eine Kodierung eingeführt, die eine beliebige GRAPH-Struktur sowie ein Tupel von Knoten als Bitstring aus $\{0,1\}^*$ ausdrückt.

Die geforderten Eigenschaften dieser Kodierung sind wie folgt:

1. Für zwei Graphen $\mathfrak{A}, \mathfrak{B}$ und Tupel $\bar{a} \in A^k, \bar{b} \in B^k$ können $(\mathfrak{A}, \bar{a})$ und $\left(\mathfrak{B}, \bar{b}\right)$ genau dann durch dieselben Worte repräsentiert werden, wenn $(\mathfrak{A}, \bar{a}) \cong \left(\mathfrak{B}, \bar{b}\right)$. Alle Repräsentationen eines Graphen bilden damit eine Äquivalenzklasse.
2. Alle Repräsentationen eines Graphen der Länge $n$ und Tupels der Länge $k$ haben die Länge $g_k(n)$, wobei $g_k : \mathbb{N} \to \mathbb{N}$ eine injektive und in $n$ höchstens polynomiell wachsende Funktion ist.

**Definition 2.24.** Sei $\mathfrak{A}$ ein Graph der Größe $n \in \mathbb{N}$, sei $\bar{a} \in A^k$ ein Tupel der Länge $k \in \mathbb{N}$ und sei $f : A \to [n]$ eine beliebig gewählte Aufzählung der Knoten von $\mathfrak{A}$. So sei $\mathrm{enc}_f(\mathfrak{A}, \bar{a}) \in \{0,1\}^*$ wie folgt definiert:

$$\begin{aligned}
\mathrm{enc}_f(\mathfrak{A}, \bar{a}) &:= v_1 \cdots v_{n^2} w_1 \cdots w_{kn} \\
v_i &:= \begin{cases} 1 & \text{falls } i = n \cdot (f(u) - 1) + f(v),\ (u,v) \in E^{\mathfrak{A}} \\ 0 & \text{sonst} \end{cases} \\
w_i &:= \begin{cases} 1 & \text{falls } i = n \cdot (j-1) + f(a_j) \\ 0 & \text{sonst} \end{cases}
\end{aligned}$$

Die geforderten Eigenschaften sind erfüllt:

1. Seien $\mathfrak{A}$ und $\mathfrak{B}$ zwei Graphen der Größe $n \in \mathbb{N}$, $\pi : \mathfrak{A} \cong \mathfrak{B}$ ein Isomorphismus, $\bar{a} \in A^k$ ein Tupel und $f : A \to [n]$ eine beliebige Aufzählung der Knoten von $\mathfrak{A}$. Dann existiert eine Aufzählung $f' : B \to [n]$, so dass $\mathrm{enc}_f(\mathfrak{A}, \bar{a}) = \mathrm{enc}_{f'}(\mathfrak{B}, \pi(\bar{a}))$ gilt:

$$\begin{aligned}
f' &:= f \circ \pi^{-1} \\
\mathrm{enc}_f(\mathfrak{A}, \bar{a}) &= v_1 \cdots v_{n^2} w_1 \cdots w_{kn} \\
\mathrm{enc}_{f'}(\mathfrak{B}, \pi(\bar{a})) &= v'_1 \cdots v'_{n^2} w'_1 \cdots w'_{kn}
\end{aligned}$$

$$\begin{aligned}
& v_{(i-1)n+j} = 1 \\
\iff\ & f^{-1}(i,j) \in E^{\mathfrak{A}} \\
\iff\ & \pi \circ f^{-1}(i,j) \in E^{\mathfrak{B}} \\
\iff\ & f' \circ f \circ \pi^{-1} \circ \pi \circ f^{-1}(i,j) \in E^{\mathfrak{B}} \\
\iff\ & f'(i,j) \in E^{\mathfrak{B}} \\
\iff\ & v'_{(i-1)n+j} = 1
\end{aligned}$$

   Umgekehrt folgt aus $\mathrm{enc}_f(\mathfrak{A}, \bar{a}) = \mathrm{enc}_g\left(\mathfrak{B}, \bar{b}\right)$, dass $\pi := f^{-1} \circ g$ ein Isomorphismus von $\mathfrak{A}$ zu $\mathfrak{B}$ mit $\pi(\bar{a}) = \bar{b}$ ist.

2. Sei $\mathfrak{A}$ ein Graph der Größe $n \in \mathbb{N}$, und $\vec{a} \in A^k$ ein Tupel. Jede Kodierung hat die Form $\mathrm{enc}_f(\mathfrak{A}, \vec{a}) = v_1 \cdots v_{n^2} w_1 \cdots w_{kn}$, so dass $|\mathrm{enc}_f(\mathfrak{A}, \vec{a})| = n^2 + kn$ ist. Damit ist $g_k(n) = n^2 + kn$ eine injektive und in $n$ polynomiell wachsende Funktion.

**Notation.** Falls die Wahl von $f$ unbedeutend ist, bezeichnet $\mathrm{enc}(\mathfrak{A}, \vec{a})$ eine Kodierung mit beliebiger Aufzählung.

## 2.6 Logische Repräsentation von Bitstrings

Um eine binäre Sprache in einer relationalen Logik zu beschreiben, muss eine Interpretation von Bitstrings als relationale Struktur definiert werden.

**Definition 2.25.** Sei $\sigma_B = \left\{P_1, \dot{\leqslant}\right\}$ eine Signatur mit einem monadischen Prädikat $P_1$ und einem zweistelligen Ordnungsprädikat $\dot{\leqslant}$. Für jedes binäre Wort $w \in \{0,1\}^*$ von beliebiger Länge $|w| = n \in \mathbb{N}$ sei $\mathfrak{B}_w$ eine geordnete $\sigma_B$-Struktur über $B = [n]$ mit $P_1^{\mathfrak{B}_w} = \{i \in [n] \ : \ w_i = 1\}$ und $\dot{\leqslant}^{\mathfrak{B}_w} = \left\{(i,j) \in [n]^2 \ : \ i \leqslant j\right\}$.

# 3 Logische Charakterisierung von $\mathsf{AC}^0$

## 3.1 Formel zu Schaltkreissequenz

Das folgende Theorem wird bewiesen.

**Theorem 3.1** (nach Neil Immerman 1983 [9, 10])**.** *Charakterisierung von FO* [**arb**] *durch* $AC^0$*:*

1. *Sei* $\varphi(\bar{x})$ *eine* $k$*-stellige FO* [**arb**]*-Formel (o.B.d.A. in Pränexnormalform) mit Alternierungstiefe* $d \in \mathbb{N}$*. Dann existiert eine Schaltkreisfamilie* $(\mathcal{C}_{n^2+kn})_{n\in\mathbb{N}}$ *mit konstanter Tiefe* $d+4$ *und der Größe* $n^{\|\varphi\|}$*, so dass für jeden Graphen* $\mathfrak{A}$ *der Größe* $n$*, jede Belegung* $\bar{a} \in A^k$ *von* $\varphi$ *und jede Ordnungs-Erweiterung* $\mathfrak{A}_f$ *gilt:*

$$[\![\varphi(\bar{a})]\!]^{\mathfrak{A}_f} = [\![\mathcal{C}_{n^2+kn}]\!]^{enc_f(\mathfrak{A},\bar{a})}$$

*Insbesondere wird die Auswertung einer arb-invariante Formel* $\varphi$ *über jeder Struktur* $\mathfrak{A}$ *der Länge* $n$ *unabhängig von der gewählten Aufzählung* $f$ *korrekt durch* $\mathcal{C}_{n^2+kn}$ *berechnet.*

Nach Definition der Kodierung ist die Länge $f_k(n) = |\mathrm{enc}_f(\mathfrak{A}, \bar{a})| = n^2 + n$ einer Struktur der Größe $n$ mit einem Tupel der Länge $k$ eine injektive Funktion über $n$. Daher kann der erste Teil des Satzes bewiesen werden, indem für $n \in \mathbb{N}$ ein Schaltkreis $\mathcal{C}_{n^2+kn}$ konstanter Tiefe und polynomieller Größe konstruiert wird, der für jede Struktur $\mathfrak{A}$ der Größe $n$ und jedes Tupel $\bar{a} \in A^k$ bei Eingabe von $\mathrm{enc}_f(\mathfrak{A}, \bar{a})$ die Auswertung $[\![\varphi(\bar{a})]\!]^{\mathfrak{A}_f}$ berechnet.

### 3.1.1 Normalform

Zunächst sei $\varphi(\bar{x})$ ohne Beschränkung der Allgemeinheit in disjunktiver Pränexnormalform:

$$\begin{aligned} \varphi(\bar{x}) &= Q_1 y_1 \cdots Q_\ell y_\ell \psi \\ Q_1, \cdots, Q_\ell &\in \{\exists, \forall\} \\ \psi &= \bigvee_{i=1}^{m} \bigwedge_{j=1}^{m_i} \psi_{i,j} \end{aligned}$$

Dabei seien $\psi_{i,j}$ atomare Formeln von der Form $\dot{R}(\bar{z})$ oder $\neg\dot{R}(\bar{z})$ für eine beliebige Relation $R \subseteq \mathbb{N}^k$ beliebiger Stelligkeit $s \in \mathbb{N}$, von der Form $E(z_1, z_2)$ oder $\neg E(z_1, z_2)$, oder $z_1 = z_2$ oder $\neg z_1 = z_2$. Es gelte in jedem Fall $\bar{z} \in \{x_1, \cdots, x_k, y_1, \cdots, y_\ell\}^s$.

### 3.1.2 Rekursionsanfang

Die in $\varphi$ verwendeten Prädikate $\dot{R} \in \sigma_{arb}$ sind unabhängig der Struktur fest definiert. Daher ist jedes Atom der Form $\dot{R}(\bar{z})$ unter einer bestimmten Belegung $\beta : \bar{x} \cdot \bar{y} \mapsto \bar{t}$ mit $\bar{t} \in [n]^{k+\ell}$ grundsätzlich erfüllt oder nicht erfüllt. Zusätzlich ist jedes Atom der Form $z_1 = z_2$ genau dann erfüllt, wenn $\beta(z_1) = \beta(z_2)$. Die Atome der Form $E(z_1, z_2)$ sind für $\mathfrak{A}_f$ genau dann erfüllt, wenn $\beta(z_1, z_2) \in E^{\mathfrak{A}}$, beziehungsweise wenn

$$\mathrm{enc}_f(\mathfrak{A})_{n\cdot(f\circ\beta(z_1)-1)+f\circ\beta(z_2)} = 1$$

Daher wird für jedes Tupel $\bar{t} \in [n]^{k+\ell}$ der Schaltkreis $\mathcal{D}_\psi^{\bar{t}}$ der Tiefe 2 konstruiert, der die Auswertung der Formel $\psi$ unter der Belegung $\beta := (x_1, \cdots, x_k, y_1, \cdots, y_\ell) \mapsto f^{-1}(\bar{t})$ berechnet.

$$\mathcal{D}_\psi^{i_1,\cdots,i_\ell} := \bigvee_{i=1}^{m} \bigwedge_{j=1}^{m_i} x_{i,j}$$

$$x_{i,j} := \begin{cases} 0 & \psi_{i,j} \hat{=} \dot{R}(\bar{v}),\ \gamma(\bar{v}) \notin R \\ & \text{oder } \psi_{i,j} \hat{=} \neg\dot{R}(\bar{v}),\ \gamma(\bar{v}) \in R \\ & \text{oder } \psi_{i,j} \hat{=} x = y,\ \gamma(x) \neq \gamma(y) \\ & \text{oder } \psi_{i,j} \hat{=} \neg x = y,\ \gamma(x) = \gamma(y) \\ 1 & \psi_{i,j} \hat{=} \dot{R}(\bar{v}),\ \gamma(\bar{v}) \in R \\ & \text{oder } \psi_{i,j} \hat{=} \neg\dot{R}(\bar{v}),\ \gamma(\bar{v}) \notin R \\ & \text{oder } \psi_{i,j} \hat{=} x = y,\ \gamma(x) = \gamma(y) \\ & \text{oder } \psi_{i,j} \hat{=} \neg x = y,\ \gamma(x) \neq \gamma(y) \\ w_{n\cdot\gamma(x)+\gamma(y)} & \psi_{i,j} \text{ hat die Form } E(x,y) \\ \neg w_{n\cdot\gamma(x)+\gamma(y)} & \psi_{i,j} \text{ hat die Form } \neg E(x,y) \end{cases}$$

$$\gamma(v) := \begin{cases} t_i & \text{falls } v = x_i \\ t_{k+i} & \text{falls } v = y_i \end{cases}$$

Gemäß der Definition von FO [**arb**] und der booleschen Schaltkreise gilt $\left[\!\left[\mathcal{D}_\psi^{\bar{t}}\right]\!\right]^{\mathrm{enc}_f(\mathfrak{A})} = 1$ genau dann wenn $\mathfrak{A} \models \psi\left(f^{-1}(\bar{t})\right)$. Es ist außerdem $T\left(\mathcal{D}_\psi^{\bar{t}}\right) = 2$ und $\left|\mathcal{D}_\psi^{\bar{t}}\right| \leqslant \|\psi\|$.

### 3.1.3 Rekursionsschritt

#### Voraussetzung

Sei $\psi(x_1, \cdots, x_k, y_1, \cdots, y_{\ell'})$ eine beliebige Formel mit Alternierungstiefe $d \in \mathbb{N}$ und Quantorenrang $m \in \mathbb{N}$. Es sei vorausgesetzt, dass für jedes Tupel $\bar{t} \in [n]^{k+\ell'}$

ein Schaltkreis $\mathcal{D}_{\psi}^{\bar{t}}$ mit der folgenden Eigenschaft existiert:

$$\mathrm{enc}_f(\mathfrak{A}) \models \mathcal{D}_{\psi}^{\bar{t}} \quad \Longleftrightarrow \quad \mathfrak{A}_f \models \psi\left(f^{-1}(\bar{t})\right)$$

Es sei außerdem $T\left(\mathcal{D}_{\psi}^{\bar{t}}\right) = d+2$ und $\left|\mathcal{D}_{\psi}^{\bar{t}}\right| \leqslant n^m \|\psi\|$.

### Folgerung

Sei $\psi'(x_1, \cdots x_k, y_1, \cdots, y_{\ell''})$ eine Formel der Form $Qy_{\ell''+1} \cdots Qy_{\ell'}\psi$ mit $Q \in \{\exists, \forall\}$ und Alternierungstiefe $d' = d+1$. Es wird für jedes Tupel $\bar{t'} \in [n]^{k+\ell''}$ ein Schaltkreis $\mathcal{D}_{\psi'}^{\bar{t'}}$ konstruiert, so dass gilt:

$$\mathrm{enc}_f(\mathfrak{A}) \models \mathcal{D}_{\psi'}^{\bar{t'}} \quad \Longleftrightarrow \quad \mathfrak{A}_f \models \psi'\left(f^{-1}\left(\bar{t'}\right)\right)$$

*Fall* 1. Sei $Q = \exists$. Gemäß Definition von FO [**arb**] gilt

$$\mathfrak{A}_f \models \exists y_{\ell''+1} \cdots \exists y_{\ell'}\psi\left(f^{-1}\left(\bar{t'}\right)\right)$$

genau dann wenn ein Tupel $\bar{t''} \in [n]^{\ell'-\ell''}$ existiert, so dass:

$$\mathfrak{A}_f \models \psi\left(f^{-1}\left(\bar{t'} \cdot \bar{t''}\right)\right)$$

Daher berechnet der folgende Schaltkreis den korrekten Wert:

$$\mathcal{D}_{\psi'}^{\bar{t'}} := \bigvee_{\bar{t''} \in [n]^{\ell'-\ell''}} \mathcal{D}_{\psi}^{\bar{t'} \cdot \bar{t''}}$$

Es ist außerdem $T\left(\mathcal{D}_{\psi'}^{\bar{t'}}\right) = d'+2$ und $\left|\mathcal{D}_{\psi'}^{\bar{t'}}\right| \leqslant n^{m'} \|\psi'\|$, wobei $m' = m + \ell' - \ell''$ der Quantorenrang von $\psi'$ ist. Die Voraussetzung ist damit erfüllt.

*Fall* 2. Sei $Q = \forall$. Gemäß Definition von FO [**arb**] gilt

$$\mathfrak{A}_f \models \forall y_{\ell''+1} \cdots \forall y_{\ell'}\psi\left(f^{-1}\left(\bar{t'}\right)\right)$$

genau dann für alle Tupel $\bar{t''} \in [n]^{\ell'-\ell''}$ gilt, dass:

$$\mathfrak{A}_f \models \psi\left(f^{-1}\left(\bar{t'} \cdot \bar{t''}\right)\right)$$

Der folgende Schaltkreis berechnet daher den korrekten Wert:

$$\mathcal{D}_{\psi'}^{\bar{t'}} := \bigwedge_{\bar{t''} \in [n]^{\ell'-\ell''}} \mathcal{D}_{\psi}^{\bar{t'} \cdot \bar{t''}}$$

Dieser Schaltkreis hat dieselbe Tiefe und Größe wie im ersten Fall.

### 3.1.4 Abschluss

Durch wiederholte Anwendung dieser Rekursion kann offensichtlich für die Formel $\varphi(x_1, \cdots, x_k)$ und jedes Tupel $\bar{t} \in [n]^k$ ein Schaltkreis $\mathcal{D}_\varphi^{\bar{t}}$ mit $T\left(\mathcal{D}_\varphi^{\bar{t}}\right) = d+2$ und $\left|\mathcal{D}_\varphi^{\bar{t}}\right| \leqslant n^\ell \|\varphi\|$ konstruiert werden, für den gilt:

$$\mathrm{enc}_f(\mathfrak{A}) \models \mathcal{D}_\psi^{\bar{t}} \quad \Longleftrightarrow \quad \mathfrak{A}_f \models \psi\left(f^{-1}(\bar{t})\right)$$

Für Sätze ohne freie Variablen ($k = 0$) ist dieser Schaltkreis bereits der gewünschte Schaltkreis $\mathcal{C}_{n^2+kn}$. Ansonsten ist ein letzter Konstruktionsschritt notwendig. Der Schaltkreis $\mathcal{C}_{n^2+kn}$ wird wie folgt gebildet:

$$\begin{aligned} \mathcal{C}_{n^2+kn} &:= \bigvee_{\bar{t}\in[n]^k} \left( \mathcal{D}_\varphi^{\bar{t}} \wedge \bigwedge_{i=1}^{k} w_{z(i,t_i)} \right) \\ z(i,t_i) &:= n^2 + n\cdot(i-1) + t_i \end{aligned}$$

Gemäß der Kodierung $\mathrm{enc}_f(\mathfrak{A}, \bar{a})$ ist $w_{z(t_i)} = 1$ genau dann wenn $t_i = f(a_i)$ ist. Daher gilt $\mathrm{enc}_f(\mathfrak{A}, \bar{a}) \models \mathcal{C}_n$ genau dann wenn $\mathrm{enc}_f(\mathfrak{A}) \models \mathcal{D}_\varphi^{f(\bar{a})}$ ist, und damit berechnet der Schaltkreis $\mathcal{C}_n$ das korrekte Ergebnis.

Zusätzlich ist $T(\mathcal{C}_{n^2+kn}) = d+4$, und $|\mathcal{C}_n| \leqslant 1 + n^k \cdot \left(2 + n^\ell \|\varphi\|\right)$. Es gilt (für $n > 1$, da $\|\varphi\| > k + \ell + 2$):

$$|\mathcal{C}_{n^2+kn}| \leqslant 3 \cdot n^{k+\ell} \leqslant n^{\|\varphi\|}$$

Die Schaltkreisfamilie hat also eine konstante Tiefe und polynomielle Größe in Abhängigkeit von $n$.

## 3.2 Schaltkreissequenz zu Satz

Es wurde nachgewiesen, dass jede durch eine arb-invariante Formel beschriebene Graph-Anfrage auch durch eine Schaltkreisfamilie in $\mathrm{AC}^0$ berechenbar ist. Umgekehrt gilt, dass jede in $\mathrm{AC}^0$ berechenbare Sprache durch einen $\mathrm{FO}[\sigma_B \cup \sigma_{arb}]$-Satz beschreibbar ist.

**Theorem 3.2.** *Sei $(\mathcal{C}_i)_{i\in\mathbb{N}}$ eine Schaltkreisfamilie mit beschränkter Tiefe $d \in \mathbb{N}$ und polynomieller Größe. Dann existiert eine Relation $Q \subseteq \mathbb{N}^k$ (mit $k \in \mathbb{N}$) und ein FO $\left[\sigma_B \cup \left\{\dot{Q}\right\}\right]$-Satz $\varphi$ mit Alternierungstiefe $d+4$, so dass für jede Länge $n \in \mathbb{N}$ und jedes Binärwort $w \in \{0,1\}^n$ gilt:*

$$[\![\varphi]\!]^{\mathfrak{B}_w} = [\![\mathcal{C}_n]\!]^w$$

*Bemerkung.* Aus diesem Theorem kann durch weitere Reduktionen gefolgert werden, dass alle Graph-Anfragen in $\mathrm{AC}^0$ auch in $\mathrm{FO}[\mathbf{arb}]$ beschrieben werden können. Dieser Beweis ist jedoch aufwendiger und wird für das Lokalitätsergebnis nicht benötigt.

### 3.2.1 Normalform für Schaltkreise

Sei $(\mathcal{C}_i)_{i\in\mathbb{N}}$ eine Schaltkreisfamilie. Es werden gemäß der Annahme Parameter $d, k \in \mathbb{N}$ vorausgesetzt, so dass jeder Schaltkreis $\mathcal{C}_n$ höchstens die Größe $f(n) = n^k$ und genau die Tiefe $d$ hat.

Ferner wird vorausgesetzt, dass der Schaltkreis ein Baum ist, dass die Junktoren stets alternieren, dass $f(\mathrm{Out}(\mathcal{C}_n)) \neq \wedge$ sei und $d$ gerade sei.

Dies schränkt die Allgemeinheit nicht ein:

*Beweis.* Es werden die Baumeigenschaft, die alternierenden Junktoren, und die Disjunktion in der Wurzel hergestellt.

- Sei zunächst $v \in \mathcal{C}_n = (G, f, x)$ ein Gatter mit mehr als einem Nachfolger. Kopien des Graphen $G_{|\mathrm{Pre}(\mathcal{C}_n, v)}$ werden dann in $G$ eingefügt, und jeder Nachfolger von $v$ mit einer Kopie von $v$ verbunden. Die Tiefe bleibt gleich, und die Größe bleibt daher polynomiell beschränkt.
- Seien $u, v \in \mathcal{C}_n$ zwei Gatter, so dass $(u, v) \in E^{\mathcal{C}_n}$, und $f(u) = f(v) \in \{\wedge, \vee\}$. So kann die Kante $(u, v)$ entfernt und durch die Kanten $(u', v)$ für alle Vorgänger von $u$ ersetzt werden. Alle Vorgänger von $u$ werden Vorgänger von $v$. Die Größe und Tiefe werden nicht vergrößert.
- Falls $f(\mathrm{Out}(\mathcal{C}_n)) = \wedge$, füge ein neues Outputgatter $x'$ mit $f(x') = \vee$ und der Kante $(\mathrm{Out}(\mathcal{C}_n), x')$ ein.
- Falls $T(\mathcal{C}_n) = d$ ungerade ist, so wähle ein Inputgatter $v$ mit maximaler Distanz vom Output, und füge zwischen $v$ und seinen Nachfolger einen Knoten ein.

□

Nun wird eine Normalform $\hat{\mathcal{C}_n} = (G', f', x)$ für alle Schaltkreise in alternierender Baumform definiert. Die Normalform behält die Tiefe $T\left(\hat{\mathcal{C}_n}\right) = T(\mathcal{C}_n) = d$ und die Größe $\left|\hat{\mathcal{C}_n}\right| \leqslant n^{kd'+1}$. Jeder Weg von einem Input zum Output hat genau die Länge $T\left(\hat{\mathcal{C}_n}\right)$. Jedes innere Gatter hat genau $n^k$ Vorgänger.

Diese Normalform schränkt die Allgemeinheit nicht ein:

*Beweis.* Per Induktion über die Tiefe $T(\mathcal{C}_n) = d$.

**Anfang:** Sei $d = 0$. Für alle $\mathcal{C}_n$ mit $T(\mathcal{C}_n) = 0$ folgt $|\mathcal{C}_n| = 1$; das Outputgatter ist ein Input. Der Schaltkreis ist also schon in Normalform.

**Schritt:** $d \to d + 1$

Annahme: Sei $d \in \mathbb{N}$ beliebig. Es gelte die Annahme, dass für jeden Schaltkreis $\mathcal{C}_n$ mit $T(\mathcal{C}_n) \leqslant d$ ein Schaltkreis $\hat{\mathcal{C}_n}$ mit den geforderten Eigenschaften existiert.

Sei $\mathcal{C}'_n$ ein Schaltkreis mit $T(\mathcal{C}'_n) = d+1$. Betrachte nun für alle Vorgänger $u$ des Outputs den Schaltkreisteil $\mathcal{C}'_{n,u}$. Da $T\left(\mathcal{C}'_{n,u}\right) \leqslant d$ gilt, existiert nach der Annahme die Normalform $\hat{\mathcal{C}'_{n,u}}$.

Es müssen alle Schaltkreisteile auf die Tiefe $d$ gebracht werden, und der Eingangsgrad jedes neuen Knotens auf $n^k$ aufgefüllt werden. Sei dafür $T_{i,x}(\mathcal{C})$ für $i \in \mathbb{N}$ und $x \in \{\wedge, \vee\}$ rekursiv wie folgt:

$$\begin{aligned} T_{0,\wedge}(\mathcal{D}) = T_{0,\vee}(\mathcal{D}) &:= \mathcal{D} \\ T_{i+1,\wedge}(\mathcal{D}) &:= \bigwedge_{1 \leqslant j \leqslant n^k} T_{i,\vee}(\mathcal{D}) \\ T_{i+1,\vee}(\mathcal{D}) &:= \bigvee_{1 \leqslant j \leqslant n^k} T_{i,\wedge}(\mathcal{D}) \end{aligned}$$

(Offensichtlich sind alle so aus $\mathcal{D}$ erzeugten Schaltkreise äquivalent zu $\mathcal{D}$.)

Nun werden die Eingänge des Outputs ausgefüllt. Sei $\hat{\mathcal{C}'_n}$ für $f(\mathrm{Out}(\mathcal{C}'_n)) = \wedge$ beziehungsweise $f(\mathrm{Out}(\mathcal{C}'_n)) = \vee$ wie folgt:

$$\begin{aligned} \hat{\mathcal{C}'_n} &= \left( \bigwedge_{u \in \mathrm{In}(\mathcal{C'}_n, v)} T_{d-T\left(\mathcal{C}'_{n,u}\right),\vee}\left(\hat{\mathcal{C}'_{n,u}}\right) \right) \wedge \left( \bigwedge_{i=1}^{n^k - \left|\mathrm{In}(\mathcal{C'}_n, v)\right|} T_{d,\wedge}(1) \right) \\ \hat{\mathcal{C}'_n} &= \left( \bigvee_{u \in \mathrm{In}(\mathcal{C'}_n, v)} T_{d-T\left(\mathcal{C}'_{n,u}\right),\wedge}\left(\hat{\mathcal{C}'_{n,u}}\right) \right) \vee \left( \bigvee_{i=1}^{n^k - \left|\mathrm{In}(\mathcal{C'}_n, v)\right|} T_{d,\vee}(0) \right) \end{aligned}$$

Damit hat $\hat{\mathcal{C}'_n}$ die geforderte Form. Außerdem gilt $f\left(\mathrm{Out}\left(\hat{\mathcal{C}_n}\right)\right) = f\left(\mathrm{Out}\left(\mathcal{C}_n\right)\right) = \vee$, und $d$ bleibt gerade. □

### 3.2.2 Kodierung der Schaltkreise

Sei $(\mathcal{C}_i)_{i \in \mathbb{N}}$ eine Schaltkreisfamilie in der vereinbarten Normalform mit Tiefe $d$.

Für jedes innere Gatter $v \in \mathcal{C}_n$ wird eine Aufzählung $g_v : \mathrm{In}(\mathcal{C}_n, v) \to \left[n^k\right]$ festgelegt, so dass jede Kante $(u, v)$ durch die Zahl $g_v(u) \in \left[n^k\right]$ kodiert werden kann. Weiterhin ist klar, dass jede Zahl $i \in \left[n^k\right]$ durch eine Funktion $\alpha_n : \left[n^k\right] \to$

$[n]^k$ als $k$-stellige Zahl in Basis $n$ dargestellt werden kann:[1]

$$m = 1 + \sum_{j=1}^{k} \Big( (\alpha_n (m))_j - 1 \Big) \, n^{k-j}$$

Jetzt wird jeder Knoten $v \in \mathcal{C}_n$ wie folgt durch die Funktion $\texttt{code} : \mathcal{C}_n \to [n]^*$ repräsentiert:

$$\begin{array}{rcl} \texttt{code}\,(\mathrm{Out}\,(\mathcal{C}_n)) & := & \varepsilon \\ \texttt{code}\,(u) & := & \texttt{code}\,(v) \cdot \alpha_n\,(g_v\,(u)) \\ & \text{f.a.} & v \in \mathcal{C}_n,\ u \in \mathrm{In}\,(\mathcal{C}_n, v) \end{array}$$

Jedes Gatter hat dadurch eine eindeutige Kodierung $\texttt{code}\,(v) \in [n]^{k\mathbb{N}}$, wobei $\{\texttt{code}\,(v)\} \times [n]^k$ die Kodierungen aller direkten Vorgänger von $v$ sind.

Die Relation $Q \subseteq \mathbb{N}^{4+kd}$ sei wie folgt definiert:

$$Q = \bigcup_{n \in \mathbb{N}} \left( \begin{array}{rl} & \{(n,1,1,i) \cdot \texttt{code}\,(v) \ : \ v \in \mathcal{C}_n,\ f\,(v) = I_i\} \\ \cup & \{(n,1,n,i) \cdot \texttt{code}\,(v) \ : \ v \in \mathcal{C}_n,\ f\,(v) = \overline{I_i}\} \\ \cup & \{(n,n,1,1) \cdot \texttt{code}\,(v) \ : \ v \in \mathcal{C}_n,\ f\,(v) = \mathbf{1}\} \\ \cup & \{(n,n,n,1) \cdot \texttt{code}\,(v) \ : \ v \in \mathcal{C}_n,\ f\,(v) = \mathbf{0}\} \end{array} \right)$$

Die Relation enthält die Kodierungen $\texttt{code}\,(v)$ und Markierungen $f\,(v)$ aller Inputgatter $v \in \mathcal{C}_n$ für $n \in \mathbb{N}$.

Es werde die Auswertungsfunktion $\texttt{eval}_n : [n]^{\{0,k,\cdots,kd\}} \times \{0,1\}^n \to \{0,1\}$ definiert, so dass $\texttt{eval}_n\,(\texttt{code}\,(v)\,, w)$ für einen Knoten $v \in \mathcal{C}_n$ und ein Wort $w \in \{0,1\}^n$ der Auswertungsfunktion $[\![\mathcal{C}_{n,v}]\!]^w$ entspricht. Damit gilt allgemein $[\![\mathcal{C}_{|w|}]\!]^w = \texttt{eval}_{|w|}\,(\varepsilon, w)$.

Die Funktion $\texttt{eval}_n$ wird rekursiv definiert.

[1] Der Bereich $[n]$ wurde als $\{1, \cdots, n\}$ definiert. Für diese Darstellung steht daher die Ziffer $i \in [n]$ für einen Stellenwert $i - 1$.

$$\begin{aligned}
\texttt{eval}_n(\bar{z}, w) &:= \begin{cases} w_i & \text{falls } (n,1,1,i) \in Q,\ i \in [n] \\ \neg w_i & \text{falls } (n,1,n,i) \in Q,\ i \in [n] \\ 1 & \text{falls } (n,n,1,1) \in Q \\ 0 & \text{sonst} \end{cases} \\
&\text{f.a.} \quad \bar{z} \in \mathbb{N}^{kd}
\end{aligned}$$

$$\begin{aligned}
\texttt{eval}_n(\bar{z}, w) &:= \begin{cases} 1 & \text{falls ex. } \bar{z'} \in [n]^k \text{ mit } \texttt{eval}_n\left(\bar{z} \cdot \bar{z'}, w\right) = 1 \\ 0 & \text{sonst} \end{cases} \\
&\text{f.a.} \quad \bar{z} \in \mathbb{N}^{ki},\ i < d \text{ gerade}
\end{aligned}$$

$$\begin{aligned}
\texttt{eval}_n(\bar{z}, w) &:= \begin{cases} 1 & \text{falls } \texttt{eval}_n\left(\bar{z} \cdot \bar{z'}, w\right) = 1 \text{ f.a. } \bar{z'} \in [n]^k \\ 0 & \text{sonst} \end{cases} \\
&\text{f.a.} \quad \bar{z} \in \mathbb{N}^{ki},\ i \text{ ungerade}
\end{aligned}$$

Die Funktion berechnet das korrekte Ergebnis.

*Beweis.* Durch absteigende Induktion über $i$.

**Anfang:** Sei $i = d$, und $\bar{z} \in [n]^{ki}$ beliebig. Sei $v \in \mathcal{C}_n$ das Inputgatter mit $\texttt{code}(v) = \bar{z}$. Per Definition von $Q$ und $\texttt{eval}_n$ gilt:

$$\begin{aligned}
& & \texttt{eval}_n(\texttt{code}(v), w) = 1 \\
\iff & & (n,n,1,1) \in Q \\
& \text{oder} & (n,1,1,i) \in Q \text{ und } w_i = 1 \\
& \text{oder} & (n,1,n,i) \in Q \text{ und } w_i = 0 \\
\iff & & f(v) = \mathbf{1} \\
& \text{oder} & f(v) = I_i \text{ und } w_i = 1 \\
& \text{oder} & f(v) = \overline{I_i} \text{ und } w_i = 0 \\
\iff & & [\![\mathcal{C}_{n,v}]\!]^w = 1
\end{aligned}$$

**Schritt:** Seien $1 \leqslant i \leqslant d$ und beliebig.

Annahme: Für alle $\bar{z} = \texttt{code}(v) \in [n]^{ki}$ gelte $\texttt{eval}_n(\bar{z}, w) = [\![\mathcal{C}_{n,v}]\!]^w$.

Sei $i' = i - 1$ und $\bar{z'} = \texttt{code}(u) \in [n]^{ki'}$.

*Fall* 1. Sei $i'$ gerade. Nun gilt:

$$\begin{aligned}
& \texttt{eval}_n\left(\texttt{code}\left(v\right), w\right) = 1 \\
\iff \quad & \text{ex. } \bar{z'} \in [n]^k \text{ mit } \texttt{eval}_n\left(\bar{z} \cdot \bar{z'}, w\right) = 1 \\
\overset{Def\ \texttt{code}}{\iff} \quad & \text{ex. } u \in \mathrm{In}\left(\mathcal{C}_n, v\right) \text{ mit } \texttt{eval}_n\left(\texttt{code}\left(u\right), w\right) = 1 \\
\overset{I.A.}{\iff} \quad & \text{ex. } u \in \mathrm{In}\left(\mathcal{C}_n, v\right) \text{ mit } \left[\!\left[C_{n,u}\right]\!\right]^w = 1 \\
\overset{Def\ [\![\cdot]\!]}{\iff} \quad & \left[\!\left[\mathcal{C}_{n,v}\right]\!\right]^w = 1
\end{aligned}$$

*Fall* 2. Sei $i'$ ungerade. Dann ist analog $\texttt{eval}_n\left(\texttt{code}\left(v\right), w\right) = 1$ genau dann wenn *alle* Vorgänger von $v$ mit 1 ausgewertet werden. Die Auswertung entspricht wieder der Definition des Schaltkreises.

Es folgt insbesondere für $i = 0$, dass $\texttt{eval}_n\left(\varepsilon, w\right) = \left[\!\left[\mathcal{C}_n\right]\!\right]^w$. □

### 3.2.3 Aufbau der Formel

Entsprechend der rekursiven Definition der Funktion `eval` wird nun ein FO $[\sigma_B \cup \sigma_{arb}]$-Satz $\varphi$ definiert, der das Prädikat $\dot{Q}$ verwendet, um die Funktion `eval` (und daher die Auswertung des Schaltkreises) zu beschreiben.

Der Satz $\varphi$ ist wie folgt:

$$\begin{aligned}
\varphi &:= \exists x_{\mathbf{1}} \exists x_{\mathbf{n}} \ \left(\psi\left(x_{\mathbf{1}}, x_{\mathbf{n}}\right) \wedge \forall x \ \left(x_{\mathbf{1}} \leqslant x \wedge x \leqslant x_{\mathbf{n}}\right)\right) \\
\psi\left(x_{\mathbf{1}}, x_{\mathbf{n}}\right) &:= \underbrace{\exists y_{2i-1,1} \cdots \exists z_{2i-1,k} \forall y_{2i,1} \cdots \forall y_{2i,k}}_{i=1,\cdots,\frac{d}{2}} \exists z \ \xi\left(\bar{y}, z, x_{\mathbf{1}}, x_{\mathbf{n}}\right) \\
\xi\left(\bar{y}, z, x_{\mathbf{1}}, x_{\mathbf{n}}\right) : &= \left(Q\left(x_{\mathbf{n}}, x_{\mathbf{1}}, x_{\mathbf{1}}, z, y_{1,1}, \cdots, y_{d,k}\right) \wedge P_1\left(z\right)\right) \vee \\
&\quad \left(Q\left(x_{\mathbf{n}}, x_{\mathbf{1}}, x_{\mathbf{n}}, z, y_{1,1}, \cdots, y_{d,k}\right) \wedge \neg P_1\left(y\right)\right) \vee \\
&\quad Q\left(x_{\mathbf{n}}, x_{\mathbf{n}}, x_{\mathbf{1}}, x_{\mathbf{1}}, y_{1,1}, \cdots, y_{d,k}\right)
\end{aligned}$$

Die Alternierungstiefe von $\varphi$ ist $d + 1$ für einen Schaltkreis der Tiefe $d$.

*Behauptung.* Für $w \in \{0,1\}^*$ gilt $\mathfrak{B}_w \models \varphi$ genau dann wenn $w \models \mathcal{C}_{|w|}$.

*Beweis.* Durch absteigende Induktion über $i$:

Sei $n \in \mathbb{N}$ und $w \in \{0,1\}^n$ beliebig.

**Anfang** Sei $i = \frac{d}{2}$. Es sei das Tupel $\bar{b} \in [n]^{kd}$ beliebig. Nun gilt per Definition von `eval` und $\varphi$:

$$\mathfrak{B}_w \models \exists z \ \xi\left(\bar{b}, z, 1, n\right) \quad \iff \quad \texttt{eval}_n\left(\bar{b}, w\right) = 1$$

Es folgt aus dem vorherigen Beweis für $v = \texttt{code}^{-1}\left(\bar{b}\right)$:

**Schritt** Sei $i \in \left[\frac{n}{2}\right]$. Es sei $\varphi_i$ die folgende Formel:

$$\varphi_i\left(y_{1,1}, \cdots, y_{2i,k}\right) \;:=\; \underbrace{\exists y_{2j+1,1} \cdots \exists z_{2j+1,k} \forall y_{2j+2,1} \cdots \forall y_{2j+2,k}}_{i \leqslant j < \frac{d}{2}} \exists z \; \xi\left(\bar{y}, z, x_{\mathbf{1}}, x_{\mathbf{n}}\right)$$

Annahme: Für jedes Tupel $\bar{b} \in [n]^{ki}$ und $v = \mathtt{code}^{-1}\left(\bar{b}\right)$ gilt:

$$\mathfrak{B}_w \models \varphi_i\left(\bar{b}, 1, n\right) \quad \Longleftrightarrow \quad \mathtt{eval}_n\left(\bar{b}, w\right) = 1$$

Sei $i' = i - 1$. Es gilt nun:

$$\varphi_{i-1}\left(y_{1,1}, \cdots, y_{2i',k}, x_{\mathbf{1}}, x_{\mathbf{n}}\right) \;:=\; \exists y_{2i+1,1} \cdots \exists y_{2i+1,k} \forall y_{2i+2,1} \forall y_{2i+2,k} \varphi_i$$

So folgt für jedes Tupel $\bar{b'} \in [n]^{ki'}$:

$$\begin{aligned}
\mathfrak{B}_w \models \varphi_{i-1}\left(\bar{b'}, 1, n\right) \quad &\Longleftrightarrow \quad \text{ex. } \bar{c} \in [n]^k \text{ so dass} \\
&\qquad \text{f.a. } \bar{c'} \in [n]^k \text{ gilt :} \\
&\qquad \mathfrak{B}_w \models \varphi_i\left(\bar{b'} \cdot \bar{c} \cdot \bar{c'}, 1, n\right) \\
&\overset{I.A.}{\Longleftrightarrow} \quad \text{ex. } \bar{c} \in [n]^k \text{ so dass} \\
&\qquad \text{f.a. } \bar{c'} \in [n]^k \text{ gilt :} \\
&\qquad \mathtt{eval}\left(\bar{b'} \cdot \bar{c} \cdot \bar{c'}, w\right) = 1 \\
&\Longleftrightarrow \quad \text{ex. } \bar{c} \in [n]^k \text{ so dass} \\
&\qquad \mathtt{eval}\left(\bar{b'} \cdot \bar{c}, w\right) = 1 \\
&\Longleftrightarrow \quad \mathtt{eval}\left(\bar{b'}, w\right) = 1
\end{aligned}$$

Damit folgt insbesondere $[\![\varphi_0\left(1, n\right)]\!]^{\mathfrak{B}_w} = \mathtt{eval}\left(\varepsilon, w\right)$ für $i = 0$. Zusammen mit dem Beweis aus **Abschnitt 3.2.2** folgt $\mathfrak{B}_w \models \varphi$ genau dann wenn $w \models \mathcal{C}_n$. $\square$

# 4 Graph-Operationen und Schaltkreisschranken

## 4.1 Austausch von $r$-Schalen

Sei $\mathfrak{A}$ ein Graph der Größe $n$, seien $a, b \in A$ zwei Knoten und $r \in \mathbb{N}$ ein Radius, so dass die $r$-Umgebungen von $a$ und $b$ isomorph und disjunkt sind:

$$\begin{aligned} \mathcal{N}_r^{\mathfrak{A}}(a) &\cong \mathcal{N}_r^{\mathfrak{A}}(b) \\ \mathcal{N}_r^{\mathfrak{A}}(a) \cap \mathcal{N}_r^{\mathfrak{A}}(b) &= \emptyset \end{aligned}$$

Für beliebige Bitstrings $w \in \{0,1\}^r$ soll eine Umformung $\mathfrak{A}_w$ definiert werden, so dass $(\mathfrak{A}_w, a) \cong (\mathfrak{A}, a)$ genau dann wenn $|w|_1$ gerade ist, und sonst $(\mathfrak{A}_w, a) \cong (\mathfrak{A}, b)$.

Diese Umformung soll trivial in einem Schaltkreis durchführbar sein: Aus einem Schaltkreis $\mathcal{C}_{n^2+n}$ soll ohne Veränderung der Größe und Tiefe ein Schaltkreis $\mathcal{C}'_r$ konstruiert werden, so dass für alle $w \in \{0,1\}^r$ gilt:

$$[\![\mathcal{C}'_r]\!]^w = [\![\mathcal{C}_n]\!]^{\mathrm{enc}(\mathfrak{A}_w, a)}$$

### 4.1.1 Ansatz

Seien $(S_i^a)_{0 \leqslant i \leqslant r}$ und $\left(S_i^b\right)_{0 \leqslant i \leqslant r}$ die Schalen der $r$-Umgebungen um $a$ und $b$ (hierbei wird $S_i^{\mathfrak{A}}(a)$ für den gegebenen Graphen $\mathfrak{A}$ mit $S_i^a$ abgekürzt). Es wird eine Umformung $\mathfrak{A}_w$ definiert, in der $S_{i-1}^a$ genau dann mit $S_i^a$ verbunden ist, wenn $w_i = 0$ ist, und sonst $S_{i-1}^a$ mit $S_i^b$ verbunden wird.

Dazu werden alle Kanten zwischen $S_{i-1}^x, S_i^x$ $(x \in \{a, b\})$ gegebenenfalls gelöscht und durch entsprechende Kanten zwischen $S_{i-1}^x, S_i^y$ $(y \in \{a, b\} \setminus \{x\})$ ersetzt.

**Beispiel.** Es wird die Vertauschung in einem Graphen gezeigt, in dem $\mathcal{N}_r^{\mathfrak{A}}(a)$ die Form eines langen Pfades hat. Kanten im Pfad werden teilweise durch Überkreuzungen ersetzt:

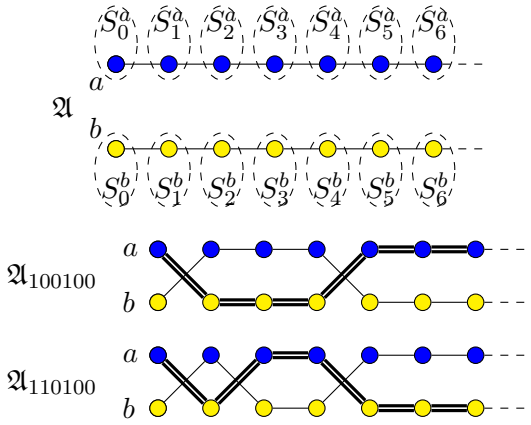


Abbildung 4.1: $(\mathfrak{A}_w, a) \cong \begin{cases} (\mathfrak{A}, a) & |w|_1 \text{ gerade} \\ (\mathfrak{A}, b) & \text{sonst} \end{cases}$

### 4.1.2 Formalisierung

Sei $\pi : \mathcal{N}_r^{\mathfrak{A}}(a) \cong \mathcal{N}_r^{\mathfrak{A}}(b)$ ein Isomorphismus mit $\pi(a) = b$. Unter der Annahme, dass die Umgebungen disjunkt sind, kann eine Funktion $\pi_{\leftrightarrows} : N_r^{\mathfrak{A}}(a) \cup N_r^{\mathfrak{A}}(b) \to N_r^{\mathfrak{A}}(a) \cup N_r^{\mathfrak{A}}(b)$ gebildet werden:

$$\pi_{\leftrightarrows}(x) = \begin{cases} \pi(x) & \text{falls } x \in N_r^{\mathfrak{A}}(a) \\ \pi^{-1}(x) & \text{falls } x \in N_r^{\mathfrak{A}}(b) \end{cases}$$

Nun wird eine Operation $\texttt{switch}(\mathfrak{A}, a, b, i)$ definiert, die die Umgebung $\mathcal{N}_{i-1}^{\mathfrak{A}}(a)$ mit der Umgebung $\mathcal{N}_{i-1}^{\mathfrak{A}}(b)$ für $i \in [r]$ im Graphen vertauscht.

Dazu müssen alle Kanten zwischen $S_{i-1}^a$ und $S_i^a$ entfernt, und entsprechende Kanten zwischen $S_{i-1}^a$ und $S_i^b$ eingefügt werden.

**Beispiel.** Die Schalenvertauschung wird in Umgebungen beliebiger Form gezeigt:

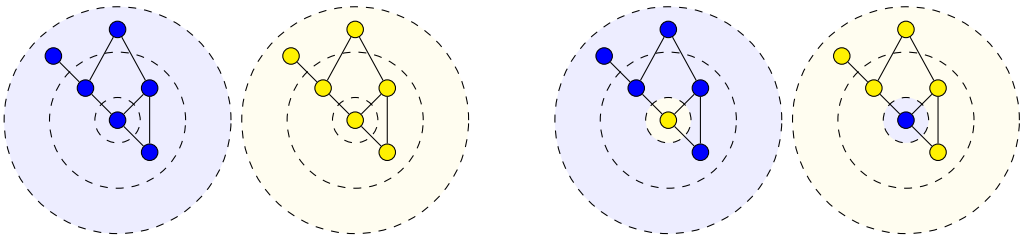

Abbildung 4.2: Beispiel für $\texttt{switch}(\mathfrak{A}, a, b, 0)$.

Formal werden in $\mathfrak{A}$ Tupel entfernt und eingefügt. Für jede Kante $(u,v) \in E^{\mathfrak{A}} \cap \left(N_r^{\mathfrak{A}}(x)\right)^2$ (mit $x \in \{a,b\}$) gilt einer der folgenden Fälle:

*Fall* 1. Es gilt $\{u,v\} \subseteq S_i^x$ für $0 \leqslant i \leqslant r$.

*Fall* 2. Ein Knoten liegt in $S_{i-1}^x$, der andere in $S_i^x$ (mit $i \in [r]$).[1]

Zunächst wird etwas Vorarbeit geleistet. Für $i \in [r]$ sei:

$$\begin{aligned} \rho_{i,a}(c) &:= \begin{cases} \pi_{\leftrightarrows}(c) & \text{falls } c \in S_i^a \\ c & \text{sonst} \end{cases} \\ \mathcal{X}_i^a &:= E^{\mathfrak{A}} \cap \left(S_{i-1}^a \times S_i^a \cup S_i^a \times S_{i-1}^a\right) \\ \mathcal{Y}_i^a &:= \{(\rho_{i,a}(u), \rho_{i,a}(v)) : (u,v) \in \mathcal{X}_i^a\} \end{aligned}$$

Danach wird die Relation $\texttt{switch}(\mathfrak{A}, a, b, i)$ für $i \in [r]$ wie folgt definiert:

$$\texttt{switch}(\mathfrak{A}, a, b, i) := E^{\mathfrak{A}} \backslash \mathcal{X}_i^a \backslash \mathcal{X}_i^b \cup \mathcal{Y}_i^a \cup \mathcal{X}_i^b$$

Die Operation `switch` wird erweitert, um mehrere Schalen zu vertauschen. Für $w \in \{0,1\}^r$ sei:

$$\begin{aligned} \texttt{switch}(\mathfrak{A}, a, b, w) &:= E^{\mathfrak{A}} \backslash \left( \bigcup_{\substack{i=1 \\ w_i=1}}^{r} \mathcal{X}_i^a \cup \bigcup_{\substack{i=1 \\ w_i=1}}^{r} \mathcal{X}_i^b \right) \cup \bigcup_{\substack{i=1 \\ w_i=1}}^{r} \mathcal{Y}_i^a \cup \bigcup_{\substack{i=1 \\ w_i=1}}^{r} \mathcal{Y}_i^b \\ \mathfrak{A}_w &:= (A, \texttt{switch}(\mathfrak{A}, a, b, w)) \end{aligned}$$

Nun ist $(\mathfrak{A}_w, a) \cong (\mathfrak{A}, a)$ genau dann wenn $|w|_1 = 0 \mod 2$, und sonst $(\mathfrak{A}_w, a) \cong (\mathfrak{A}, b)$.

### 4.1.3 Schaltkreis

Sei $\mathcal{C}_{n^2+n} = (G, f, x)$ ein Schaltkreis, der eine einstellige Anfrage auf Kodierungen von $\mathfrak{A}$ berechnet, so dass $[\![\mathcal{C}_{n^2+n}]\!]^{\mathrm{enc}(\mathfrak{A},a)} = 1$ und $[\![\mathcal{C}_{n^2+n}]\!]^{\mathrm{enc}(\mathfrak{A},b)} = 0$.

Das Ziel ist ein Schaltkreis $\mathcal{C}'_r = (G, f', x)$, der als Eingabe $w \in \{0,1\}^r$ erhält, und der sie genau dann akzeptiert, wenn $(\mathfrak{A}_w, \bar{a}) \cong (\mathfrak{A}, \bar{a})$ gilt (was per Definition äquivalent zu $|w|_1 = 0 \mod 2$ ist).

Es wurde $\mathfrak{A}$ und $a$ fest vorgegeben, und es sei auch eine beliebige Aufzählung $g : A \to [n]$ festgelegt; dadurch entsteht eine eindeutige Kodierung $\mathrm{enc}_g(\mathfrak{A}, a) \in \{0,1\}^{n^2+n}$. Nun gilt für jedes $i \in \left[n^2+n\right]$ folgendes:

[1] Falls $u \in S_i^x, v \in S_{i+j}^x$, so enthält der Gaifman-Graph die Kante $\{u,v\} \in E$, und damit ist $\mathrm{dist}(a,v) \leqslant \mathrm{dist}(a,u) + \mathrm{dist}(u,v) = i+1$; daher ist $j \leqslant 1$.

*Fall* 1. Das Bit $\mathrm{enc}_g(\mathfrak{A}, a)_i = 1$ kodiert eine Kante aus $\mathcal{X}_j^x$ für ein $j \in [r]$, $x \in \{a, b\}$. Solche Kanten werden entfernt, falls $w_j = 1$ ist. Für alle $v \in \mathcal{C}_{n^2+n}$ mit $f(v) = I_i$ bzw. $\overline{I_i}$ wird $f'(v) := \overline{I_j}$ bzw. $I_j$ definiert.

*Fall* 2. Das Bit $\mathrm{enc}_g(\mathfrak{A}, a)_i = 0$ kodiert eine Kante aus $\mathcal{Y}_j^x$ für ein $j \in [r]$, $x \in \{a, b\}$. Diese Kanten werden eingefügt, falls $w_j = 1$ ist. Für alle $v \in \mathcal{C}_{n^2+n}$ mit $f(v) = I_i$ bzw. $\overline{I_i}$ wird $f'(v) := \overline{I_j}$ bzw. $I_j$ definiert.

*Fall* 3. Das Bit $\mathrm{enc}_g(\mathfrak{A}, a)_i$ kodiert etwas anderes, und ist daher gleich $\mathrm{enc}_g(\mathfrak{A}_w, a)_i$. Diese Stellen sind fest für alle $w \in \{0,1\}^r$. Für alle $v \in \mathcal{C}_{n^2+n}$ mit $f(v) \in \left\{I_i, \overline{I_i}\right\}$ wird $f'(v) \in \{\mathbf{0}, \mathbf{1}\}$ entsprechend dem Wert von $w_i$ definiert.

Der Graph des Schaltkreises bleibt unverändert; nur die Markierung ändert sich. Für alle $w \in \{0,1\}^r$ gilt $[\![\mathcal{C}'_r]\!]^w = [\![\mathcal{C}_{n^2+n}]\!]^{\mathrm{enc}_g(\mathfrak{A}_w, a)}$.

.

## 4.2 Rotation von $r$-Schalen

Sei $\mathfrak{A}$ ein Graph der Größe $n$, seien $a, b \in A$ zwei Knoten, sei $r \in \mathbb{N}$ ein Radius und $\pi : \mathcal{N}_r^{\mathfrak{A}}(a) \cong \mathcal{N}_r^{\mathfrak{A}}(b)$ ein Isomorphismus.

Es wird vorausgesetzt, dass $\mathcal{U} = \left\{\pi^j(a) \,:\, j \in \mathbb{N}\right\} \subseteq \mathcal{N}_r^{\mathfrak{A}}(a)$ eine geschlossene zyklische Bahn beschreibe, und dass die $i$-Umgebungen $\mathcal{N}_i^{\mathfrak{A}}(\mathcal{U})$ für $i \in [r]$ unter $\pi$ abgeschlossen seien. Sei $m \leqslant \frac{r}{2}$.

Das Ziel ist die Konstruktion eines Graphen $\mathfrak{A}_w$ für $w \in \{0,1\}^{2m}$ mit einem Element $a' \in A$, so dass $(\mathfrak{A}_w, a') \cong (\mathfrak{A}, a)$ falls $|w|_1 = m$, und $(\mathfrak{A}_w, a') \cong (\mathfrak{A}, b)$ falls $|w|_1 = m + 1$.

Die Konstruktion soll wieder trivial durch einen Schaltkreis berechenbar sein: Aus einem Schaltkreis $\mathcal{C}_{n^2+n}$ und einer beliebigen Aufzählung $f : A \to [n]$ wird ein Schaltkreis $\mathcal{C}'_{2m}$ konstruiert, so dass gilt:

$$[\![\mathcal{C}'_{2m}]\!](w) = [\![\mathcal{C}_{n^2+n}]\!]\left(\mathrm{enc}_f\left(\mathfrak{A}_w, \pi^{-m}(a)\right)\right)$$

### 4.2.1 Ansatz

Zunächst wird $\mathcal{N}_{\mathfrak{A}}^{2m}(\mathcal{U})$ in die Schalen $S_0, \cdots, S_{2m}$ aufgeteilt (es werde $S_i^{\mathfrak{A}}(\mathcal{U})$ durch $S_i$ abgekürzt), wobei $\mathcal{S}_0 = \mathcal{U}$ ist. Alle Schalen sind per Annahme unter $\pi$ geschlossen.

Es sollen durch die Operation `rotate` $(\mathfrak{A}, a, i)$ für $i \in [2m]$ die Schalen $S_{i-1}$ und $S_i$ so gegeneinander verdreht werden, dass alle Kanten zwischen $c \in \mathcal{S}_{i-1}$ und $c' \in S_i$ durch Kanten zwischen $c$ und $\pi(c')$ ersetzt werden. Analog zu `switch`

wird $\texttt{rotate}(\mathfrak{A}, a, w)$ für $w \in \{0,1\}^{2m}$ definiert, so dass für alle $i \in [2m]$ genau dann die Schalen $S_{i-1}$ und $S_i$ gegeneinander rotiert werden, wenn $w_i = 1$.

Dann sei $a' = \pi^{-m}(a)$. Falls genau $m$ Schalen gegeneinander rotiert werden, dann ist $(\mathfrak{A}_w, a') \cong (\mathfrak{A}, a)$. Falls genau $m+1$ Schalen rotiert werden, ist $(\mathfrak{A}_w, a') \cong (\mathfrak{A}, \pi(a)) = (\mathfrak{A}, b)$.

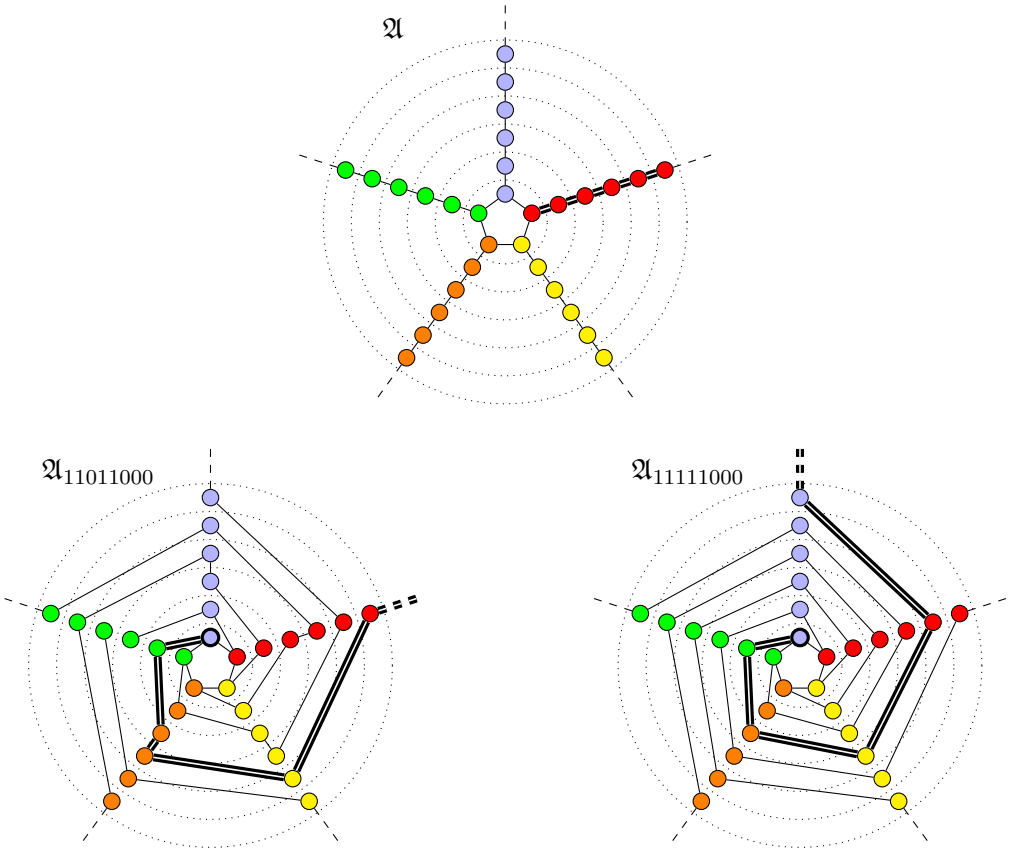


Abbildung 4.3: Der Isomorphismus $\pi$ verläuft im Uhrzeigersinn. Die Schalen $S_6, S_7, S_8$ sind nicht dargestellt. Der fett markierte Knoten ist $\pi^{-4}(a)$.

### 4.2.2 Formalisierung

Wieder werden einige Operationen und Mengen definiert. Für $i \in [2m]$ sei:

$$\begin{aligned} \rho_i(c) &:= \begin{cases} \pi(c) & \text{falls } c \in S_i \\ c & \text{sonst} \end{cases} \\ \mathcal{X}_i &:= E^{\mathfrak{A}} \cap (S_{i-1} \times S_i \cup S_i \times S_{i-1}) \\ \mathcal{Y}_i &:= \{(\rho_i(u), \rho_i(v)) : (u,v) \in \mathcal{X}_i\} \end{aligned}$$

Durch das Entfernen der Kanten $\mathcal{X}_i$ und Einfügen der Kanten $\mathcal{Y}_i$ werden die Kanten zwischen Elementen $c \in \mathcal{S}_{i-1}$ und $c' \in \mathcal{S}_i$ durch Kanten zwischen $\pi^{-1}(c)$ und $c$ (beziehungsweise $c$ und $\pi(c)$) ersetzt. Daher sei nun $\texttt{rotate}(\mathfrak{A}, a, w)$ entsprechend `switch` wie folgt definiert:

$$\begin{aligned} \texttt{rotate}(\mathfrak{A}, a, w) &:= \mathfrak{A}_w = \left(A, E^{\mathfrak{A}_w}\right) \\ E^{\mathfrak{A}_w} &:= \left(E^{\mathfrak{A}} \setminus \bigcup_{\substack{i=1 \\ w_i=1}}^{2m} \mathcal{X}_i\right) \cup \bigcup_{\substack{i=1 \\ w_i=1}}^{2m} \mathcal{Y}_i \end{aligned}$$

### 4.2.3 Schaltkreis

Es sei wieder ein Schaltkreis vorgegeben, der $\text{enc}(\mathfrak{A}, a)$ akzeptiert und $\text{enc}(\mathfrak{A}, b)$ ablehnt. Analog zum letzten Abschnitt wird ein Schaltkreis konstruiert, der $[\![\mathcal{C}_{n^2+n}]\!]^{\text{enc}(\mathfrak{A}_w, \pi^{-m}(a))}$ bei Eingabe von $w \in \{0,1\}^{2m}$ berechnet. Dieser Schaltkreis akzeptiert dann bei $|w|_1 = m$ und lehnt bei $|w|_1 = m+1$ ab.

## 4.3 Parity und der Satz von Håstad

Das PARITY-Problem zählt die Einsen in einem Bitstring. Es wird eine bekannte untere Schranke für PARITY in Booleschen Schaltkreisen verwendet, um die in dieser Arbeit vorgestellten Lokalitätsergebnisse nachzuweisen.

**Definition 4.1.** Für eine Zahl $m \in \mathbb{N}$ sei $\text{PARITY}_{2m} : \{0,1\}^{2m} \to \{0,1\}$ eine Funktion, so dass $\text{PARITY}_{2m}(w) = 1$ genau dann wenn $|w|_1$ gerade ist.

Das Problem ist bekanntermaßen nicht in $\text{AC}^0$ berechenbar:

**Theorem 4.2** (nach Furst, Saxe und Sipser 1984 [5, 3, 1])**.** *Es existiert keine Schaltkreisfamilie konstanter Tiefe und polynomieller Größe, die* PARITY *berechnet.*

Zum Nachweis der Lokalität wird eine verstärkte Variante dieses Theorems verwendet. Bereits das Promise-Problem, das PARITY auf Eingaben $w \in \{0,1\}^{2m}$ mit $|w|_1 \in \{m, m+1\}$ berechnen soll, ist nicht in $\text{AC}^0$ entscheidbar, und es wurde eine präzise untere Schranke für die Größe jedes solchen Schaltkreises definiert.

**Theorem 4.3** (implizit in Håstad 1987 [8], zitiert aus [2])**.** *Für jede Tiefe $d \in \mathbb{N}$ existieren Schranken $c, m_0 \in \mathbb{N}_{>0}$, so dass für alle $m \geqslant m_0$ der kleinste Schaltkreis $\mathcal{C}_{2m}$ mit Tiefe $d$, der alle Wörter $w \in \{0,1\}^{2m}$ mit $|w|_1 = m$ akzeptiert und alle mit $|w|_1 = m+1$ ablehnt, mindestens die Größe $2^{c \cdot \sqrt[d-1]{m}}$ hat (kurz: $|\mathcal{C}_{2m}| \in 2^{\Omega(\sqrt[d-1]{m})}$).*

## 4.4 $\text{Mod}_q$ und der Satz von Razborov und Smolensky:

Das $\text{MOD}_q$-Problem ist eine Verallgemeinerung des PARITY-Problems für beliebige Zahlen $q \in \mathbb{N}$. Während $\text{MOD}_2$ genau das PARITY-Problem ist, gilt allgemein folgendes:

**Definition 4.4.** Für jede natürliche Zahl $q \in \mathbb{N}$ ist $\text{MOD}_q : \{0,1\}^* \to \{0,1\}$ eine Funktion, so dass $\text{MOD}_q(w) = 1$ genau dann wenn $|w|_1$ ein Vielfaches von $q$ ist.

Während $\text{MOD}_q$ durch eine triviale $\oplus^q$-Familie berechnet werden kann, gibt es allgemein keine Möglichkeit, durch einen kleinen Schaltkreis aus $p$-Zählgattern ein Zählgatter für eine andere Zahl $q \neq p$ zu ersetzen: Hier nach der Formulierung von Smolensky:

**Theorem 4.5** (nach Smolensky 1987 [3, 12, 14])**.** *Sei $p \in \mathbb{N}$ eine Primzahl und $q \in \mathbb{N}$ eine natürliche Zahl, die keine Potenz $p^i$ ist*[2]*. Für jedes $d \in \mathbb{N}$ hat jede $\oplus^p$-Schaltkreisfamilie $(\mathcal{C}_m)_{m\in\mathbb{N}}$ mit Tiefe $d$, die $\text{MOD}_q$ berechnet, mindestens die Größe $2^{\Omega(\sqrt[2d]{m})}$. Präzise existieren also $c, m_0 \in \mathbb{N}_{>0}$, so dass $|\mathcal{C}_{2m}| \geqslant 2^{c\cdot\sqrt[2d]{m}}$ für alle $m \geqslant m_0$ gilt.*

Diese Schranke wird genutzt, um ein Lokalitätsergebnis für die Klasse $\text{FO+MOD}_p$ zu erhalten.

[2] Für diese Arbeit reicht bereits aus, dass das Theorem für alle Paare $p, q \in \mathbb{N}$ von verschiedenen Primzahlen $p \neq q$ gilt.

# 5 Lokalität der arb-invarianten FO [arb]-Logik

Das folgende Theorem wird bewiesen.

**Theorem 5.1** (nach Anderson, van Melkebeek, Schweikardt und Segoufin, 2011[2]). *Gaifman-Lokalität von FO* [**arb**]*:*

*Für jede Formel $\varphi \in FO\,[\mathbf{arb}]$ mit Alternierungstiefe $d$, und für jede Konstante $c > d + 3$, existiert eine Schranke $n_{\varphi,c} \in \mathbb{N}_{>0}$, so dass die Formel auf allen Graphen $\mathfrak{A}$ der Größe $n \geqslant n_{\varphi,c}$* ***Gaifman-lokal*** *mit dem Radius $(\log n)^c$ ist, auf denen sie auch arb-invariant ist.*

Insbesondere ist jede arb-invariante Formel $\varphi$ dann $(\log n)^c$-lokal für $c > d + 3$.

Die Konstruktion des Beweises wird erheblich leichter, wenn wir die Allgemeinheit auf Formeln mit einer einzigen freien Variable einschränken. Zunächst wird dieser Fall betrachtet. Später wird eine Reduktion skizziert, die den Beweis auf mehrstellige Formeln ausweitet.

## 5.1 Unäre Formeln

Aus einer vorausgesetzten einstelligen Formel mit Alternierungstiefe $d$, die arb-invariant aber für einen gegebenen Parameter $m \in \mathbb{N}$ nicht $10m$-lokal auf einem Graphen der Größe $n$ ist, wird durch eine Fallunterscheidung die Existenz eines Schaltkreises $\mathcal{C}_{2m}$ mit Tiefe $d + 4$ und Größe $n^{\|\varphi\|}$ gefolgert, der alle Eingaben $w \in \{0,1\}^{2m}$ mit $|w|_1 = m$ annimmt und alle mit $|w|_1 = m + 1$ ablehnt.

Aus dem Lemma von Håstad folgt, dass eine Schranke $c \in \mathbb{N}$ existiert, so dass die Größe eines solchen Schaltkreises mindestens $2^{c\cdot\left(\sqrt[d+3]{m}\right)}$ für jedes $m \in \mathbb{N}$ ist. Für hinreichend große Werte von $m$ wird daher ein Widerspruch folgen [2].

In den folgenden beiden Abschnitten werden die Details hierzu ausgeführt.

### 5.1.1 Fallunterscheidung über die Form der Umgebungen

**Satz 5.2.** *Sei $\mathfrak{A}$ ein Graph mit $\left(\mathcal{N}_r^{\mathfrak{A}}(a), a\right) \cong \left(\mathcal{N}_r^{\mathfrak{A}}(b), b\right)$ für ein $r \geqslant 10m$, und $\varphi(x)$ eine bezüglich $\mathfrak{A}$ arb-invariante FO [**arb**]-Formel mit Alternierungstiefe $d$, so dass $\mathfrak{A} \models \varphi(a)$ und $\mathfrak{A} \not\models \varphi(b)$.*

*Dann existiert ein Schaltkreis $\mathcal{C}'_{2m}$ der Tiefe $d+4$ und Größe $n^{\|\varphi\|}$, der die Eingabe $w \in \{0,1\}^{2m}$ annimmt falls $|w|_1 = m$, und ablehnt falls $|w|_1 = m+1$.*

*Beweis.* Sei $\pi : \mathcal{N}_r^{\mathfrak{A}}(a) \cong \mathcal{N}_r^{\mathfrak{A}}(b)$ ein Isomorphismus mit $\pi(a) = b$.

Eine Schaltkreisfamilie $(\mathcal{C}_n^{\varphi})_{n\in\mathbb{N}}$ mit Tiefe $d+4$ und polynomieller Größe $n^{\|\varphi\|}$ kann nach **Theorem 3.1** die Formel $\varphi$ auswerten. Durch eine Fallunterscheidung wird aus $\mathcal{C}^{\varphi}_{n^2+n}$ nun $\mathcal{C}'_{2m}$ konstruiert. □

*Fall* 1. $\operatorname{dist}(a,b) > 4m$

Falls $a$ und $b$ mindestens die Distanz $4m+1$ voneinander haben, sind ihre $2m$-Umgebungen disjunkt. Konstruiere dann $\mathfrak{A}_w = \texttt{switch}(\mathfrak{A}, a, b, w)$ gemäß **Abschnitt 4.1**, und erzeuge den Schaltkreis $\mathcal{C}'_{2m}$, der $[\![\varphi(a)]\!]^{\mathfrak{A}_w}$ berechnet. Dieser Schaltkreis akzeptiert $w$ genau dann wenn $|w|_1$ gerade ist. Falls $m$ gerade ist, werden alle Worte mit $|w|_1 = m$ angenommen, und alle mit $|w|_1 = m+1$ abgelehnt. (Ist $m$ ungerade, so verwende man einfach $\neg\varphi$ anstatt $\varphi$.)

*Fall* 1. $\operatorname{dist}(a,b) \leqslant 4m$, aber $\operatorname{dist}\left(a, \pi^i(a)\right) > 8m$ für ein $i > 1$.

Sei $i$ minimal, so dass $\operatorname{dist}\left(a, \pi^j(a)\right) \leqslant 8m < r$ für $j < i$ , und daher $\pi^j(a) \in \operatorname{Def}(\pi)$).

Per Definition ist $\operatorname{dist}\left(a, \pi^i(a)\right) > 8m > 4m$, und es folgt auch $\operatorname{dist}\left(b, \pi^i(a)\right) \geqslant \operatorname{dist}\left(a, \pi^i(a)\right) - \operatorname{dist}(a,b) > 4m$.

Außerdem ist $\mathcal{N}^{\mathfrak{A}}_{2m}\left(\pi^{i-1}(a)\right) \subseteq \mathcal{N}^{\mathfrak{A}}_{10m}(a)$, und daher muss $\mathcal{N}^{\mathfrak{A}}_{2m}\left(\pi^{i-1}(b)\right) \subseteq \mathcal{N}^{\mathfrak{A}}_{10m}(b)$ sein. Es gilt:

$$\mathcal{N}^{\mathfrak{A}}_{2m}(a) \cong \mathcal{N}^{\mathfrak{A}}_{2m}(\pi(a)) \cong \cdots \cong \mathcal{N}^{\mathfrak{A}}_{2m}\left(\pi^{i-1}(a)\right) \cong \mathcal{N}^{\mathfrak{A}}_{2m}\left(\pi^{i-1}(b)\right) = \mathcal{N}^{\mathfrak{A}}_{2m}\left(\pi^{i}(a)\right)$$

*Fall* 1. $\left(\mathfrak{A}, \pi^i(a)\right) \models \varphi$.

Dann wähle die disjunkten isomorphen Umgebungen $\mathcal{N}^{\mathfrak{A}}_{2m}\left(\pi^i(a)\right)$ und $\mathcal{N}^{\mathfrak{A}}_{2m}(b)$. Konstruiere gemäß **Abschnitt 4.1** den Schaltkreis $\mathcal{C}'_{2m}$, der $[\![\varphi\left(\pi^i(a)\right)]\!]^{\mathfrak{A}_w}$ berechnet.

*Fall* 1. $\left(\mathfrak{A}, \pi^i(a)\right) \not\models \varphi$.

Dann wähle die disjunkten isomorphen Umgebungen $\mathcal{N}^{\mathfrak{A}}_{2m}(a)$ und $\mathcal{N}^{\mathfrak{A}}_{2m}\left(\pi^i(a)\right)$. Konstruiere $\mathfrak{A}_w = \texttt{switch}\left(\mathfrak{A}, a, \pi^i(a), w\right)$. Der Schaltkreis $\mathcal{C}'_{2m}$ soll nun $\varphi(a)$ auf $\mathfrak{A}_w$ auswerten.

*Fall* 1. $\operatorname{dist}\left(a, \pi^i(a)\right) \leqslant 8m$ für alle $i \in \mathbb{N}$.

Dann sei $\mathcal{U} = \left\{\pi^i(a) \ : \ i \in \mathbb{N}\right\}$ die Bahn der Elemente, die durch die wiederholte Anwendung von $\pi$ erzeugt wird.

Nun betrachte die Schalen $S_i^{\mathfrak{A}}(\mathcal{U})$ für $i \in [2m]$. Da $\pi : \mathcal{N}^{2m}_{\mathfrak{A}}\left(\pi^j\right) \cong \mathcal{N}^{2m}_{\mathfrak{A}}\left(\pi^{j+1}\right)$ für alle $j \in \mathbb{N}$ ein Isomorphismus ist, gilt $\operatorname{dist}\left(\pi^i(a), \pi^i(c)\right) = \operatorname{dist}(a,c)$ für

$c \in S_{\mathfrak{A}}^{2m}(a)$; die Schalen sind also unter $\pi$ abgeschlossen. Damit sind die Voraussetzungen für die Schalenrotation gemäß **Abschnitt 4.2** erfüllt; konstruiere $\mathfrak{A}_w = \texttt{rotate}(\mathfrak{A}, a, w)$.

Bilde einen Schaltkreis $\mathcal{C}'_{2m}$, der $[\![\varphi(\pi^{-m}(a))]\!]^{\mathfrak{A}_w}$ berechnet.

### 5.1.2 Erzeugung des Widerspruchs

*Behauptung.* Für alle unären FO [**arb**]-Formeln $\varphi(x)$ mit Alternierungstiefe $d \in \mathbb{N}$ und alle $c > d+3$ existiert ein $n_0 \in \mathbb{N}$, so dass für jeden Graphen $\mathfrak{A}$ der Größe $n \geqslant n_0$ gilt: Ist $\varphi(x)$ auf $\mathfrak{A}$ arb-invariant, so hält $\varphi$ auf $\mathfrak{A}$ einen Lokalitätsradius von $(\log n)^c$ ein.

*Beweis.* Angenommen, es existiere eine Formel $\varphi(x)$ mit Alternierungstiefe $d$, und ein $c > d+3$ so dass $\varphi$ für jedes $n_0 \in \mathbb{N}$ in einem Graphen $\mathfrak{A}$ der Größe $n \geqslant n_0$ arb-invariant ist, und zwischen zwei Elementen $a, b \in A$ mit isomorphen $(\log n)^c$-Umgebungen unterscheidet.

Nach **Theorem 3.1** kann $\varphi$ durch eine Schaltkreisfamilie mit einer festen Tiefe $d+4 \in \mathbb{N}$ und Größe $n^{\|\varphi\|}$ berechnet werden.

Sei nun $m := \left\lfloor \frac{(\log n)^c}{10} \right\rfloor$, so dass gemäß **Satz 5.2** ein Schaltkreis $\mathcal{C}'_{2m}$ mit der Tiefe $d+4$ und der Größe $n^{\|\varphi\|}$ zwischen allen Eingaben mit $|w|_1 = m$ und $|w|_1 = m+1$ unterscheidet. Nach **Theorem 4.3** existiert eine nur von $d+4$ abhängige Konstante $\alpha \in \mathbb{N}_{>0}$, so dass $n^{\|\varphi\|} \geqslant 2^{\alpha \cdot \left(\sqrt[d+3]{m}\right)}$ gilt.

Daher folgt für alle $n, c \in \mathbb{N}$:

$$\begin{aligned}
n^{\|\varphi\|} &\geqslant 2^{\alpha \cdot \left(\sqrt[d+3]{m}\right)} \\
\Longrightarrow \|\varphi\| (\log n) &\geqslant \alpha \cdot \left(\sqrt[d+3]{m}\right) \\
\Longrightarrow \frac{\|\varphi\|}{\alpha} (\log n) &\geqslant \sqrt[d+3]{\frac{(\log n)^c}{10}} = \frac{(\log n)^{\frac{c}{d+3}}}{\sqrt[d+4]{10}} \\
\Longrightarrow \frac{\|\varphi\| \sqrt[d+3]{10}}{\alpha} &\geqslant (\log n)^{\frac{c}{d+3}-1}
\end{aligned}$$

Da $c > d+3$ ist, folgt $\frac{c}{d+3} - 1 > 0$, und $(\log n)^{\frac{c}{d+3}-1}$ wird für hinreichend große Werte von $n$ unbeschränkt groß. ↯ □

## 5.2 Mehrstellige Formeln

Nach dem die Lokalität aller einstelligen Formeln nachgewiesen ist, soll der Beweis auf mehrstellige Formeln erweitert werden. Bei disjunkte Umgebungen

(die schwache Gaifman-Lokalität) kann mit wenig Mühe die Operation aus **Abschnitt 4.1** angepasst werden.

Für allgemeine Umgebungen (die starke Gaifman-Lokalität) wird eine Reduktion aufgestellt, um von der Existenz einer $k$-stelligen Formel $\varphi$ auf die Existenz einer $k'$-stelligen Formel $\varphi'$ mit $k' < k$ zu schließen, deren Lokalitätsradius nicht viel kleiner ist.

### 5.2.1 Disjunkte Umgebungen

Es wird analog zu **Satz 5.2** ein PARITY-Schaltkreis hergeleitet, der die untere Schranke aus **Theorem 4.2** verletzt.

**Satz 5.3.** *Sei $\varphi$ eine $k$-stellige FO [**arb**]-Formel mit Alternierungstiefe $d \in \mathbb{N}$. Sei $\mathfrak{A}$ ein Graph hinreichender Größe $n$, so dass $\varphi$ zwischen zwei Tupeln $\bar{a}, \bar{b} \in A^k$ mit $\left(\mathcal{N}_{2m}^{\mathfrak{A}}(\bar{a}), \bar{a}\right) \cong \left(\mathcal{N}_{2m}^{\mathfrak{A}}\left(\bar{b}\right), \bar{b}\right)$ (für $m \in \mathbb{N}$) unterscheidet:*

$$\mathfrak{A} \models \varphi(\bar{a}) \quad \text{und} \quad \mathfrak{A} \not\models \varphi\left(\bar{b}\right)$$

*So existiert ein Schaltkreis $\mathcal{C}'_{2m}$ mit der Tiefe $d+4$ und Größe $n^{\|\varphi\|}$, der für $w \in \{0,1\}^{2m}$ die* PARITY*-Funktion berechnet:*

$$w \models \mathcal{C}'_{2m} \iff |w|_1 \equiv 0 \mod 2$$

*Beweis.* Per **Theorem 3.1** existiert ein Schaltkreis $\mathcal{C}^{\varphi}_{n^2+kn}$ mit der Tiefe $d+4$ und der Größe $n^{\|\varphi\|}$, so dass $\mathrm{enc}(\mathfrak{A}, \bar{a}) \models \mathcal{C}^{\varphi}_{n^2+n}$ und $\mathrm{enc}\left(\mathfrak{A}, \bar{b}\right) \not\models \mathcal{C}^{\varphi}_{n^2+kn}$.

Die `switch`-Operation aus **Abschnitt 4.1** wird angepasst, um aus $\mathcal{C}^{\varphi}_{n^2+kn}$ den Schaltkreis $\mathcal{C}'_{2m}$ zu erzeugen.

Die $2m$-Kugeln um $\bar{a}, \bar{b}$ werden in Schalen partitioniert:

$$\begin{aligned} N_{2m}^{\mathfrak{A}}(\bar{a}) &= \dot{\bigcup}_{i=0}^{2m} S_i^{\mathfrak{A}}(\bar{a}) \\ N_{2m}^{\mathfrak{A}}\left(\bar{b}\right) &= \dot{\bigcup}_{i=0}^{2m} S_i^{\mathfrak{A}}\left(\bar{b}\right) \end{aligned}$$

Der Isomorphismus wird zur selbst-inversen Funktion $\pi_{\leftrightarrows} : N_{2m}^{\mathfrak{A}}\left(\bar{a}, \bar{b}\right) \to N_{2m}^{\mathfrak{A}}\left(\bar{a}, \bar{b}\right)$ erweitert:

$$\pi_{\leftrightarrows}(x) := \begin{cases} \pi(x) & \text{falls } x \in N_{2m}^{\mathfrak{A}}(\bar{a}) \\ \pi^{-1}(x) & \text{sonst} \end{cases}$$

Die folgenden Kantenmengen werden definiert:

$$\begin{aligned}
\mathcal{X}_i &:= \left(S^{\mathfrak{A}}_{i-1}(\bar{a}) \times S^{\mathfrak{A}}_{i}(\bar{a})\right) \cup \\
&\quad \left(S^{\mathfrak{A}}_{i}(\bar{a}) \times S^{\mathfrak{A}}_{i-1}(\bar{a})\right) \cup \\
&\quad \left(S^{\mathfrak{A}}_{i-1}(\bar{b}) \times S^{\mathfrak{A}}_{i}(\bar{b})\right) \cup \\
&\quad \left(S^{\mathfrak{A}}_{i}(\bar{b}) \times S^{\mathfrak{A}}_{i-1}(\bar{b})\right) \\
\mathcal{Y}_i &:= \left\{(x, \pi_{\leftrightarrows}(y)) \;:\; (x,y) \in \mathcal{X}_i \cap E^{\mathfrak{A}}\right\}
\end{aligned}$$

Die Operation $\texttt{switch}(\mathfrak{A}, w)$ sei nun wie folgt definiert:

$$\begin{aligned}
\texttt{switch}(\mathfrak{A}, w) &:= \left(E^{\mathfrak{A}} \Big\backslash \bigcup_{\substack{i=1 \\ w_i=1}}^{2m} \mathcal{X}_i\right) \cup \bigcup_{\substack{i=1 \\ w_i=1}}^{2m} \mathcal{Y}_i \\
\mathfrak{A}_w &:= (A, \texttt{switch}(\mathfrak{A}, w))
\end{aligned}$$

Analog zu den unären $r$-Umgebungen gilt $(\mathfrak{A}_w, \bar{a}) \cong (\mathfrak{A}, \bar{a})$ genau dann wenn $|w|_1 \equiv 0 \mod 2$, und sonst $(\mathfrak{A}_w, \bar{a}) \cong (\mathfrak{A}_w, \bar{b})$.

Sei $\mathcal{C}^{\varphi}_{n^2+kn} = (G, f, x)$ der Schaltkreis und $g : A \to [n]$ eine beliebige Aufzählung von $A$. Dann sei $\mathcal{C}'_{2m} = (G, f', x)$ wie folgt:

$$f'(v) := \begin{cases}
f(v) & \text{falls } f(v) \in \{\mathbf{0}, \mathbf{1}, \wedge, \vee\} \\
\overline{I_i} & \text{falls } f(v) = I_{n\cdot g(x)+g(y)},\ (x,y) \in E^{\mathfrak{A}} \cap \mathcal{X}_i \\
& \text{oder } f(v) = \overline{I_{n\cdot g(x)+g(y)}},\ (x,y) \in \mathcal{Y}_i \\
I_i & \text{falls } f(v) = I_{n\cdot g(x)+g(y)},\ (x,y) \in \mathcal{Y}_i \\
& \text{oder } f(v) = \overline{I_{n\cdot g(x)+g(y)}},\ (x,y) \in E^{\mathfrak{A}} \cap \mathcal{X}_i \\
\mathbf{1} & \text{sonst, falls } f(v) = I_j,\ (\mathrm{enc}_g(\mathfrak{A}, \bar{a}))_j = 1 \\
\mathbf{0} & \text{sonst}
\end{cases}$$

Der Schaltkreis $\mathcal{C}'_{2m}$ berechnet dann $[\![\mathcal{C}'_{2m}]\!]^w = \left[\!\!\left[\mathcal{C}^{\varphi}_{n^2+kn}\right]\!\!\right]^{\mathrm{enc}_g(\mathfrak{A}_w, \bar{a})}$, und es gilt $w \models \mathcal{C}'_{2m}$ genau dann wenn $|w|_1 \equiv 0 \mod 2$. □

*Behauptung.* Für alle $k$-stelligen FO [**arb**]-Formeln $\varphi(\bar{x})$ und alle $c > d + 3$ existiert ein $n_0 \in \mathbb{N}$, so dass für jeden Graphen $\mathfrak{A}$ der Größe $n \geqslant n_0$ gilt: Ist $\varphi(x)$ auf $\mathfrak{A}$ arb-invariant, so hält $\varphi$ auf $\mathfrak{A}$ einen schwachen Lokalitätsradius von $(\log n)^c$ ein.

*Beweis.* Durch Widerspruch. Sei $\varphi$ eine $k$-stellige FO [**arb**]-Formel mit der Alternierungstiefe $d$. Angenommen, es existiere ein $c > d+3$ und für jede Schranke $n_0 \in \mathbb{N}$ ein Graph $\mathfrak{A}$ der Größe $n \geqslant n_0$, und zwei Tupel $\bar{a}, \bar{b} \in A^k$ mit $\left(\mathcal{N}_{2m}^{\mathfrak{A}}(\bar{a}), \bar{a}\right) \cong \left(\mathcal{N}_{2m}^{\mathfrak{A}}\left(\bar{b}\right), \bar{b}\right)$ und $\mathcal{N}_{2m}^{\mathfrak{A}}(\bar{a}) \cap \mathcal{N}_{2m}^{\mathfrak{A}}\left(\bar{b}\right) = \emptyset$ (für $2m = \lfloor (\log n)^c \rfloor$), so dass $\varphi$ zwischen $\bar{a}$ und $\bar{b}$ unterscheidet.

Per **Satz 5.3** existiert ein Schaltkreis $\mathcal{C}'_{2m}$ der Tiefe $d+4$ und Größe $n^{\|\varphi\|}$, der PARITY berechnet.

Nach **Theorem 4.3** von Håstad muss für hinreichend große $m \geqslant m_0$ eine von $d+4$ abhängige Konstante $\alpha \in \mathbb{N}$ existieren, so dass ein solcher Schaltkreis mindestens die Größe $2^{\alpha \cdot \left(\sqrt[d+3]{m}\right)}$ besitzt. Es gilt also:

$$\begin{aligned}
n^{\|\varphi\|} &\geqslant 2^{\alpha\left(\sqrt[d+3]{m}\right)} \\
\Longrightarrow \|\varphi\| (\log n) &\geqslant \alpha \left(\sqrt[d+3]{m}\right) \\
\Longrightarrow \frac{\|\varphi\|}{\alpha} (\log n) &\geqslant \sqrt[d+3]{\frac{(\log n)^c}{2}} \\
\Longrightarrow \frac{\|\varphi\|}{\alpha} (\log n) &\geqslant \frac{(\log n)^{\frac{c}{d+3}}}{\sqrt[d+3]{2}} \\
\Longrightarrow \frac{\|\varphi\| \sqrt[d+3]{2}}{\alpha} &\geqslant (\log n)^{\frac{c}{d+3}-1}
\end{aligned}$$

Aus der Annahme $c > d+3$ folgt dann ein Widerspruch. □

### 5.2.2 Nicht-disjunkte Umgebungen

Um die starke Gaifman-Lokalität nachzuweisen, wird eine logische Reduktion aufgestellt. Die logische Reduktion erweitert GRAPH um zusätzliche Prädikate; daher müssen **Theorem 3.1** und **Theorem 5.1** um das folgende Korollar auf allgemeine relationalen Strukturen erweitert werden:

**Korollar.** *Für alle endlichen Signaturen $\sigma$ sind alle FO $[\sigma \cup \sigma_{arb}]$-Formeln durch Schaltkreisfamilien in $AC^0$ entscheidbar, und auch $(\log n)^c$-lokal.*

Die in **Kapitel 4** vorgestellten Methoden zur Kodierung und Umformung von Graphen können entsprechend erweitert werden (hier ohne formalen Beweis), so dass der vorgestellte Beweis auch für allgemeine relationale Strukturen gilt.

Die Reduktion wird durch das folgende Lemma formalisiert:

**Lemma 5.4** (nach Anderson et al 2012 [2])**.** *Sei $\varphi$ eine FO $[\sigma \cup \sigma_{arb}]$-Formel der Stelligkeit $k \in \mathbb{N}$ und Alternierungstiefe $d \in \mathbb{N}$, die auf einer $\sigma$-Struktur $\mathfrak{A}$ arb-invariant ist und für den Radius $r \in \mathbb{N}$ zwei Tupel $\bar{a}, \bar{b} \in A^k$ mit isomorphen $r$-Umgebungen unterscheidet.*

$$\pi : \mathcal{N}_r^{\mathfrak{A}}(\bar{a}) \cong \mathcal{N}_r^{\mathfrak{A}}\left(\bar{b}\right)$$

$$\mathfrak{A} \models \varphi(\bar{a}) \quad \textit{und} \quad \mathfrak{A} \not\models \varphi(\bar{b})$$

*So existiert eine FO*[**arb**]*-Formel* $\varphi'$ *mit Stelligkeit* $k' < k$*, die auf einer erweiterten* $\sigma'$*-Struktur (mit* $\sigma' \supseteq \sigma$*)* $\mathfrak{A}'$ *arb-invariant ist und zwischen zwei Tupeln* $\bar{a}', \bar{b}' \in A^{k'}$ *mit isomorphen* $r'$*-Umgebungen unterscheidet, wobei* $\frac{r}{r'} \in \mathcal{O}(k)$*.*

Daher folgt aus einer $k$-stelligen Formel, die für ein festes $c \in \mathcal{O}(k!)$ zwei isomorphe $c \cdot (\log n)^{d+4}$-Umgebungen unterscheidet, eine unäre Formel, die isomorphe $(\log n)^{d+4}$-Umgebungen unterscheidet, im Widerspruch zu **Abschnitt 5.1**.

Die Fallunterscheidung des Beweises wird skizziert. Mehrfach werden dabei die Begriffe von "weiter Entfernung" und "Nähe" verwendet, die hier nicht durch präzise Radien konkretisiert werden.

*Fall* 1. Die Tupel haben eine Komponente $a_i = b_i$ gemeinsam. Dann kann durch eine neue Relation $\dot{R}^{\mathfrak{A}'} := \{a_i\}$ und die Formel $\exists x_i \left(\dot{R}(x_i) \wedge \varphi\right)$ die Stelligkeit auf $k-1$ reduziert werden, ohne den Lokalitätsradius zu verändern.

*Fall* 2. Alle Komponenten $a_i$ besitzen in $\pi$ eine kleine geschlossene Umlaufbahn $\mathcal{U} = \left\{\pi^t(a_i) \,:\, t \in \mathbb{N}\right\}$. Dann haben alle $\pi^t(\bar{a})$ isomorphe $r'$-Umgebungen, wobei $r'$ nicht viel kleiner ist als $r$.

Per Ausschluss von Fall 1 gilt $a_1 \neq \pi^t(a_1)$ oder $\mathfrak{A} \not\models \varphi\left(\pi^t(\bar{a})\right)$ für alle $t > 0$. Daher wird jedes erfüllende Tupel $\pi^t(\bar{a})$ eindeutig durch $\pi^t(a_1)$ identifiziert. Durch eine neue Relation $\dot{R}^{\mathfrak{A}} := \left\{\pi^t(\bar{a}) \,:\, t \in \mathbb{N}\right\}$ kann die Stelligkeit wie folgt auf 1 reduziert werden.

$$\varphi'(x_1) := \exists x_2 \cdots \exists x_k \ \left(\dot{R}(\bar{x}) \wedge \varphi\right)$$

*Fall* 1. Die Formel $\varphi$ unterscheidet zwischen Tupeln $\bar{a}, \bar{b}$ mit isomorphen $r$-Umgebungen, die Komponenten von $\bar{a}$ liegen nah zusammen, und $a_i$ und $b_i$ (o.B.d.A. $i = 1$) sind einander fern.

Dann sind $\bar{a}$ und $\bar{b}$ voneinander hinreichend fern, sodass die Relation $\dot{R}^{\mathfrak{A}} := \left\{\bar{a}, \bar{b}\right\}$ den Isomorphismus $\pi$ auf einer kleineren $r'$-Umgebung von $\bar{a}$ und $\bar{b}$ nicht zerstört. Die gleiche Formel wie in Fall 2 unterscheidet zwischen $a_1$ und $b_1$.

*Fall* 2. Einige Komponenten $\bar{a}$ sind weit voneinander entfernt, und $b_i$ (o.B.d.A. $i = 1$) ist weit von $\bar{a}$. Ordne das Tupel nach Distanz von $a_1$ und trenne $\bar{a} = \bar{a'} \cdot \bar{a''}$ sowie $\bar{b} = \bar{b'} \cdot \bar{b''}$, so dass $\bar{b'}$ fern von $\bar{b''}$ und fern von $\bar{a''}$ liegt.

Eine Abbildung $\pi'$, die in der Nähe von $\bar{b'}$ alle Elemente auf sich selbst abbildet, und in der Nähe von $\bar{a''}$ wie $\pi$ funktioniert, ist dann auf einer kleineren $r'$-Umgebung von $\bar{b'} \cdot \bar{a''}$ ein Isomorphismus.

In diesem Fall unterscheidet $\varphi$ zwischen den isomorphen $r'$-Umgebungen von $\bar{b'} \cdot \bar{a''}$ und $\bar{b'} \cdot \bar{b''}$, und die gemeinsamen Komponenten können gemäß Fall 1 entfernt werden.

## 5.3 Untere Schranke

**Theorem 5.5.** *Für jede Konstante $c \in \mathbb{N}$ existiert eine unäre FO [**arb**]-Formel $\varphi_c$, die auf einem Graphen $\mathfrak{A}$ mit Größe $n$ arb-invariant ist, aber zwischen $a, b \in A$ mit $\mathcal{N}_m^{\mathfrak{A}}(a) \cong \mathcal{N}_m^{\mathfrak{A}}(b)$ und $m = (\log n)^c$ unterscheidet.*

Damit hat jede Formel zwar eine polylogarithmische Lokalität, aber keine solche Schranke gilt für alle Formeln.

Zum Nachweis sei $c \in \mathbb{N}$ beliebig. Nun soll $\varphi_c$ in allen Graphen mit höchstens $(\log n)^{c+1}$ nicht-isolierten Knoten alle Knoten ausgeben, die über einen Weg beliebiger Länge von einer $K_3$-Klique aus erreichbar sind.

**Lokalität:** Sei $\mathfrak{A}$ ein Graph hinreichender Größe $n \in \mathbb{N}$, der aus zwei disjunkten Pfaden $\bar{a}, \bar{b}$ der Länge $(\log n)^c + 1$ besteht, wobei nur das Ende von $\bar{a}$ mit einer $K_3$-Klique verbunden ist. Die übrigen $n - 2\left((\log n)^c + 1\right) - 3$ Knoten seien isolierte Knoten ohne Kanten. In diesem Graph unterscheidet die Formel zwischen den isomorphen $(\log n)^c$-Umgebungen von $a_1$ und $b_1$.

**Konstruktion:** Jede Sequenz von maximal $m = (\log n)^{c+1}$ nicht-isolierten Knoten kann durch ein Tupel $[m]^m$ repräsentiert werden. Die logarithmische Schranke sorgt dafür, dass $|m^m| < n^k$ ist, und daher jeder mögliche Weg durch ein Tupel $\bar{a} \in A^k$ repräsentiert werden kann. Daher können alle möglichen Wege quantisiert werden; eine Formel kann prüfen, ob ein gegebenes Tupel $\bar{a} \in A^k$ einen gültigen Weg kodiert.

Die Schranke von $(\log n)^{c+1}$ nicht-isolierten Knoten kann ebenfalls als Formel formuliert werden.

# 6 Erweiterung des Resultats auf arb-invariante FO + MOD$_p$-Logik

Das folgende Theorem wird bewiesen:

**Theorem 6.1** (nach Straubing 1995 [15, 16])**.** *Charakterisierung von* $(FO + MOD_p)$ [**arb**] *durch* $ACC^0$ $[p]$*.*

1. *Sei* $p \in \mathbb{N}$ *eine Primzahl und* $\varphi(\bar{x})$ *eine* $k$*-stellige* $(FO + MOD_p)$ [**arb**]*-Formel (o.B.d.A. in Pränexnormalform) mit* $d \in \mathbb{N}$ *Quantoren. Dann existiert eine* $\oplus^p$*-Schaltkreisfamilie* $(\mathcal{C}_{n^2+kn})_{n\in\mathbb{N}}$ *konstanter Tiefe* $d+4$ *und der Größe* $n^{\|\varphi\|}$*, so dass für jeden Graphen* $\mathfrak{A}$ *der Größe* $n$*, jede Belegung* $\bar{a} \in A^k$ *von* $\varphi$ *und jede Ordnungs-Erweiterung* $\mathfrak{A}_f$ *gilt:*

$$\mathfrak{A}_f \models \varphi(\bar{a}) \iff enc_f(\mathfrak{A}, \bar{a}) \models \mathcal{C}_{n^2+kn}$$

*Insbesondere wird die Auswertung einer arb-invariante Formel* $\varphi$ *über jeder Struktur* $\mathfrak{A}$ *unabhängig von der gewählten Kodierung* $enc_f(\mathfrak{A}, \bar{a})$ *korrekt durch* $\mathcal{C}_{n^2+kn}$ *berechnet.*

## 6.1 Formel zu Schaltkreissequenz

### 6.1.1 Normalform

Ohne Beschränkung der Annahme sei die Formel $\varphi$ in disjunktiver Pränexnormalform.

$$\begin{aligned} \varphi(x_1, \cdots, x_k) &= Q_1 y_1 \cdots Q_d y_d \psi \\ Q_1, \cdots, Q_d &\in \left\{\exists, \forall, \exists^{(p,i)} \ : \ 0 \leqslant i < d\right\} \\ \psi(x_1, \cdots, x_k, y_1, \cdots, y_d) &= \bigvee_{i=1}^{m} \bigwedge_{j=1}^{m_i} \psi_{i,j} \end{aligned}$$

Die Formeln $\psi_{i,j}$ haben die Form $u = v$, $\neg u = v$, $E(u, v)$, $\neg E(u, v)$, $\dot{R}(\bar{t})$ oder $\neg\dot{R}(\bar{t})$ für $R \subseteq \mathbb{N}^k$.

### 6.1.2 Rekursionsanfang

Sei $n \in \mathbb{N}$ beliebig. Für $\psi(x_1, \cdots, x_k, y_1, \cdots, y_d)$ und $t \in [n]^{k+d}$ wird der Schaltkreis $\mathcal{D}_\psi^t$ entsprechend **Abschnitt 3.1.2** definiert.

### 6.1.3 Rekursionsschritt

Sei $\psi(x_1, \cdots, x_k, y_1, \cdots, y_i)$ eine Formel in Pränexnormalform mit $d \in \mathbb{N}$ Quantoren, so dass für alle $\bar{t} \in [n]^{k+i}$ ein Schaltkreis $\mathcal{D}_\psi^{\bar{t}}$ existiert mit $\left[\!\left[\mathcal{D}_\psi^{\bar{t}}\right]\!\right] = [\![\psi]\!]\left(\mathfrak{A}_f, f^{-1}(\bar{t})\right)$. Die Tiefe des Schaltkreises sei $d+2$, und die Größe sei höchstens $n^d(\|\psi\| + pd)$ Nun sei $\psi'(x_1, \cdots, x_k, y_1, \cdots, y_{i-1}) := Q_i y_i \psi$ und $\bar{t}' \in [n]^{k+i-1}$ beliebig.

*Fall* 1. Sei $Q_i = \exists$. So sei $\mathcal{D}_{\psi'}^{\bar{t}'}$ der folgende Schaltkreis:

$$\mathcal{D}_{\psi'}^{\bar{t}'} = \bigvee_{i=1}^{n} \mathcal{D}_\psi^{\bar{t}' \cdot i}$$

Die Formel $\psi'$ wird von $f^{-1}(\bar{t}')$ und $\mathfrak{A}_f$ erfüllt, genau dann wenn ein $i \in [n]$ existiert, so dass $\psi$ von $f^{-1}(\bar{t}' \cdot i)$ und $\mathfrak{A}_f$ erfüllt wird. Es gilt auch $w \models \mathcal{D}_{\psi'}^{\bar{t}'}$ genau dann wenn ein $i \in [n]$ existiert, so dass $w \models \mathcal{D}_\psi^{\bar{t}' \cdot i}$. Nach der Induktionsannahme ist der Schaltkreis also korrekt. Die Tiefe ist $d+3$, und die Größe ist höchstens $n^{d+1}(\|\psi\| + pd)$.

*Fall* 2. Sei $Q_i = \forall$. So sei $\mathcal{D}_{\psi'}^{\bar{t}'}$ der folgende Schaltkreis:

$$\mathcal{D}_{\psi'}^{\bar{t}'} = \bigwedge_{i=1}^{n} \mathcal{D}_\psi^{\bar{t}' \cdot i}$$

Die Formel $\psi'$ wird von $f^{-1}(\bar{t}')$ und $\mathfrak{A}_f$ erfüllt, genau dann wenn für alle $i \in [n]$ gilt, dass $\psi$ von $f^{-1}(\bar{t}' \cdot i)$ und $\mathfrak{A}_f$ erfüllt wird. Es gilt auch $w \models \mathcal{D}_{\psi'}^{\bar{t}'}$ genau dann wenn für alle $i \in [n]$ gilt, dass $w \models \mathcal{D}_\psi^{\bar{t}' \cdot i}$. Nach der Induktionsannahme ist der Schaltkreis also korrekt, und hat die selbe Tiefe und Größe wie in Fall 1.

*Fall* 3. Sei $Q_i = \exists^{(p,r)}$ für $0 \leqslant r < p$. So sei $\mathcal{D}_{\psi'}^{\bar{t}'}$ der folgende Schaltkreis:

$$\mathcal{D}_{\psi'}^{t'} = \bigoplus{}^{p}\left(\underbrace{\mathcal{D}_\psi^{\bar{t}' \cdot i}}_{i \in [n]}\ ,\ \underbrace{\mathbf{1}}_{p-r}\right)$$

Es folgt für $w = \mathrm{enc}_f(\mathfrak{A}, \bar{a})$:

$$\begin{aligned}
w \models \mathcal{D}_{\psi'}^{\bar{t}'} \quad &\iff \quad \left(\sum_{i=1}^{n} \left[\!\left[\mathcal{D}_\psi^{\bar{t}' \cdot i}\right]\!\right]^w + p - r\right) \equiv 0 \mod p \\
&\iff \quad \sum_{i=1}^{n} \left[\!\left[\mathcal{D}_\psi^{\bar{t}' \cdot i}\right]\!\right]^w \equiv r \mod p \\
&\overset{I.A.}{\iff} \quad \sum_{i=1}^{n} [\![\psi\left(f^{-1}(\bar{t}' \cdot i)\right)]\!]^{\mathfrak{A}_f} \equiv r \mod p \\
&\iff \quad \mathfrak{A} \models \psi'\left(f^{-1}(\bar{t}')\right)
\end{aligned}$$

Also berechnet der Schaltkreis also das korrekte Ergebnis. Seine Tiefe ist $d+3$, und seine Größe ist höchstens

$$n^{d+1}\left(\|\psi\|+pd\right)+p \leqslant n^{d+1}\left(\|\psi\|+p\left(d+1\right)\right)$$

Nach dieser rekursiven Definition existiert allgemein ein Schaltkreis $\mathcal{D}_{\varphi}^{\bar{t}}$ für alle $\bar{t} \in [n]^k$, so dass $w \models \mathcal{D}_{\varphi}^{\bar{t}}$ genau dann wenn $\mathfrak{A}_f \models \varphi\left(f^{-1}\left(\bar{t}\right)\right)$. Der Schaltkreis hat die Tiefe $d+2$ und die Größe $n^d\left(\|\psi\|+pd\right)$.

### 6.1.4 Abschluss

Es wird nun der Schaltkreis $\mathcal{C}_{n^2+kn}$ wie folgt formuliert:

$$\begin{aligned}\mathcal{C}_{n^2+kn} &:= \bigvee_{\bar{t}\in[n]^k}\left(\bigwedge_{i=1}^{k} w_{z(i,t_i)} \wedge \mathcal{D}_{\varphi}^{\bar{t}}\right)\\ z\left(i,t_i\right) &:= n^2+n\cdot\left(i-1\right)+t_i\end{aligned}$$

Die Korrektheit folgt analog zu **Abschnitt 3.1.4**. Der Schaltkreis hat die Tiefe $d+4$ und die Größe $n^{d+k}\left(\|\psi\|+pd\right) \in \mathcal{O}\left(n^{d+k}\right)$.

## 6.2 Umkehrrichtung

Es wurde nachgewiesen, dass jede arb-invariante $(\mathrm{FO}+\mathrm{MOD}_p)\,[\mathbf{arb}]$-Formel äquivalent zu einer Schaltkreisfamilie in $\mathrm{ACC}^0\,[p]$ ist. Umgekehrt gilt auch, dass jede Schaltkreisfamilie in $\mathrm{ACC}^0\,[p]$ äquivalent zu einem $(\mathrm{FO}+\mathrm{MOD}_p)\,[\mathbf{arb}]$-Satz ist:

**Theorem 6.2.** *Sei $(\mathcal{C}_i)_{i\in\mathbb{N}}$ eine $\oplus^p$-Schaltkreisfamilie mit beschränkter Tiefe $d \in \mathbb{N}$ und polynomieller Größe. Dann existiert ein ein $(FO+MOD_p)\,[\mathbf{arb}]$-Satz $\varphi$, so dass für jede Länge $n \in \mathbb{N}$ und jeden Bitstring $w \in \{0,1\}^n$ gilt:*

$$\mathfrak{B}_f \models \varphi \iff w \models \mathcal{C}_n$$

### 6.2.1 Normalform

Für jeden $\oplus^p$-Schaltkreis $\mathcal{C}_n$ wird o.B.d.A. die folgende Normalform (siehe **Abschnitt 3.2.1**) vorausgesetzt:

1. Der Graph des Schaltkreises sei ein Baum.
2. Alle Wege von einem Inputgatter zum Output haben die gleiche Länge $d$.
3. Die Größe des Schaltkreises sei höchstens $n^k$.
4. Es existieren keine Gatter mit $f\left(v\right) \in \{\mathbf{0},\mathbf{1}\}$. Diese werden durch die Schaltkreise $w_1 \wedge \neg w_1$ oder $w_1 \vee \neg w_1$ ersetzt.

### 6.2.2 Kodierung

Sei $f_n : \mathcal{C}_n \to [n]^k$ eine Kodierung, die jedem Gatter $v$ des Schaltkreises $\mathcal{C}_n$ ein Tupel $f_n(v) = t \in [n]^k$ zuweist. Es werden einige Relationen definiert, die zusammen die Struktur aller Schaltkreise beschreiben.

- Sei $AND \subseteq \mathbb{N}^{k+1}$ die Relation aller $\wedge$-Gatter:

$$AND := \bigcup_{n\in\mathbb{N}} \{(n, t_1, \cdots, t_k) \ : \ v \in \mathcal{C}_n,\ f(v) = \wedge,\ f_n(v) = \bar{t}\}$$

- Seien $OR \subseteq \mathbb{N}^{k+1}$ und $MOD \subseteq \mathbb{N}^{k+1}$ analog dazu die Relationen aller $\vee$- und $\oplus^p$-Gatter.
- Seien $INPUT_0, INPUT_1 \subseteq \mathbb{N}^{k+2}$ die Relationen aller negierten und nicht negierten Input-Gatter:

$$\begin{aligned} INPUT_0 &= \bigcup_{n\in\mathbb{N}} \{(n, j, t_1, \cdots, t_k) \ : \ v \in \mathcal{C}_n,\ f(v) = \overline{w_j},\ f_n(v) = \bar{t}\} \\ INPUT_1 &= \bigcup_{n\in\mathbb{N}} \{(n, j, t_1, \cdots, t_k) \ : \ v \in \mathcal{C}_n,\ f(v) = w_j,\ f_n(v) = \bar{t}\} \end{aligned}$$

- Sei $EDGE \subseteq \mathbb{N}^{2k+1}$ die kodierte Kantenrelation der Schaltkreise:

$$EDGE := \bigcup_{n\in\mathbb{N}} \left\{(n, s_1, \cdots, s_k, t_1, \cdots, t_k) \ : \ (u, v) \in E^{\mathcal{C}_n},\ \bar{s} = f_n(u),\ \bar{t} = f_n(\bar{v})\right\}$$

### 6.2.3 Konstruktion der Formel

**Satz 6.3.** *Sei $0 \leqslant i \leqslant d$. Es existiert eine Formel $\psi_i(x_{\mathbf{n}}, y_1, \cdots, y_k)$, für die folgendes gilt:*

*Sei $n \in \mathbb{N}$ beliebig, und sei $\bar{t} \in [n]^k$. So gilt $\mathfrak{B}_w \models \psi_i(n \cdot \bar{t})$ genau dann wenn $\bar{t}$ ein Gatter $v \in \mathcal{C}_n$ mit $T(v) = i$ kodiert, und $[\![\mathcal{C}_{n,v}]\!]^w = 1$ ist.*

*Beweis.* Per Induktion über $i$.

**Anfang:** Sei $i = 0$. So soll $\mathfrak{B}_w \models \psi_0(n \cdot \bar{t})$ genau dann gelten, wenn $\bar{t} \in [n]^k$ ein Inputgatter $v$ kodiert, und entweder $f(v) = I_j$ mit $w_j = 1$, oder $f(v) = \overline{I_j}$ mit $w_j = 0$ gilt.

Die folgende Formel erfüllt diese Forderung:

$$\begin{aligned} \psi_0(x_{\mathbf{n}}, \bar{y}) := \quad \exists z \quad & INPUT_0(x_{\mathbf{n}}, z, y_1, \cdots, y_k) \wedge \neg P_1(z) \vee \\ & INPUT_1(x_{\mathbf{n}}, z, y_1, \cdots, y_k) \wedge P_1(z) \end{aligned}$$

**Schritt:** Sei $0 \leqslant i < d$ beliebig.

Annahme: Es existiert eine Formel $\psi_i$ mit der geforderten Eigenschaft.

Sei $i' = i+1$, und seien $\psi_{i',X}$ für $X \in \{\wedge, \vee, \oplus^p\}$ die folgenden Teilformeln:

$$\begin{aligned}
\psi_{i',\wedge}\left(x_{\mathbf{n}} \cdot \bar{y}\right) &:= \forall z_1 \cdots \forall z_k \left(EDGE\left(x_{\mathbf{n}} \cdot \bar{z} \cdot \bar{y}\right) \rightarrow \psi_i\left(x_{\mathbf{n}} \cdot \bar{z}\right)\right) \\
\psi_{i',\vee}\left(x_{\mathbf{n}} \cdot \bar{y}\right) &:= \exists z_1 \cdots \exists z_k \left(EDGE\left(x_{\mathbf{n}} \cdot \bar{z} \cdot \bar{y}\right) \wedge \psi_i\left(x_{\mathbf{n}} \cdot \bar{z}\right)\right) \\
\psi_{i',\oplus^p}\left(x_{\mathbf{n}} \cdot \bar{y}\right) &:= \exists^{(p,0)}\left(z_1 \cdots z_k\right)\left(EDGE\left(x_{\mathbf{n}} \cdot \bar{z} \cdot \bar{y}\right) \wedge \psi_i\left(x_{\mathbf{n}} \cdot \bar{z}\right)\right)
\end{aligned}$$

Dabei steht $\exists^{(p,0)}\left(z_1, \cdots, z_k\right)\psi$ abgekürzt für den folgenden rekursiven Ausdruck, der genau dann erfüllt ist, wenn die Anzahl der Tupel $\bar{t} \in [n]^k$, die $\psi$ erfüllen, ein Vielfaches von $p$ ist:

$$\begin{aligned}
\exists^{(p,0)}\left(z_1\right) &:= \exists^{(p,0)} z_1 \psi \\
\exists^{(p,0)}\left(z_1, \cdots, z_k\right) &:= \bigvee_{\bar{t} \in X_k} \bigwedge_{j=1}^{p} \exists^{(p,j-1)} z_k \exists^{(p,t_j)}\left(z_1, \cdots, z_{k-1}\right) \\
X_k &:= \left\{ \bar{t} \in \{0, \cdots, p-1\}^p \;:\; \sum_{j=1}^{k} t_j \cdot (j-1) \equiv 0 \mod p \right\}
\end{aligned}$$

Nun kann die Formel $\psi_{i'}$ wie folgt zusammengesetzt werden:

$$\begin{aligned}
\psi_{i'}\left(x_{\mathbf{n}} \cdot \bar{y}\right) := \; & \left(AND\left(x_{\mathbf{n}} \cdot \bar{y}\right) \wedge \psi_{i',\wedge}\right) \vee \\
& \left(OR\left(x_{\mathbf{n}} \cdot \bar{y}\right) \wedge \psi_{i',\vee}\right) \vee \\
& \left(MOD\left(x_{\mathbf{n}} \cdot \bar{y}\right) \wedge \psi_{i',\oplus^p}\right)
\end{aligned}$$

Sie wird von einem Tupel $\bar{t} \in [n]^k$ genau dann erfüllt, wenn das Tupel $\bar{t}$ ein Gatter kodiert, das die seinem Typ entsprechende Teilformel erfüllt.

□

Insbesondere wird nach diesem Beweis die Formel $\psi_d$ von $\mathfrak{B}_w$ und $\bar{t} \in [n]^k$ genau dann erfüllt, wenn $\bar{t} = f_n\left(\mathrm{Out}\left(\mathcal{C}_n\right)\right)$ und $[\![\mathcal{C}_n]\!]^w = 1$ ist. Sei daher der Satz $\varphi$ wie folgt:

$$\varphi := \exists y_1 \cdots \exists y_k \exists x_{\mathbf{n}} \left(\psi_d\left(x_{\mathbf{n}} \cdot \bar{y}\right) \wedge \forall x \; x \leqslant x_{\mathbf{n}}\right)$$

Nun gilt:

$$\mathfrak{B}_w \models \varphi \iff w \models \mathcal{C}_n$$

Die Lokalität der Logik erster Stufe mit Arb-Erweiterung ist ein aktuelles Forschungsthema in der deskriptiven Komplexitätstheorie. Mehrere Ergebnisse sind noch offen; ein Teil kann aus den Lokalitätsergebnissen von FO [**arb**] abgeleitet werden.

**Theorem 6.4.** *Gaifman-Lokalität von* $(FO + MOD_p)$ [**arb**]

*Sei* $p \in \mathbb{N}$ *eine beliebige Primzahl mit* $p \neq 2$.

*Für jede* $(FO + MOD_p)$ [**arb**]*-Formel* $\varphi$ *mit* $d \in \mathbb{N}$ *Quantoren und jede Konstante* $c > 2d + 8$ *existiert eine Schranke* $n_0 \in \mathbb{N}$*, so dass* $\varphi$ *auf allen Strukturen* $\mathfrak{A}$ *der Größe* $n \geqslant n_0$*, auf denen sie auch arb-invariant ist,* ***schwach Gaifman-lokal*** *mit dem Radius* $(\log n)^c$ *ist.*

## 6.3 Schwache Lokalität für $p \neq 2$

Es wird die logische Charakterisierung von ACC [$p$] verwendet, um einen $\oplus$-Schaltkreis konstanter Tiefe zu erhalten, der PARITY berechnet.

**Satz 6.5.** *Sei* $p \in \mathbb{N}$ *eine Primzahl mit* $p \neq 2$*. Sei* $\varphi$ *eine* $k$*-stellige* $(FO + MOD_p)$ [**arb**]*-Formel mit* $d \in \mathbb{N}$ *Quantoren und sei* $\mathfrak{A}$ *ein Graph der Größe* $n$*, so dass* $\varphi$ *zwischen zwei Tupeln* $\bar{a}, \bar{b} \in A$ *mit isomorphen und disjunkten* $r$*-Nachbarschaften* ($r \in \mathbb{N}$) *unterscheidet.*

$$\begin{aligned} \mathcal{N}_r^{\mathfrak{A}}(\bar{a}) &\cong \mathcal{N}_r^{\mathfrak{A}}(\bar{b}) \\ \mathfrak{A} &\models \varphi(\bar{a}) \\ \mathfrak{A} &\not\models \varphi(\bar{b}) \end{aligned}$$

*Dann existiert ein Schaltkreis* $\mathcal{C}'_r$ *der Tiefe* $d + 4$ *und der Größe* $n^{\|\varphi\|}$*, der für* $w \in \{0,1\}^r$ *die* PARITY*-Funktion berechnet.*

*Beweis.* Nach Theorem **Theorem 6.1** existiert ein $\oplus^p$-Schaltkreis $\mathcal{C}_{n^2+kn}$ mit der Tiefe $d + 4$ und der Größe $n^{\|\varphi\|}$, der die Formel auf $\mathfrak{A}$ auswertet.

Ferner sind $\mathcal{N}_r^{\mathfrak{A}}(\bar{a})$ und $\mathcal{N}_r^{\mathfrak{A}}(\bar{b})$ isomorph und disjunkt.

Entsprechend der Konstruktion aus **Abschnitt 4.1** und **Abschnitt 5.2.1** kann daher ein $\oplus^p$-Schaltkreis $\mathcal{C}'_r$ konstruiert werden, der die Formel für $w \in \{0,1\}^r$ auf dem modifizierten Graphen $\mathfrak{A}_w = (A, \texttt{switch}(\mathfrak{A}, w))$ berechnet. Ungeachtet der zusätzlichen Zählgatter kann die Markierung der Eingänge wie folgt verändert

werden:

$$f'(v) := \begin{cases} f(v) & \text{falls } f(v) \in \{\mathbf{0}, \mathbf{1}, \wedge, \vee, \oplus^p\} \\ \\ \overline{I_i} & \text{falls } f(v) = I_{n\cdot g(x)+g(y)},\ (x,y) \in E^{\mathfrak{A}} \cap \mathcal{X}_i \\ & \text{oder } f(v) = \overline{I_{n\cdot g(x)+g(y)}},\ (x,y) \in \mathcal{Y}_i \\ \\ I_i & \text{falls } f(v) = I_{n\cdot g(x)+g(y)},\ (x,y) \in \mathcal{Y}_i \\ & \text{oder } f(v) = \overline{I_{n\cdot g(x)+g(y)}},\ (x,y) \in E^{\mathfrak{A}} \cap \mathcal{X}_i \\ \\ \mathbf{1} & \text{sonst, falls } f(v) = I_j,\ \left(\mathrm{enc}_g(\mathfrak{A}, \bar{a})\right)_j = 1 \\ \mathbf{0} & \text{sonst} \end{cases}$$

Es gilt $w \models \mathcal{C}'_r$ genau dann wenn $(\mathfrak{A}_w, \bar{a}) \cong (\mathfrak{A}, \bar{a})$, und daher genau dann wenn $|w|_1 \equiv 0 \mod p$. □

Daraus folgt ein Widerspruchsbeweis für **Theorem 6.4**.

*Beweis.* Angenommen, es existiere eine $k$-stellige $(\mathrm{FO} + \mathrm{MOD}_p)$ [**arb**]-Formel $\varphi$ mit $d \in \mathbb{N}$ Quantoren, und eine Konstante $c > 2d + 8$, so dass für alle $c \in \mathbb{N}$ ein Graph $\mathfrak{A}$ hinreichender Größe existiert, auf dem $\varphi$ arb-invariant ist und zwischen zwei Tupeln $\bar{a}, \bar{b} \in A$ mit isomorphen und disjunkten $r$-Umgebungen für $r = \lceil (\log n)^c \rceil$ unterscheidet.

Dann existiert nach **Satz 6.5** ein Schaltkreis der Tiefe $d+4$ und Größe $n^{\|\varphi\|}$, der alle Worte $w \in \{0,1\}^r$ akzeptiert, für die $|w|_1 \equiv 0 \mod 2$ gilt.

Da $2 \neq p$ ist (und insbesondere 2 keine Potenz der Primzahl $p$ ist), muss nach **Theorem 4.5** von Smolensky ein solcher Schaltkreis mindestens die Größe $2^{\Omega\left(\sqrt[2d+8]{r}\right)}$ besitzen. Für hinreichend große $r \in \mathbb{N}$ existiert also eine Konstante $\alpha \in \mathbb{N}_{>0}$, so dass folgt:

$$\begin{aligned} n^{\|\varphi\|} &\geqslant 2^{\alpha\cdot\left(\sqrt[2d+8]{r}\right)} \\ \implies \|\varphi\| (\log n) &\geqslant \alpha \cdot \left(\sqrt[2d+8]{r}\right) \\ \implies \frac{\|\varphi\|}{\alpha} (\log n) &\geqslant \sqrt[2d+8]{(\log n)^c} \\ \implies \frac{\|\varphi\|}{\alpha} (\log n) &\geqslant (\log n)^{\frac{c}{2d+8}} \\ \implies \frac{\|\varphi\|}{\alpha} &\geqslant (\log n)^{\frac{c}{2d+8}-1} \end{aligned}$$

Aus der Annahme $c > 2d + 8$ folgt analog zu den bisherigen Beweisen aus **Kapitel 5** ein Widerspruch. □

# 7 Zusammenfassung und Ausblick

Die Schaltkreisklasse $\mathrm{AC}^0$ ist nach Kapitel 3 durch das Logiksystem $\mathrm{FO}\,[\mathbf{arb}]$ charakterisiert [9].

Mittels dieser Charakterisierung folgt nach Kapitel 4 und 5 aus jeder unären $\mathrm{FO}\,[\mathbf{arb}]$-Formel, die nicht polylogarithmisch lokal ist (oder einer mehrstelligen Formel, die die schwache Gaifman-Lokalität verletzt), ein Schaltkreis in $\mathrm{AC}^0$ für das Promise-Problem, welches PARITY auf die Eingaben $w \in \{0,1\}^{2m}$ mit $|w|_1 \in \{m, m+1\}$ einschränkt.

Aus der unteren Schaltkreisschranke für dieses Problem folgt damit ein Widerspruch [8]. Es gilt der Schluss, dass alle arb-invarianten $\mathrm{FO}\,[\mathbf{arb}]$-Formeln einen polylogarithmischen Lokalitätsradius einhalten [2].

Eine skizzierte Reduktion weitet dieses Ergebnis auf die starke Lokalität mehrstelliger Formeln aus.

Die Schaltkreisklasse $\mathrm{ACC}\,[p]$ für Primzahlen $p \in \mathbb{N}$ ist durch das Logiksystem $\mathrm{FO} + \mathrm{MOD}_p\,[\mathbf{arb}]$ charakterisiert [15, 16].

Aus einer Formel, die hinreichend große Umgebungen unterscheidet, kann damit eine Lösung des Problems $\textsc{Mod}_2$ in $\mathrm{ACC}^0\,[p]$ abgeleitet werden. Nach dem Satz von Smolensky folgt, dass alle $\mathrm{FO}+\mathrm{MOD}_p\,[\mathbf{arb}]$-Formeln mit $p \neq 2$ eine schwache polylogarithmische Gaifman-Lokalität besitzen [14].

Auf $\mathrm{FO} + \mathrm{MOD}_2\,[\mathbf{arb}]$-Formeln lässt sich dieser Beweis nicht erweitern, da der Satz von Smolensky nur eine Aussage über das Problem $\textsc{Mod}_q$ in $\mathrm{ACC}^0\,[p]$ für $q \neq p^i$ macht. Tatsächlich kann $\textsc{Mod}_2$ in $\mathrm{ACC}^0\,[2]$ trivial gelöst werden. Lediglich eine Graph-Operation, aus der eine Lösung für $\textsc{Mod}_q$ mit $q \neq 2^i$ entsteht, würde für $p = 2$ zum Ziel führen.

Ein ähnliches allgemeines Resultat wie für $\mathrm{FO}\,[\mathbf{arb}]$ ohne zählende Quantoren gibt es nicht: Für 2-stellige Formeln mit $p = 2$ existiert sogar ein Gegenbeispiel, dass die starke Gaifman-Lokalität widerlegt. Allgemeine Ergebnisse zur starken Lokalität von $\mathrm{FO} + \mathrm{MOD}_p\,[\mathbf{arb}]$-Formeln beliebiger Stelligkeit sind noch weitgehend offene Forschungsfragen.

# Literaturverzeichnis


[1] M. Ajtai. $\sum_1^1$-formulae on finite structures. *Annals of Pure and Applied Logic*, 24(1):1 – 48, 1983.

[2] M. Anderson, D. van Melkebeek, N. Schweikardt, and L. 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, New York, NY, USA, 1st edition, 2009.

[4] H.D. Ebbinghaus and J. Flum. *Finite Model Theory*. Springer Monographs in Mathematics. Springer, 2005.

[5] Merrick L. Furst, James B. Saxe, and Michael Sipser. Parity, circuits, and the polynomial-time hierarchy. *Mathematical Systems Theory*, 17(1):13–27, 1984.

[6] Haim Gaifman. On local and non-local properties. In J. Stern, editor, *Proceedings of the Herbrand Symposium*, volume 107 of *Studies in Logic and the Foundations of Mathematics*, pages 105 – 135. Elsevier, 1982.

[7] Martin Grohe and Thomas Schwentick. Locality of order-invariant first-order formulas. *ACM Trans. Comput. Logic*, 1(1):112–130, July 2000.

[8] Johan Torkel Håstad. *Computational limitations for small-depth circuits*. MIT Press, Cambridge, MA, USA, 1987.

[9] Neil Immerman. Languages which capture complexity classes. In *Proceedings of the fifteenth annual ACM symposium on Theory of computing*, STOC '83, pages 347–354, New York, NY, USA, 1983. ACM.

[10] Neil Immerman. *Descriptive complexity*. Graduate texts in computer science. Springer, 1999.

[11] Leonid Libkin. *Elements Of Finite Model Theory (Texts in Theoretical Computer Science. An Eatcs Series)*. SpringerVerlag, 2004.

[12] A. A. Razborov and Mark Alan Epstein. Lower bounds for the size of circuits of bounded depth in basis, 1986.

[13] Amitabha Roy and Howard Straubing. Definability of languages by generalized first-order formulas over (n. In *In 23rd Symp. on Theoretical Aspects of Comp. Sci. (STACS'06*, pages 489–499, 2006.

[14] R. Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, STOC '87, pages 77–82, New York, NY, USA, 1987. ACM.

[15] H. Straubing. *Finite Automata, Formal Logic, and Circuit Complexity.* Progress in Theoretical Computer Science Series. Birkhäuser, 1994.

[16] H. Straubing, D. Thérien, and W. Thomas. Logics for regular languages, finite monoids, and circuit complexity. *NATO ASI Series C Mathematical and Physical Sciences-Advanced Study Institute*, 466:119–146, 1995.

[17] Heribert Vollmer. *Introduction to Circuit Complexity: A Uniform Approach.* Springer-Verlag New York, Inc., Secaucus, NJ, USA, 1999.

# Eidesstattliche Erklärung

Hiermit versichere ich an Eides statt, dass ich den Inhalt der vorliegenden Arbeit selbständig ohne fremde Hilfe angefertigt und nur die angegebenen Hilfsmittel verwendet habe.

Frankfurt, den 10. Dezember 2012

Christoph Burschka