# 1 *Suchprobleme und die Hypothese* Q *im Kontext des Pudlákschen Programms*

In der Einleitung dieser Arbeit wurde bereits angedeutet, dass die Hypothese Q von Fenner u. a. große Nähe und Verwandtschaft zu Hypothesen hat, die Suchprobleme im Allgemeinen und Beweissystemen im Speziellen betreffen. Damit ergeben sich Beziehungen zu Hypothesen aus dem Pudlákschen Programm, insbesondere ¬SAT (also dass eine NP-vollständige Mengen mit P-optimalem Beweissystem für diese Menge existiert). In diesem Kapitel werden wir diese Beziehungen näher erarbeiten. Zur Erinnerung:

**Vermutung ??** (Q, Fenner u. a., 2003)**.** *Für jede totale NPTM $N$ (d.h. $L(N) = \Sigma^*$) existiert eine Funktion $g \in$ FP sodass für alle $x$ das Bild $g(x)$ ein akzeptierender Rechenweg von $N(x)$ ist.*

Im Kapitel werden wir uns grob folgenden drei Desiderata widmen: erstens, nähern wir uns in Abschnitt 1.1 erneut der Frage zwischen Levin- und Karp-Vollständigkeit bzw. der Hypothese KvL aus vorigem Kapitel. Insbesondere analysieren wir die Beziehungen von KvL zu Q und versuchen, KvL in das Pudlákschen Programm einzuordnen.

Zweitens, in Abschnitt 1.2, verallgemeinern wir Charakterisierungen Q, die sich insbesondere auf Suchprobleme und deren assoziierte Beweissysteme beziehen. Insbesondere zeigen wir für eine große Klasse von vollständigen NP-Suchproblemen $R$ (nämlich jene die Levin-paddable sind) dass das zu $R$ assoziierte *Standardbeweissystem* ($(x, y)$ mit $R(x, y)$ ist ein Beweis für $x$) P-optimal ist, genau dann wenn Q. Damit wird die P-Optimalität des entsprechenden Standardbeweissystems zu einer Invariante, die entweder für *alle* Levin-paddable NP-Suchprobleme zutrifft, oder für *keins*.

Drittens ergänzen wir im gesamten Verlauf dieses Kapitels das Pudlákschen Programm um weitere Hypothesen (KvL, Q, … ), sodass Abbildung **??** der Beziehungen zwischen den Pudlákschen Hypothesen vergrößert wird. Damit erreichen wir den Stand, der in Abbildung 1 dargestellt wird. Damit einher wird abschließend ein Überblick über Orakel angegeben, welche Hypothesen des Pudlákschen Programms (ergänzt um Q, KvL, … ) trennen.

Für alle dieser drei Desiderata ist es zunächst notwendig, auf die Hypothese Q einzugehen. Fenner u. a. (2003) beobachten, dass das Invertieren von surjektiven ehrlichen FP-Funktionen eine erstaunlich robuste Aussage ist, die eine Vielzahl von äquivalenten „fundamentalen“ (Fenner u. a., 2003) Charakterisierungen aus der Komplexitätstheorie zulässt, so zum Beispiel die effiziente Lösbarkeit von TFNP-Suchproblemen, oder das effiziente Ausrechnen akzeptierender Rechenwege einer totalen NPTM. Wir können jetzt schon festhalten, dass die aktuelle Forschung diese Hypothese als sehr stark einschätzt, und eher die negative Beantwortung (i.e. ¬Q) vermutet.

**Satz 1.1** (Äquivalente Formulierungen der Hypothese Q; Fenner u. a., 2003)**.** *Folgende Aussagen sind äquivalent:*

*(1)* *Hypothese* Q*.*

*(2)* $\mathrm{NPMV}_t \subseteq_c \mathrm{FP}$*.*

*(3)* $\mathrm{TFNP} \subseteq_c \mathrm{FP}$*.*

*(4)* $\mathrm{P} = \mathrm{NP} \cap \mathrm{coNP}$ *und* $\mathrm{NPMV}_t \subseteq_c \mathrm{NPSV}_t$*.*

*(5)* *Jede surjektive ehrlichen Funktion* $f \in \mathrm{FP}$ *ist* P*-invertierbar.*

*(6)* *Für jede Menge* $L \in \mathrm{P}$ *und jede NPTM* $N$ *mit* $L(N) = L$ *existiert eine Funktion* $h \in \mathrm{FP}$ *mit*

$$x \in L \implies N(x) \text{ akz. mit Rechenweg } h(x).$$

Fenner u. a. (2003) und Messner (2000) charakterisieren Q noch durch zwei weitere Formen, diesmal über je eine Aussage über die Menge SAT:

**Satz 1.2.** *Folgende Aussagen sind äquivalent:*

*(1) Hypothese* Q*.*

*(2) (Fenner u. a., 2003) Für jede NPTM $N$ mit $L(N) = \mathtt{SAT}$ existiert eine Funktion $h \in \mathrm{FP}$ sodass*

$$N(\varphi) \text{ akz. mit Rechenweg } w \implies h(w) \text{ ist eine erfüllende Belegung für } \varphi.$$

*(3) (Messner, 2000) Das Standardbeweissystem sat*

$$sat(\varphi, w) = \begin{cases} \varphi & \text{wenn } w \text{ eine erfüllende Belegung für } \varphi \text{ ist} \\ \bot & \text{sonst.} \end{cases}$$

*für* $\mathtt{rSAT}$ *ist* P*-optimal.*

*Dieser Satz relativiert nicht.*

In anderen Worten sagt Aussage (2) aus, dass es modulo Umcodieren nur einen einzigen SAT-Solver gibt, und insbesondere alle SAT-Solver äquivalent zum trivialen Solver ist, welcher nur alle möglichen Belegungen ausprobiert. Die Aussage (3) macht eine analoge Aussage über Beweissysteme: egal wie komplex ein Beweissystem $h$ für $\mathtt{SAT}$ ist, wir können immer einen $h$-Beweis für $\varphi$ in eine erfüllende Belegung für $\varphi$ (quasi ein trivialer Beweis für $\varphi \in \mathtt{SAT}$) transformieren. Damit ist auch leicht zu sehen, dass $\mathsf{Q} \Rightarrow \neg\mathsf{SAT}$, zumindest im unrelativierten Fall.

In Abschnitt 1.2 werden wir sehen, dass sich die obigen Charakterisierungen auf weitere (aber möglicherweise nicht alle) vollständigen NP-Relationen generalisiert, womit insbesondere auch die beiden Charakterisierungen von Fenner u. a. und Messner zu einer *relativierbaren* Variante verallgemeinert werden. Mit dieser Verallgemeinerung ist es dann auch für uns möglich, Q formal in das Pudláksche Programm (u.a. durch $\mathsf{Q} \Rightarrow \neg\mathsf{SAT}$) einzuordnen. Hierfür führen wir jetzt schon den Begriff eines Standardbeweissystems formal ein.

**Definition 1.3** (Standardbeweissystem einer NP-Relation)**.** Sei $R$ eine NP-Relation. Wir definieren bezüglich $R$ das *Standardbeweissystem* $std_R$ für $\mathrm{Proj}(R)$ wie folgt:

$$std_R(w) \stackrel{\text{df}}{=} \begin{cases} x & \text{wenn } w = (x,y) \text{ und } (x,y) \in R, \\ \bot & \text{sonst.} \end{cases} \qquad \triangleleft$$

Damit ist, wie durch die Formulierung oben suggeriert, $sat = std_{\mathtt{rSAT}}$. Bevor wir nun mit einer Diskussion zwischen Karp-Vollständigkeit und Levin-Vollständigkeit fortsetzen, schließen wir diesen Einstieg mit folgender einfachen Beobachtung ab:

**Beobachtung 1.4.** *Für jede NP-Relation $R$ ist das Standardbeweissystem $std_R$ für* $\mathrm{Proj}(R)$ *ehrlich, optimal, und hat kurze Beweise.*

*Beweis.* Nachdem $R$ polynomiell längenbeschränkt ist, folgt sofort dass $std_R$ kurze Beweise hat. Nach Beobachtung **??** damit auch optimal. Insbesondere hat $std_R$ *nur* polynomiell längere Beweise, also ist $std_R$ ehrlich. □

## 1.1 *Karp-Vollständigkeit vs. Levin-Vollständigkeit*

Wir wiederholen hier erneut die zentrale offene Frage und Vermutung aus Abschnitt **??**:

**Frage ??.** *Wenn* $\mathrm{Proj}(R)$ *eine* $\leq^{\mathrm{p}}_{\mathrm{m}}$*-vollständige Menge für* NP *ist, ist dann auch $R$ eine* $\leq^{\mathrm{p}}_{\mathrm{L}}$*-vollständige NP-Relation für* FNP*?*

**Vermutung ??** (KvL)**.** *Es existiert eine NP-Relation $R$ sodass* $\mathrm{Proj}(R) \leq^{\mathrm{p}}_{\mathrm{m}}$*-vollständig für* NP *ist, aber $R$ ist nicht* $\leq^{\mathrm{p}}_{\mathrm{L}}$*-vollständig für* FNP*.*

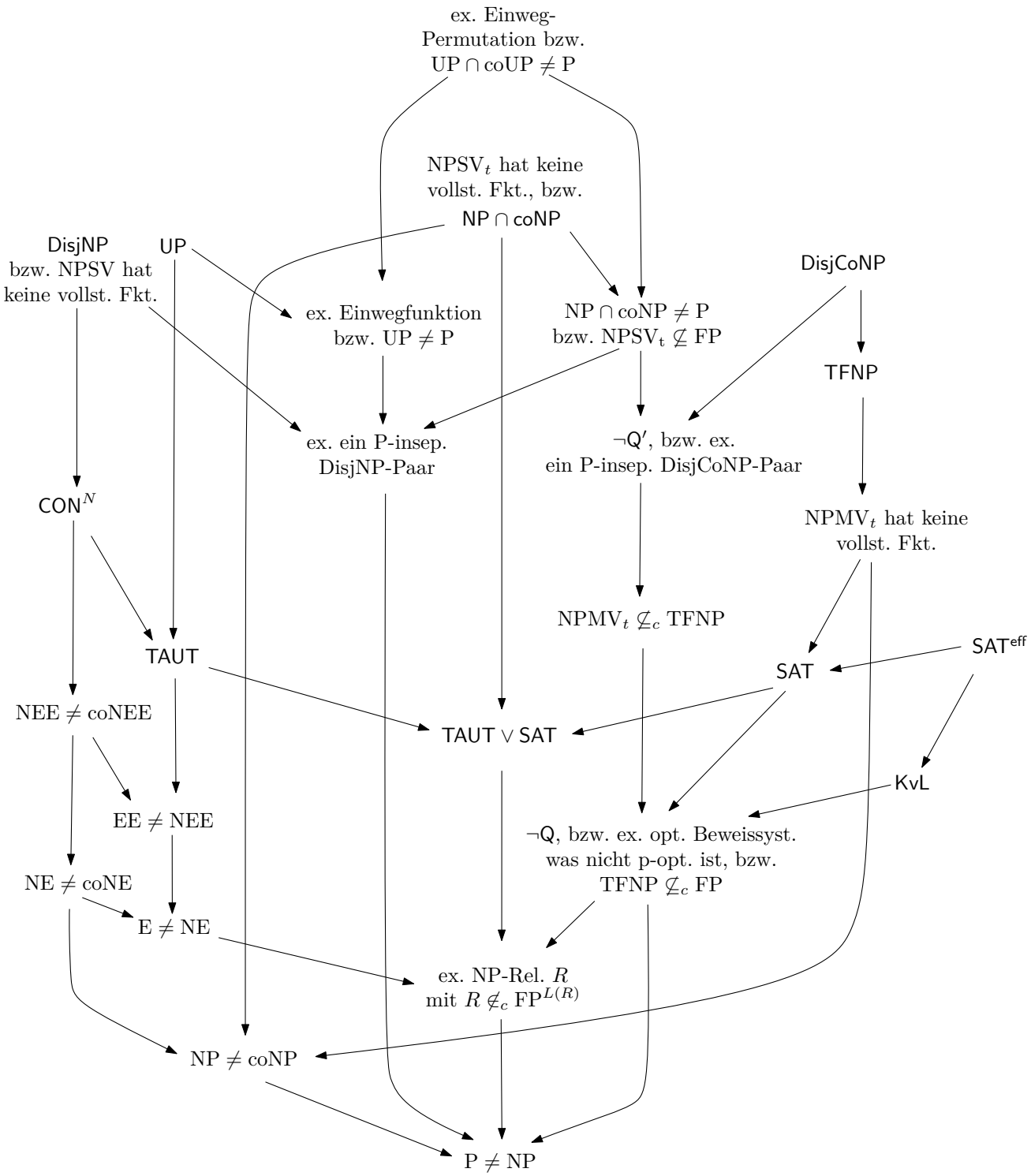



**Abbildung 1:** Bekannte (relativierenden) Implikationen zwischen den betrachteten Hypothesen und weiteren Aussagen. Satz 1.24 gibt Belegstellen für jede dieser Implikationen an.

Zunächst sei hier noch einmal hervorgehoben, dass eine Beantwortung der Frage **??** schwer ist. Zum einen haben wir bereits gesehen, dass ein Beweis KvL auch sofort $\mathrm{P} \neq \mathrm{NP}$ berweisen würde. Insbesondere ist ein relativierender Beweis von KvL ausgeschlossen, denn existiert ein Orakel, relativ zu diesem ¬KvL (z.B. ein PSPACE-vollständiges Orakel, welches NP auf P kollabiert).

Wir werden uns daher im Folgenden insbesondere auf Beziehungen zwischen Hypothesen und KvL konzentrieren. In diesem Sinne möchte ich argumentieren, dass die obige Frage bzw. Vermutung eng mit der Hypothese Q zusammenhängt. Im Speziellen werden wir sehen, dass die Hypothese Q so charakterisiert werden kann, dass sie einer Verstärkung der Vermutung KvL entspricht.[1]

[1] Fenner u. a. (2003) gaben hierbei eine ähnliche Aussage an (Cor. 3: „Q holds iff every Karp reduction from $A$ to $B$ can be extended to a Levin reduction"), es ist aber hervorzuheben, dass die Autoren von einem unüblichen Begriff von Levin-Reduktionen ausgehen, der sich von dem hier verwendeten unterscheidet. Dieser umfasst nicht eine „Rückwärts-Translation" von Zertifikaten für $B$-Instanzen zu $A$-Instanzen, sondern eine „Vorwärts-Translation" von Zertifikaten für $A$-Instanzen zu $B$-Instanzen.

**Satz 1.5.** *Folgende Aussagen sind äquivalent:*

*(1) Hypothese* Q, *bzw.* $\mathrm{TFNP} \subseteq_{\mathrm{c}} \mathrm{FP}$.

*(2) Für jedes Paar von NP-Relationen $A, B$ gilt:*

$$\mathrm{Proj}(A) \leq^{\mathrm{p}}_{\mathrm{m}} \mathrm{Proj}(B) \iff A \leq^{\mathrm{p}}_{\mathrm{L}} B.$$

*Beweis.* (1) $\implies$ (2): Die Richtung von rechts nach links ist klar. Für die andere Richtung sei $\mathrm{Proj}(A) \leq^{\mathrm{p}}_{\mathrm{m}} \mathrm{Proj}(B)$ mit $A, B$ NP-Relationen. Sei $q$ hierbei das Polynom was die Zertifikatslänge in $A$ begrenzt. Wir wollen nun eine Levin-Reduktion von $A$ auf $B$ angeben. Sei $f \in \mathrm{FP}$ die Funktion, welche die Reduktion $\mathrm{Proj}(A) \leq^{\mathrm{p}}_{\mathrm{m}} \mathrm{Proj}(B)$ realisiert.

Definiere folgende Relation $R$ mit

$$\textit{set-}R(w) = \begin{cases} \{y \mid y \in \Sigma^{\leq q(|x|)}, (x,y) \in A\} & \text{falls } w = (x,y'), (f(x),y') \in B \\ \{\varepsilon\} & \text{sonst.} \end{cases}$$

Es ist leicht zu sehen, dass $R$ eine totale NP-Relation ist. Nach (1) existiert nun eine (totale) Verfeinerung $g \in \mathrm{FP}$ von $R$.

Damit lässt die Levin-Reduktion von $A$ auf $B$ angeben: wähle $f$ als Reduktionsfunktion, und sei die Funktion $g$ von oben die Translationsfunktion. Dann gilt

$$\begin{aligned} &(f(x),y') \in B \implies (x,y') \in \mathrm{Proj}(R) \\ &\implies ((x,y'),g(x,y')) \in R \\ &\implies (x,g(x,y')) \in A \text{ nach Def. von } R \end{aligned}$$

wie gewünscht. Wir haben $A \leq^{\mathrm{p}}_{\mathrm{L}}$ via $f, g$.

(2) $\implies$ (1): Sei $A$ eine totale NP-Relation Definere nun die NP-Relation

$$B \stackrel{\mathrm{df}}{=} \{(x,\varepsilon) \mid x \in \Sigma^*\}.$$

Es ist leicht zu sehen das $\mathrm{Proj}(A) = \Sigma^* = \mathrm{Proj}(B)$ und dass $\mathrm{Proj}(A) \leq^{\mathrm{p}}_{\mathrm{m}} \mathrm{Proj}(B)$ über die Identitätsfunktion. Nach Annahme (2) lässt sich nun diese Reduktion zu einer Levin-Reduktion $A \leq^{\mathrm{p}}_{\mathrm{L}} B$ verstärken, mit Reduktionsfunktion $f \in \mathrm{FP}$ und Translationsfunktion $g \in \mathrm{FP}$. Für alle $x$ gilt nun $(f(x),\varepsilon) \in B$ nach Definition, nach Levin-Reduktion also auch $(x,g(x,\varepsilon)) \in A$. Definieren wir nun $h(x) \stackrel{\mathrm{df}}{=} g(x,\varepsilon)$, dann ist $(x,h(x)) \in A$ für alle $x$, also $h \in \mathrm{FP}$ eine Verfeinerung von $A$, also $A \in_{\mathrm{c}} \mathrm{FP}$, wie gewünscht. □

Beachte, dass in Aussage (2) die Implikation von rechts nach links ohnehin immer gilt. Damit lässt sich Aussage (2) auch so formulieren, dass jede Karp-Reduktion zu einer Levin-Reduktion verstärkt werden kann, indem zur Reduktionsfunktion $f$ eine geeignete Translationsfunktion $g$ hinzugefügt wird. Mit dieser Charakterisierung folgt auch unmittelbar, dass Q hinreichend für ¬KvL ist.

**Satz 1.6.** KvL $\implies$ ¬Q.

*Beweis.* Wir zeigen die Kontraposition, und starten mit der Voraussetzung Q. Wir wollen nun ¬KvL zeigen. Sei hierfür $R$ eine beliebige NP-Relation sodass $\mathrm{Proj}(R) \leq_{\mathrm{m}}^{\mathrm{p}}$-vollständig ist. Damit gilt also schon für alle weiteren NP-Relationen $A$, dass $\mathrm{Proj}(A) \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{Proj}(R)$. Nach Satz 1.21 gilt also auch die Aussage 1.21(6), und damit $A \leq_{\mathrm{L}}^{\mathrm{p}} R$. Also ist $R$ auch $\leq_{\mathrm{L}}^{\mathrm{p}}$-vollständig, wie gewünscht und wir haben ¬KvL gezeigt. □

Was sind natürlich notwendige Bedingungen für die Hypothese KvL? Diese Frage erscheint tatsächlich wesentlich schwieriger als gedacht. Insbesondere scheint es unklar, ob aus irgend einer von Pudláks Hypothesen die Aussage KvL folgt.

Besonders interessant erscheint aber die Beziehung zur Hypothese ¬Q, also genau die Umkehrung von Satz 1.6. Zumindest in der obigen Charakterisierung von Satz scheint ¬Q schwächer, denn mit Satz würde das bedeuten, dass ein *beliebiges* Paar $A, B$ von NP-Relationen existiert mit $\mathrm{Proj}(A) \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{Proj}(B)$, aber $A \not\leq_{\mathrm{L}}^{\mathrm{p}} B$. Weder $A$ noch $B$ müssen eine $\leq_{\mathrm{m}}^{\mathrm{p}}$-vollständige Projektion haben, was KvL ja verlangt.

Paradoxerweise scheint die Charakterisierung von ¬Q durch Fenner u. a. in Satz 1.2(2) dienlicher: Betrachten wir hierbei exemplarisch den Fall Relationen für SAT. Ich vermute, dass ¬Q ⇒ KvL; um das zu plausibilisieren möchte ich zeigen, dass ¬Q ∧ ¬KvL unwahrscheinlich ist.

Starten wir mit ¬Q, dann gilt mit Satz 1.2 für alle Funktionen $h \in \mathrm{FP}$

$$N(\psi) \text{ akz. mit Rechenweg } w \;\not\Longrightarrow\; (\psi, h(\psi, w)) \in \mathtt{rSAT}. \tag{1.1}$$

In anderen Worten: es existiert zwar eine NPTM $N$ welche SAT entscheidet, aber aus den akzeptierenden Rechenwegen $w$ von $N(x)$ auf $x \in \mathtt{SAT}$ kann nicht effizient eine akzeptierende Belegung für $x$ abgeleitet werden.

Wir können $N$ äquivalent als NP-Relation $R_N$ repräsentieren, mit $(\varphi, w) \in R_N$ genau dann wenn $N(x)$ mit Rechenweg $w$ akzeptiert. Damit kann Gleichung 1.1 so verstanden werden, dass $\mathtt{rSAT} \not\leq_{\mathrm{L}}^{\mathrm{p}} R_N$ *falls die Reduktionsfunktion $f$ die Identitätsfunktion ist.*

Unter der Annahme ¬KvL existiert nun eine Levin-Reduktion $\mathtt{rSAT} \leq_{\mathrm{L}}^{\mathrm{p}} R_N$ mit Reduktions- bzw. Translationsfunktion $f, g$. Das ist zunächst kein Widerspruch, denn es könnte ja $f \neq \mathrm{id}$. Gleichzeitig wäre die Existenz einer solchen Reduktion überraschend. Wir hätten nach Definition

$$N(f(\varphi)) \text{ akz. mit Rechenweg } w \;\Longrightarrow\; \varphi \text{ wird von Belegung } g(\varphi, w) \text{ erfüllt}. \tag{1.2}$$

Einerseits ist es also nicht möglich, aus dem Rechenweg $w$ effizient eine akzeptierende Belegung für $f(\varphi)$ zu bestimmen, obwohl $w$ bezeugt dass $f(\varphi)$ erfüllbar ist. (Ersetze in (1.1) $\psi$ mit $f(\varphi)$.) Andererseits reicht der „Beweis“ $w$ aber aus, um (zusammen mit der Information $\varphi$) effizient wieder eine erfüllende Belegung für $\varphi$ zu berechnen. Das *plausibilisiert* zwar einen Widerspruch, bzw. dass ¬Q ∧ ¬KvL wahrscheinlich falsch ist, ist aber natürlich kein solcher. Die Umkehrung von Satz 1.6 bleibt offen.

Dennoch vermute ich, dass solche Funktionen $f, g$ nicht jeweils für alle NPTM $N$ mit $L(N) = \mathtt{SAT}$ existieren können. Tatsächlich können wir die eben formulierte Vermutung auch in der Theorie der Beweissystemen formulieren: hierfür können wir die beiden Aussagen aus Gleichung 1.2 je als Aussagen über „Beweissysteme“ verstehen. Links ist der Rechenweg $w$ der „Beweis“ für $f(\varphi) \in \mathtt{SAT}$ über den Verifikator $N$, und rechts ist $g(\varphi, w)$ die erfüllende Belegung für $\varphi$, also ein *sat*-Beweis für $\varphi \in \mathtt{SAT}$.

Um diese Idee nun zu formalisieren, definieren wir zunächst eine abgeschwächte Variante der P-Simulation.

**Definition 1.7.** Seien $h, h'$ Beweissysteme für $L$. Das Beweissystem $h$ P-*simuliert effektiv* $h'$ falls Funktionen $f, g \in \mathrm{FP}$ existieren sodass

(1) $x \in L \iff f(x) \in L$,

(2) $h'(w) = f(x) \implies h(g(x, w)) = x$.

Wir schreiben in diesem Fall auch $h' \leq_{\mathrm{eff}}^{\mathrm{p}} h$. ◁

In anderen Worten, falls $h' \leq^p_{\text{eff}} h$, dann kann $h$ zwar nicht *jeden* $h'$-Beweis $w$ für $x \in L$ in einen $h$-Beweis für (das gleiche) $x$ effizient umrechnen, es kann aber zumindest alle *relevanten* $h'$-Beweise effizient umrechnen, nämlich für jedes $x \in L$ die $h'$-Beweise für $f(x)$ in $h$-Beweise für $x$. Anstelle „$h$ P-simuliert effektv $h'$“ ließe sich äquivalent auch $h^{-1} \leq^{\text{p}}_{\text{L}} h'^{-1}$ schreiben. Beachte, dass die Relation $h^{-1}$ nur Lösungen mit ihren Beweisen reliert. Klar ist: P-Simulation impliziert effektive P-Simulation impliziert Simulation unter Beweissystemen.

Die obige Intuition lässt sich also folgendermaßen formulieren: ich vermute, zumindest unter der Annahme ¬Q, dass das Standardbeweissystem *sat* nicht jedes Beweissystem effektiv P-simulieren kann, insbesondere nicht jenes was von der oben genannten NPTM $N$ induziert wird. Wir können diese Vermutung auch allgemeiner ohne Bezugnahme auf SAT bzw. *sat* formulieren:

**Vermutung 1.8** (KvL formuliert unter Beweissystemen)**.** *Es existiert eine NP-Relation $Q$ mit $\leq^{\text{p}}_{\text{m}}$-vollständigem* $\text{Proj}(Q)$*, wobei $\text{std}_Q$ nicht alle anderen optimalen Beweissysteme für* $\text{Proj}(Q)$ *effektiv* P*-simulieren kann.*

Dass die Formulierung der Vermutungen **??** und 1.8 äquivalent sind, zeigt folgende Beobachtung:

**Beobachtung 1.9.** *Folgende Aussagen sind äquivalent:*

*(1) Für jede NP-Relation $R$ mit $\leq^{\text{p}}_{\text{m}}$-vollständigem* $\text{Proj}(R)$ *ist $R \leq^{\text{p}}_{\text{L}}$-vollständig. (Das ist die Aussage* ¬KvL.*)*

*(2) Für jede NP-Relation $Q$ mit $\leq^{\text{p}}_{\text{m}}$-vollständigem* $\text{Proj}(Q)$ *kann $\text{std}_Q$ jedes optimale Beweissystem $h$ für* $\text{Proj}(Q)$ *effektiv* P*-simulieren. (Das ist die Negation von der Vermutung 1.8.)*

*Beweis.* (1)⇒(2): Sei $R$ eine NP-Relation mit $\leq^{\text{p}}_{\text{m}}$-vollständigem $\text{Proj}(R)$. Wir zeigen, dass $\text{std}_R$ jedes andere optimale Beweissystem $h$ effektiv P-simulieren kann. Nachdem $h$ optimal ist, hat es auch kurze Beweise (Beob. **??**): für jedes $x \in \text{Proj}(R)$ existiert ein $h$-Beweis $w$ mit $|w| \leq q(|x|)$ für geeignetes Polynom $q$. Definiere

$$R_h \stackrel{\text{df}}{=} \{(x, w) \mid |w| \leq q(|x|), h(w) = x\}.$$

Diese Relation ist offenbar eine NP-Relation und $\text{Proj}(R_h) = \text{Proj}(R)$ und damit ist $\text{Proj}(R_h)$ auch $\leq^{\text{p}}_{\text{m}}$-vollständig.

Nach Voraussetzung (1) ist also $R_h$ auch $\leq^{\text{p}}_{\text{L}}$-vollständig. Insbesondere gilt also auch $R \leq^{\text{p}}_{\text{L}} R_h$. Damit existieren also Funktionen $f, g \in \text{FP}$ sodass $x \in \text{Proj}(R) \leftrightarrow f(x) \in \text{Proj}(R)$ und

$$(f(x), w) \in R_h \implies (x, g(x, w)) \in R.$$

Nach Definition gilt also

$$h(w) = f(x) \implies \text{std}_R(g(x, w)) = x,$$

und damit ist $h \leq^{\text{p}}_{\text{eff}} \text{std}_R$.

(2)⇒(1): Sei $R$ eine NP-Relation wobei $\text{Proj}(R) \leq^{\text{p}}_{\text{m}}$-vollständig ist. Wir zeigen nun, dass $R$ auch $\leq^{\text{p}}_{\text{L}}$-vollständig ist. Sei hierfür $Q$ eine beliebige NP-Relation; wir wollen $Q \leq^{\text{p}}_{\text{L}} R$ zeigen.

Aus der $\leq^{\text{p}}_{\text{m}}$-Vollständigkeit folgt unmittelbar die Existenz einer Reduktionsfunktion $f$ mit

$$x \in \text{Proj}(Q) \iff f(x) \in \text{Proj}(R).$$

Definiere

$$h(w) \stackrel{\text{df}}{=} \begin{cases} x & \text{falls } w = (x, y) \text{ und } (f(x), y) \in R \\ \bot & \text{sonst.} \end{cases}$$

Wir zeigen, dass $h$ ein Beweissystem für $\text{Proj}(Q)$ ist. Es ist offenbar dass $h \in \text{FP}$. Die Funktion $h$ ist korrekt: wenn $h(x, y) = x$ dann ist $f(x) \in \text{Proj}(R)$ und nach Eigenschaft von $f$ auch $x \in \text{Proj}(Q)$. Die Funktion $h$ ist vollständig: Sei $x \in \text{Proj}(Q)$. Dann ist schon $f(x) \in \text{Proj}(R)$ und es gibt ein $y$ mit $(f(x), y) \in R$. Also ist $(x, y)$ ein $h$-Beweis für $x$.

Außerdem ist klar, dass $h$ kurze Beweise hat, damit ist $h$ auch optimal (Beob. **??**). Damit gilt nach (2) nun, dass $h \leq^{\mathrm{p}}_{\mathrm{eff}} std_Q$. Also existieren Funktionen $f', g' \in \mathrm{FP}$ sodass

$$x \in \mathrm{Proj}(Q) \iff f'(x) \in \mathrm{Proj}(Q), \quad h(w) = f'(x) \implies std_Q(g'(x,w)) = x.$$

Das reicht aus, $Q \leq^{\mathrm{p}}_{\mathrm{L}} R$ zu zeigen: wähle $f''(x) \stackrel{\mathrm{df}}{=} f(f'(x))$ als Reduktionsfunktion, dann gilt

$$(f''(x), y) \in R \implies (f(f'(x)), y) \in R \implies h(\underbrace{f'(x), y}_{w}) = f'(x)$$

$$\implies std_Q(g'(x,w)) = x \implies (x, g'(x,w)) \in Q.$$

Die Translationsfunktion $g''$, welche $(x,y)$ zu $g'(x,w)$ übersetzt, lässt sich leicht angeben. □

Mit der Definition der effektiven P-Simulation und der eben bewiesenen äquivalenten Formulierung der Karp-vs-Levin-Vermutung lässt sich nun zumindest die Hypothese SAT so verstärken, dass diese hinreichend für KvL ist.

**Vermutung 1.10** ($\mathrm{SAT}^{\mathrm{eff}}$)**.** *Keine $\leq^{\mathrm{p}}_{\mathrm{m}}$-vollständige Menge $L \in \mathrm{NP}$ hat ein optimales Beweissystem $h$, welches alle anderen optimalen Beweissysteme für $L$ effektiv* P*-simulieren kann.*

Wir sehen nun, dass $\mathrm{SAT}^{\mathrm{eff}}$ eine Verstärkung von sowohl SAT als auch KvL ist:

**Satz 1.11.** *(1)* $\mathrm{SAT}^{\mathrm{eff}} \implies \mathrm{SAT}$

*(2)* $\mathrm{SAT}^{\mathrm{eff}} \implies \mathrm{KvL}$

*Beweis.* Zu (1): Klar aus Kontraposition. Wenn $\neg$SAT, dann existiert für eine $\leq^{\mathrm{p}}_{\mathrm{m}}$-vollständige Menge $L \in \mathrm{NP}$ ein P-optimales Beweissystem $h$ für $L$ existiert, dann kann dieses (optimale) $h$ auch alle anderen Beweissysteme P-simulieren, und damit insbesondere auch alle optimalen Beweissysteme $h'$ effektiv P-simulieren.

Zu (2): Wieder klar aus Kontraposition. Unter $\neg$KvL folgt mit der Formulierung aus Vermutung 1.8 dass für jede NP-Relation $Q$, $\mathrm{Proj}(Q)$ vollständig, das (optimale) Standardbeweissystem $std_Q$ alle optimalen Beweissysteme für $\mathrm{Proj}(Q)$ effektiv P-simulieren kann. Das gilt dann insbesondere auch für die $\leq^{\mathrm{p}}_{\mathrm{L}}$-vollständige NP-Relation `rKAN`, also hat die $\leq^{\mathrm{p}}_{\mathrm{m}}$-vollständige Menge `KAN` *ein* Beweissystem, welches alle optimalen Beweissysteme effektiv P-simulieren kann. □

Wir haben also je eine notwendige ($\neg$Q) und eine hinreichende Hypothese ($\mathrm{SAT}^{\mathrm{eff}}$) für KvL. Nichtsdestotrotz bleiben noch viele Fragen offen, die wir hier aus Platzgründen nicht weiter verfolgen werden. Zum einen zur Charakterisierung von KvL: Wir konnten zwar KvL als Aussage über Beweissysteme formulieren, aber sind auch andere äquivalente Aussagen möglich, z.B. ähnlich wie bei Q?

Zum anderen die Beziehungen zwischen KvL und anderen Hypothesen bzw. Annahmen. Gibt es natürliche (z.B. kryptographische) Annahmen die hinreichend für KvL sind? Wie ist die Beziehung zu den anderen Pudlákschen Hypothesen? Wie verhält sich insbesondere SAT zu $\mathrm{SAT}^{\mathrm{eff}}$? Diese Fragen werden wir zum Teil in Kapitel 2 klären; dort wird ein Orakel konstruiert, welches zeigt, dass selbst unter der Annahme von DisjNP und UP es nicht möglich ist, mit relativierenden Beweismethoden auf KvL zu schließen. Wir kommen hierauf am Ende dieses Kapitels noch einmal zurück.

Insgesamt ist durch die vorherigen Überlegungen aber ein erster Schritt getan, die Beziehung zwischen Levin- und Many-one-Vollständigkeit über die Vermutung KvL im Kontext des Pudlákschen Programms einzuordnen. Weitere Forschung in diese Richtung erscheint vielversprechend.

## 1.2 *Hypothese* Q *und Suchprobleme*

Wie im Einstieg des Kapitels angesprochen, geben Fenner u. a. (2003) bzw. Messner (2000) äquivalente Charakterisierungen der Hypothese Q an, welche sich im Wesentlichen auf auf der $\leq^{\mathrm{p}}_{\mathrm{L}}$-Vollständigkeit von `rSAT` aufbauen (Satz 1.2). Wir wiederholen hier noch einmal die Aussage,

aber mit einer etwas abstrakteren Notation. Ganz ähnlich wie NP-Relationen ein Standardbeweissystem induzieren, können wir auch das Standardbeweissystem bezüglich einer NPTM definieren:

**Definition 1.12** (Standardbeweissystem von NPTM)**.** Sei $N$ eine NTM. Wir definieren bezüglich $N$ das das *Standardbeweissystem* $std_N$ für $L(N)$ wie folgt:

$$std_N(w) \stackrel{\text{df}}{=} \begin{cases} x & \text{wenn } w = (x, \alpha) \text{ und } N(x) \text{ akzeptiert auf RW } \alpha, \\ \bot & \text{sonst.} \end{cases}$$ ◁

Ähnlich wie bei Standardbeweissysteme für NP-Relationen ist $std_N$ für jede nichtdeterministische *Polynomialzeit*-TM $N$ ehrlich, optimal, und hat kurze Beweise.

**Satz 1.2.** *Folgende Aussagen sind äquivalent:*

*(1) Hypothese* Q*.*

*(2) Für jede NPTM $N$ mit $L(N) = \texttt{SAT}$ gilt $std_N \leq^{\text{p}}_{\text{m}}$ sat. Es existiert also eine Funktion $h \in \text{FP}$ sodass*

$$N(\varphi) \text{ akz. mit Rechenweg } w \implies h(w) \text{ ist erfüllende Belegung für } \varphi.$$

*(3) Das Standardbeweissystem sat für* `rSAT` *ist* P*-optimal.*

*Dieser Satz relativiert nicht.*

Diese beiden Charakterisierungen wollen wir im Folgenden verallgemeinern und auf beliebige $\leq^{\text{p}}_{\text{L}}$-vollständige NP-Relationen $R$ übertragen. Hieraus ergibt sich schon unmittelbar der technische Beitrag, dass dann diese Charakterisierungen auch in einer relativierten Umgebung angewendet werden können, um z.B. ein geeignetes Orakel zu konstruieren, was Q von anderen Hypothesen trennt.

Zweitens ergibt sich aus der Verallgemeinerung das überraschende Ergebnis, dass $\leq^{\text{p}}_{\text{L}}$-Vollständigkeit allein zur Generalisierung nicht ausreicht. In den originalen Beweisen von Fenner u. a. und Messner wurden stillschweigend zusätzliche Eigenschaften von `rSAT` mitgedacht und ausgenutzt. Die folgende Generalisierung deckt diese Eigenschaften auf, und plausibilisiert dass diese womöglich nicht von allen $\leq^{\text{p}}_{\text{L}}$-vollständigen NP-Relationen geteilt werden.

Eine dieser stärkeren Eigenschaften von `rSAT`, welche Fenner u. a. in ihren Beweisen gebrauchten, ist die $\leq^{\text{p}}_{1,\text{i}}$-Vollständigkeit von `rSAT`. Wir schwächen im Folgenden diese Voraussetzunt ab, und verlangen nur, dass eine NP-Relation unter ehrlichen Reduktionen vollständig ist. Dies gilt insbesondere für `rSAT`. Für welche $\leq^{\text{p}}_{\text{L}}$-vollständigen NP-Relationen das noch zutrifft, werden wir unten betrachten.

Mit dieser ehrlichen Levin-Vollständigkeit lässt sich nun die Charakterisierung von Fenner u. a., Thm. 2 generalisieren:

**Lemma 1.13.** *Sei $R$ eine $\leq^{\text{p}}_{\text{L}}$-vollständige NP-Relation, mit der zusätzlichen Eigenschaft dass für die jeweilige entsprechende Problem-Reduktionsfunktion $f : Q \to R$ für $Q \leq^{\text{p}}_{\text{L}} R$ immer gilt, dass $f$ ehrlich ist. Folgende Aussagen sind äquivalent:*

*(1) Aussage* Q*.*

*(2) Für alle NPTM $N$ mit $L(N) = \text{Proj}(R)$ lassen sich akzeptierende Rechenwege von $N$ in Zertifikate umrechnen: es gilt $std_N \leq^{\text{p}}_{\text{m}} std_R$, bzw. existiert eine Funktion $h \in \text{FP}$ sodass*

$$N(x) \text{ akz. mit Rechenweg } \alpha \implies (x, h(x, \alpha)) \in R.$$

*Beweis.* (1)⇒(2): Nachdem Q gilt, gilt auch TFNP $\subseteq_{\text{c}}$ FP nach Beobachtung **??**. Sei nun $R$ eine beliebige NP-Relation mit Zertifikatsschranke $q$, und sei $N$ eine beliebige NPTM mit $L(N) = \text{Proj}(R)$. Definiere nun folgende Relation $Q$ mittels:

$$\textit{set-}Q(x, \alpha) \stackrel{\text{df}}{=} \begin{cases} \{y \mid y \in \Sigma^{\leq q(|x|)}, (x, y) \in R\} & \text{falls } N(x) \text{ auf RW } \alpha \text{ akzeptiert,} \\ \{\varepsilon\} & \text{sonst.} \end{cases}$$

Es ist leicht zu sehen, dass $Q$ eine totale NP-Relation ist. Insbesondere im ersten Fall gilt $x \in L(N) = \text{Proj}(R)$, also existiert auch mindestens ein $y \in \mathit{set}\text{-}R(x)$.

Nach Annahme gilt also $Q \in_c \text{FP}$, sei also $h \in \text{FP}$ eine Verfeinerung von $Q$. Nun gilt

$$\begin{aligned}
&\mathit{std}_N(x, \alpha) = x \\
&\implies N(x) \text{ akz. mit Rechenweg } \alpha \\
&\implies \mathit{set}\text{-}Q(x, \alpha) = \mathit{set}\text{-}R(x) \\
&\implies h(x, \alpha) \in \mathit{set}\text{-}R(x) \implies (x, h(x, \alpha)) \in R, \\
&\implies \mathit{std}_R(x, h(x, \alpha)) = x.
\end{aligned}$$

wie gewünscht.

(2)⇒(1): Sei $Q \in \text{TFNP}$. Sei ferner $R$ eine $\leq_L^p$-vollständige NP-Relation unter ehrlichen Problem-Reduktionsfunktionen (z.B `rKAN`), und Zertifikatsschranke $p$. Da $R$ ja vollständig ist, gilt $Q \leq_L^p R$ via $f, g \in \text{FP}$ und (nach Voraussetzung) ist $f$ ehrlich; es existiert ein Polynom $q$ sodass $q(|f(x)|) \geq |x|$.

Definiere nun die folgende NPTM $N'(w)$:

1 Rate nichtdeterministisch $x \in \Sigma^{\leq q(|w|)}$
2 **wenn** $f(x) = w$ **dann** akzeptiere
*(Ab hier kann man x wegwerfen)*
3 Rate nichtdeterministisch $y \in \Sigma^{\leq p(|w|)}$
4 Akzeptiere genau dann wenn $(w, y) \in R$.

Wir zeigen nun, dass $L(N') = \text{Proj}(R)$. Wir müssen hierfür nur die Fälle betrachten, wenn $N'(w)$ in Z. 2 akzeptiert. In diesem Fall gilt $f(x) = w$, und wir haben

$$x \in \Sigma^* \implies x \in \text{Proj}(Q) \implies f(x) \in \text{Proj}(R) \implies w \in \text{Proj}(R),$$

wie gewünscht.

Nach (2) gilt nun also, dass eine Funktion $h \in \text{FP}$ existiert sodass

$$N'(w) \text{ akz. mit Rechenweg } \alpha \implies (w, h(w, \alpha)) \in R.$$

Beobachte wie für $N'(f(x))$ immer ein trivialer akzeptierender Rechenweg $\alpha_x$ existiert: nämlich jener, welcher in Z. 1 das Urbild $x$ rät. Beobachte dass die Umformung $x \mapsto \alpha_x$ in Polynomialzeit möglich ist.

Um nun (1) zu zeigen müssen wir aus $x \in \Sigma^*$ effizient einen akzeptierenden Rechenweg für $N$ bestimmen. Wir haben

$$\begin{aligned}
&N'(f(x)) \text{ akz. mit Rechenweg } \alpha_x \implies (f(x), h(f(x), \alpha_x)) \in R \\
&\implies (x, \underbrace{g(h(f(x), \alpha_x))}_{r(x)}) \in Q \quad \text{nach Translationsfunktion } g.
\end{aligned}$$

Damit ist $r \in \text{FP}$, $r(x) \stackrel{\text{df}}{=} g(h(f(x), \alpha_x))$, eine Verfeinerung von $Q$ und $Q \in_c \text{FP}$, wie gewünscht. □

Wir wollen nun auch die zweite Charakterisierung von Messner generalisieren. Im originalen Beweis wurde erneut eine sekundäre stärkere Eigenschaft von `rSAT` ausgenutzt, die einer schwachen Form von Paddability entspricht. Ähnlich wie bei der Berman–Hartmanis-Paddability wollen wir beliebige Instanzen $x$ zu längeren Instanzen $x'$ vergrößern. Zusätzlich verlangen wir, dass wir auch auf Zertifikaten $y$ für $x'$ wieder Zertifikate $y$ für $x$ zurückrechnen können. In anderen Worten: wir codieren „redundante Teile“ in $x$ hinein, um $x'$ zu erhalten. Für Zertifikate $y'$ für $x'$ können wir dann den Teil des Zertifikats wegwerfen, welcher sich ohnehin nur auf das redundanten Padding bezieht, und erhalten wieder ein Zertifikat für $x$.

**Definition 1.14** (Levin-Paddability)**.** Eine NP-Relation $R$ ist *Levin-paddable* wenn Funktionen $pad \in \mathrm{FP}$ und $padsol \in \mathrm{FP}$ existieren, sowie ein Polynom $r$ sodass

(1) $x \in \mathrm{Proj}(R) \iff pad(x, 1^n) \in \mathrm{Proj}(R)$,

(2) $(pad(x, 1^n), y) \in R \implies (x, padsol(x, 1^n, y)) \in R$,

(3) $r(|pad(x, 1^n)|) \geq n$. (Funktion $pad$ ist ehrlich bzgl. der zweiten Komponente.) ◁

Beachte dass wir im Gegensatz zur Berman–Hartmanis-Paddability keine Invertierbarkeit der Padding-Funktion verlangen. Später werden wir sehen, welche NP-Relationen alle diese Eigenschaft der Levin-Paddability erfüllen. Festhalten können wir aber, dass `rSAT` Levin-paddable ist. Das ist einfach zu sehen: padde Formeln $\varphi$ auf, indem z.B. Disjunktionen neue Variablen hinzugefügt werden, i.e.

$$\varphi' = pad(\varphi, 1^n) = \varphi \vee x_k \vee x_{k+1} \vee \cdots \vee x_{k+n},$$

wobei $k$ hinreichend groß sein soll, dass $x_k, x_{k+1}, \ldots$ nicht als Variable in $\varphi$ vorkommt. Ist nun $w'$ eine erfüllende Belegung für $\varphi'$, dann entferne alle Variablenbelegungen $x_k, x_{k+1}, \ldots$ aus $w'$; es ergibt sich eine erfüllende Belegung $w$ für $\varphi$.

Diese Eigenschaft lässt sich auch leicht für die kanonische NP-Relation `rKAN` überprüfen, und gilt insbesondere auch im relativierten Fall.

**Beobachtung 1.15.** *Die kanonische Levin-vollständige NP-Relation* `rKAN` *ist Levin-paddable.*

*Skizze.* Padde Instanzen $(N, x, 1^n)$ zu $(N', x, 1^n)$ auf, wobei die NTM $N'$ aus $N$ hervorgeht, indem Zustände hinzugefügt werden die über die Transitionsrelation von $N$ nicht erreichbar sind. Ein akzeptierender Rechenweg auf $N'(x)$ ist dann genau ein akzeptierender Rechenweg auf $N(x)$. □

Mit dieser Definition können wir nun einen Beweis von Messner (2000, Thm. 5.2) generalisieren. Beachte dass hier nicht notwendigerweise von vollständigen NP-Relationen gesprochen wird, und das im Beweis (3)⇒(1) die Levin-Paddability notwendig zu sein scheint, damit $std_R$ auch nicht-ehrliche Beweissysteme P-simulieren kann.

**Lemma 1.16.** *Sei $R$ eine NP-Relation die Levin-paddable ist. Folgende Aussagen sind äquivalent:*

*(1) Das Standardbeweissystem $std_R$ bzgl. $R$ ist* P*-optimal.*

*(2) Für alle NTM $N$ (ohne Laufzeitbeschränkung) mit $L(N) = \mathrm{Proj}(R)$ gilt $std_N \leq^{\mathrm{p}}_{\mathrm{m}} std_R$.*

*(3) Für alle NPTM $N$ mit $L(N) = \mathrm{Proj}(R)$ gilt $std_N \leq^{\mathrm{p}}_{\mathrm{m}} std_R$.*

*Beweis.* (1)⇒(2): Klar.

(2)⇒(3): Klar.

(3)⇒(1): Angenommen (3) gilt. Seien $pad$, $padsol$ die entsprechenden Funktionen, welche die Levin-Paddability von $R$ realisieren. Das Polynom $r$ sei so gewählt dass $r(|pad(x, 1^n)|) \geq n$ (vgl. 1.14(3)).

Wir wollen nun zeigen, dass $std_R$ auch P-optimal ist. Sei hierfür $f$ ein beliebiges Beweissystem für $\mathrm{Proj}(R)$. Wir zeigen nun, dass $f \leq^{\mathrm{p}}_{\mathrm{m}} std_R$. Seien $pad$, $padsol$ die entsprechenden Padding-Funktionen von $R$. Definiere nun

$$f'(w) = \begin{cases} pad(x, 1^{|w|}) & \text{falls } w = 1z \text{ und } f(z) = x, \\ x & \text{falls } w = 0z \text{ und } std_R(z) = x, \\ \bot & \text{sonst.} \end{cases}$$

Es ist leicht zu sehen, dass $f'$ ein Beweissystem für $\mathrm{Proj}(R)$ ist. Außerdem ist $f'$ ehrlich es ist ehrlich für Eingaben $0z$, denn das Standardbeweissystem $std_R$ ist ehrlich nach Beobachtung 1.4. Es ist ehrlich für Eingaben $w = 1z$, denn

$$|1z| = |w| \leq r(|\underbrace{pad(x, 1^{|w|})}_{f'(1z)}|) = r(|f'(|w|)|).$$

Sei im Folgenden dann das Polynom $r'$ so gewählt, dass $|w| \leq r'(|f'(w)|)$ gilt.

Definiere nun die NPTM $N_{f'}$ welche auf Eingabe $x$ erst nichtdeterministisch einen Beweis $w$, $|w| \leq r'(|x|)$ rät, und genau dann akzeptiert falls $f'(w) = x$. Es ist klar, dass $L(N_{f'}) = \mathrm{Proj}(R)$. Nach Voraussetzung (3) gilt $std_{N_{f'}} \leq^{\mathrm{p}}_{\mathrm{m}} std_R$, es gibt es also nun eine Funktion $h \in \mathrm{FP}$ sodass

$$N_{f'}(x) \text{ akz. mit Rechenweg } \alpha \implies (x, h(x,\alpha)) \in R. \tag{1.3}$$

Jetzt können wir zeigen, dass $std_R$ das Beweissystem $f$ P-simuliert: sei $z$ ein $f$-Beweis für $x$, d.h. $f(z) = x$. Wir wissen, dass $f'(1z) = pad(x, 1^{|1z|}) = x'$. Daher können wir aus $z$ einen Rechenweg $\alpha_z$ konstruieren, sodass $N_{f'}(x')$ akzeptiert, nämlich jener der den $f'$-Beweis $1z$ rät. Die Abbildung $z \mapsto \alpha_z$ lässt sich in Polynomialzeit leisten.

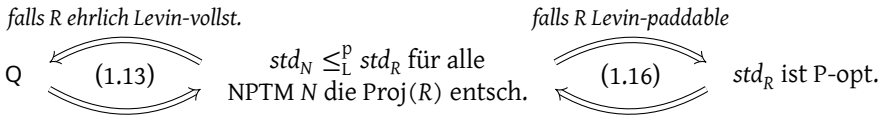
Nun gilt

$$\begin{aligned}
&N_{f'}(x') \text{ akz. mit } \alpha_z \implies (x', \underbrace{h(x', \alpha_z)}_{y'}) \in R \text{ nach (1.3)} \\
&\implies (pad(x, 1^{|1z|}), y') \in R \text{ mit } y' = h(x', \alpha_z) \text{ und obiger Def. von } x' \\
&\implies (x, \underbrace{padsol(x, 1^{|1z|}, y')}_{y}) \in R \text{ nach Def. 1.14(2)} \\
&\implies std_R(x,y) = x \text{ mit } y = padsol(x, 1^{|1z|}, y')
\end{aligned}$$

und wir haben aus dem $f$-Beweis $z$ für $x$ einen $std_R$-Beweis $(x,y)$ für $x$ bestimmt. Es ist klar, dass die Übersetzung $z \mapsto (x,y)$ in Polynomialzeit möglich ist. □

Wir fassen kurz den aktuellen Stand zusammen. Sei $R$ eine NP-Relation. Wir haben nun folgendes Bild:

TODO: Irgendwie möglich von $std_N$ wegzukommen und stattdessen über z.B. ps mit kurzen Beweisen zu sprechen?




Wir wollen nun eine möglichst breite Klasse an NP-Relationen angeben, für die diese beiden obigen Äquivalenzen gelten, also insbesondere diejenigen NP-Relationen, welche die selbe Charakterisierung wie `rSAT` im Fall der unvelativierbaren Charakterisierung von Fenner u. a. und Messner zulassen.

Wir überlegen uns hierzu zunächst, dass „$\leq^{\mathrm{p}}_{\mathrm{L}}$-vollständig und Levin-paddable“ ausreichend ist, da Levin-Paddability insbesondere zulässt, eine Levin-Reduktion so zu padden, dass die Reduktionsfunktion auch ehrlich ist.

**Lemma 1.17.** *Die in Lemma 1.13 und 1.16 genannten Voraussetzungen an die NP-Relation $R$ werden von allen solchen $R$ erfüllt, die $\leq^{\mathrm{p}}_{\mathrm{L}}$-vollständig sind und Levin-paddable sind.*

*Beweis.* Es ist sofort klar, dass $R$ die Voraussetzungen von Lemma 1.16 erfüllt. Es bleibt nur zu zeigen, dass für jede NP-Relation $Q$ eine $\leq^{\mathrm{p}}_{\mathrm{L}}$-Reduktion angegeben werden kann, bei dem die Problem-Reduktionsfunktion ehrlich ist. Wir nutzen hierbei aus, dass $R$ eine Levin-paddable Relation ist.

Nachdem $R$ vollständig ist, gilt $Q \leq^{\mathrm{p}}_{\mathrm{L}} R$; sei $f, g \in \mathrm{FP}$ die Reduktions- bzw. Translationsfunktion welche diese Reduktion realisieren. Wir werden nun Funktionen $f', g' \in \mathrm{FP}$ angeben, welche die gleiche Reduktion realisieren, aber $f'$ ehrlich, wie gewünscht.

Sei $pad, padsol$ die zu $R$ zugehörigen Padding-Funktionen. Definiere

$$f'(x) \stackrel{\mathrm{df}}{=} pad(f(x), 1^{|x|}).$$

Es gilt

$$x \in \mathrm{Proj}(Q) \iff f(x) \in \mathrm{Proj}(R) \iff pad(f(x), 1^{|x|}) = f'(x) \in \mathrm{Proj}(R),$$

wobei erste Implikation die Eigenschaft der Reduktionsfunktion $f$ ist, und die zweite aus der Definition von Levin-Paddability folgt. Aus der Definition von Levin-Paddability folgt auch $r(|f'(x)|) \geq |x|$ für ein geeignetes Polynom $r$, und damit ist auch $f'$ ehrlich.

Definiere

$$g'(x,z) \stackrel{\text{df}}{=} g(x, padsol(f(x), 1^{|x|}, z)).$$

Sei nun $(f'(x), z) \in R$. Die Funktion $g'$ berechnet nun ein Zertifikat $y$ für $x$: Wir haben $(pad(f(x), 1^{|x|}), z) \in R$, also gilt nach Levin-Paddability dass

$$(f(x), padsol(f(x), 1^{|x|}, z)) \in R,$$

und nach Definition der Translationsfunktion $g$ gilt dann

$$(x, g(x, padsol((f(x), 1^{|x|}, z))) \in Q,$$

und das ist genau $(x, g'(x,z)) \in Q$, wie gewünscht. □

Folgende Beobachtung hilft uns, natürliche NP-Relationen zu identifizieren, welche Levin-vollständig und gleichzeitig Levin -paddable sind.

**Beobachtung 1.18.** *(1) Gilt* $\mathtt{rKAN} \leq^{\text{p}}_{\text{L}} R$*, und ist die zugehörige Reduktionsfunktion* $f$ *ehrlich, dann ist* $R$ *Levin-paddable (und* $\leq^{\text{p}}_{\text{L}}$*-vollständig).*

*(2) Jede* $\leq^{\text{p}}_{\text{L,1,inv}}$*-vollständige NP-Relation* $R$ *ist auch Levin-paddable.*

Damit können wir schon als Ergebnis festhalten, dass jede $\leq^{\text{p}}_{\text{L,1,inv}}$-vollständige Relation $R$ die in Lemma 1.16 und 1.13 genannten Voraussetzungen an die NP-Relation $R$ erfüllt. Das sind nach Goldreich (2008) unrelativierten Fall u.a. `rSAT`, `rSETCOVER`, `rVERTEXCOVER`, `rCLIQUE`, `r3COLORABILITY`.

*Beweis zu Beobachtung 1.18.* Aussage (2) folgt unmittelbar aus (1): Wir haben $\mathtt{rKAN} \leq^{\text{p}}_{\text{L,1,inv}} R$ und damit ist die entsprechende Reduktionsfunktion $f$ P-invertierbar, und damit ehrlich.

Für (1) nutzen wir die Levin-Paddability von `rKAN` aus: übersetze Instanz $x$ von $R$ nach `rKAN`, padde dort hoch, und übersetze zu $R$-Instanz $x'$ zurück. Ist dann $y'$ ein Zertifikat für $x'$, dann lässt sich dies auf ähnlichem Weg wieder zu einem Zertifikat für $x$ zurückrechnen.

Seien $f, g$ die Reduktions- bzw. Translationsfunktion, welche $\mathtt{rKAN} \leq^{\text{p}}_{\text{L}} R$ bezeugen, und seinen analog $f', g'$ jene Funktionen, welche $R \leq^{\text{p}}_{\text{L}} \mathtt{rKAN}$ bezeugen. Erstere existieren nach Voraussetzung, zweitere existieren weil $\mathtt{rKAN} \leq^{\text{p}}_{\text{L}}$-vollständig ist. Nach Voraussetzung ist $f$ ehrlich. Und nach Beobachtung 1.15 existieren für `rKAN` Padding-Funktionen $pad_{\mathtt{rKAN}}$, $padsol_{\mathtt{rKAN}}$. Sei $q$ ein entsprechendes Polynom mit $q(|pad_{\mathtt{rKAN}}(x, 1^n)|) \geq n$, $q(|f(x)|) \geq |x|$.

Definiere nun

$$pad_R(x, 1^n) \stackrel{\text{df}}{=} f(pad_{\mathtt{rKAN}}(f'(x), 1^n)).$$

Die Zugehörigkeit zu $\text{Proj}(R)$ bleibt erhalten:

$$\begin{aligned} &x \in \text{Proj}(R) \iff f'(x) \in \mathtt{KAN} \iff pad_{\mathtt{rKAN}}(f'(x), 1^n) \in \mathtt{KAN} \\ &\iff f(pad_{\mathtt{rKAN}}(f'(x), 1^n)) \in \text{Proj}(R) \iff pad_R(x, 1^n) \in \text{Proj}(R). \end{aligned}$$

Ferner gilt

$$\begin{aligned} &q(q(|pad_R(x, 1^n)|)) \\ &= q(q(|f(pad_{\mathtt{rKAN}}(f'(x), 1^n)|)) \\ &\geq q(|pad_{\mathtt{rKAN}}(f'(x), 1^n)|) \\ &\geq n. \end{aligned}$$

und damit ist $pad_R$ wie gewünscht ehrlich bzgl. $n$ (mit Polynom $q \circ q$).

Es verbleibt noch die Funktion $padsol_R$. Nehme hierfür an dass wir ein $y'$ haben mit $(pad_R(x, 1^n), y') \in R$. Wir können über $g, g'$ das Zertifikat $y'$ zu Zertifikat $y$ mit $(x, y) \in R$ zurück übersetzen: Sei $p \stackrel{\text{df}}{=} pad_{\texttt{rKAN}}(f'(x), 1^n)$, dann gilt

$$(f(p), y') \in R \implies (p, \underbrace{g(p, y')}_{z}) \in \texttt{rKAN}.$$

Definiere $z = g(p, y')$. Nun haben wir

$$\begin{aligned}&(p, z) = (pad_{\texttt{rKAN}}(f'(x), 1^n), z) \in \texttt{rKAN}\\ &\quad\implies (f'(x), \underbrace{padsol_{\texttt{rKAN}}(f'(x), 1^n, z)}_{z'}) \in \texttt{rKAN}\end{aligned}$$

und mit $z' = padsol_{\texttt{rKAN}}(f'(x), 1^n, z)$ gilt

$$(f'(x), z') \in \texttt{rKAN} \implies (x, \underbrace{g'(x, z')}_{y}) \in R.$$

Es ist leicht zu sehen, dass sich eine Funktion $padsol_R \in \text{FP}$ angeben kann, die aus $x, 1^n, y'$ dieses entsprechende $y$ berechnen kann. □

Anstelle der Betrachtung, wie die *Reduktionen* zwischen den einzelnen NP-Relationen aufgebaut sind, können wir auch strukturelle Eigenschaften von NP-Relationen ausnutzen, um Paddability zu zeigen. Hierbei macht die Definition von *Universalität* durch Agrawal und Biswas (1992) aus dem Abschnitt **??** einen produktiven Beitrag. Ist eine NP-Relation *joinable*, dann können wir auch zu einer Instanz beliebig viele Dummy-Instanzen anhängen. Aufgrund der speziellen Eigenschaften der *join*-Funktion können wir auch den relevanten Teil aus Zertifikaten für die verlängerten Instanz zielgenau auslesen.

**Beobachtung 1.19.** *Jede strenge NP-Relation $R \neq \emptyset$ die* joinable *ist, ist auch Levin-paddable.*

Vor dem Beweis können wir mit dieser Aussage festhalten, dass jede universelle Relation $R$ die in Lemma 1.16 und 1.13 genannten Voraussetzungen an die NP-Relation $R$ erfüllt. Das sind nach Agrawal und Biswas (1992) u.a. `rSAT`, `rHAM`, `rINDSET`, `rKNAPSACK`, `rMAXCUT`.

*Beweis zu Beobachtung 1.19.* Sei $R$ eine NP-Relation, mit zugehörigem Polynom $q$, welches die Zertifikatsgröße spezifiziert. Zur Erinnerung, nachdem $R$ streng ist, gilt $(x, y) \in R \Rightarrow |y| = q(|x|) > 0$. Ferner haben wir eine Instanz $z \in \text{Proj}(R)$. Damit existiert also auch ein $w$ mit $(z, w) \in R$ und $q(|z|) = |w| > 0$.

Wir zeigen zunächst, wie wir für beliebige Instanz $x$ und $n \in \mathbb{N}$ auf eine Instanz $x'$ hochpadden, in dem Sinne dass $q(|x'|) \geq n$. Nach Voraussetzungen ist die Relation $R$ auch *joinable*, das heißt wir haben eine Funktion $join \in \text{FP}$. Sei

$$(x', \delta) \stackrel{\text{df}}{=} join(x, \underbrace{z, z, \dots, z}_{n \text{ mal}}).$$

Intuitiv muss nun $\delta$ (und damit $x'$) lang sein, da nun aus all den $n$ vielen Instanzen $z$ wieder das jeweilige Zertifikat aus jedem Zertifikat für $x'$ extrahiert werden muss. Nach Definition **??** gilt

$$q(|x'|) \geq |\delta| = q(|x|) + \underbrace{q(|z|) + \cdots + q(|z|)}_{n \text{ mal}} \geq n \cdot q(|z|) \geq n.$$

Sei nun *pad* genau jene polynomialzeit-berechenbare Funktion, die aus $x$ und $1^n$ die Instanz $x'$ konstruiert:

$$pad(x, 1^n) \stackrel{\text{df}}{=} x' \quad \text{wobei } (x', \delta) = join(x, \underbrace{z, z, \dots, z}_{n \text{ mal}}).$$

Dann gilt schon sofort, dass $q(|pad(x, 1^n)|) = q(|x'|) \geq n$ wie gewünscht.

Wir zeigen jetzt, dass die Zugehörigkeit zu $\text{Proj}(R)$ erhalten bleibt. Zur Erinnerung, wir haben nach Eigenschaften der *join*-Funktion

$$\{y'[\delta] \mid y' \in set\text{-}R(x')\} = \{yy_1y_2 \cdots y_n \mid y \in set\text{-}R(x), y_1, y_2, \dots, y_n \in set\text{-}R(z)\}. \tag{1.4}$$

Gilt $x \notin \text{Proj}(R)$, dann ist die rechte Menge in (1.4) leer, also auch die linke Menge und damit $x' = pad(x, 1^n) \notin \text{Proj}(R)$. Falls anders herum $x \in \text{Proj}(R)$, dann ist die rechte Menge nicht leer, existiert ja ein Zertifikat $y$ für $x$ und je ein $y_i = w$ für jedes $z$. Also ist auch die linke Menge nicht leer, damit $pad(x, 1^n) \in \text{Proj}(R)$.

Die noch verbleibende Funktion *padsol* ist durch die bitweise Projektion durch $\delta$ leicht möglich:

$$padsol(x, 1^n, y') \stackrel{\text{df}}{=} y'[\delta][0, 1, \dots, q(|x|) - 1] \quad \text{wobei } (\cdot, \delta) = join(x, \underbrace{z, z, \dots, z}_{n \text{ mal}}).$$

Wir verifizieren: Sei $(pad(x, 1^n), y') \in R$, dann ist nach (1.4) $y'[\delta] = yy_1y_2 \cdots$ wobei $(x, y) \in R$. Nachdem $R$ streng ist, gilt insbesondere $y \in \Sigma^{q(|x|)}$ und wir haben

$$padsol(x, 1^n, y') = y'[\delta][0, 1, \dots, q(|x|) - 1] = (yy_1y_2 \cdots)[0, 1, \dots, q(|x|) - 1] = y$$

und damit $(x, padsol(x, 1^n, y')) = (x, y) \in R$, wie gewünscht. □

Es bleibt die Frage offen, ob Levin-Paddability für *alle* vollständigen NP-Relationen zutrifft. Unter Annahmen einer geeigneten Einwegfunktion ist dies nicht der Fall. Die Argumentation verläuft hier ähnlich zur *Encrypted Complete Set Conjecture*. Wir setzen hier eine stärkere *secure one-way function* (Grollmann und Selman, 1988) $f$ voraus, die selbst mithilfe funktionaler Orakel-Queries nur auf einer dünnen Menge P-invertierbar ist. Präzise meinen wir damit folgendes: sei $A$ ein beliebiger Polynomialzeit-Algorithms, der auf Eingabe $w$ versucht, das Urbild $f^{-1}(w)$ zu berechnen. Zusätzlich darf $A$ das Urbild $f^{-1}(w')$ von einem Wort $w' \neq w$ erfragen. Selbst dann wird $A$ nur auf einer dünnen Menge $W \subseteq \Sigma^*$ das korrekte Urbild aller $w \in W$ bestimmen können. (Vgl. die Ähnlichkeit zur Selbstreduzierbarkeit aus Abschnitt **??**.) Die Existenz einer solchen Einwegfunktion erscheint aus kryptographischer Perspektive naheliegend.

Betrachte nun, analog zur Encrypted Complete Set Conjecture, die NP-Relation

$$Q = \{(f(\varphi), (\varphi, z)) \mid x, z \in \Sigma^*, (\varphi, z) \in \texttt{rSAT}\}.$$

Es ist leicht zu sehen dass $\texttt{rSAT} \leq_{\text{L}}^{\text{p}} Q$ und damit ist $Q$ auch $\leq_{\text{L}}^{\text{p}}$-vollständig. Gleichzeitig kann dann $Q$ nicht Levin-paddable sein. Denn angenommen, $Q$ ist Levin-paddable, dann lässt sich $f$ mit einem funktionalen Orakel-Query *zumindest auf den Werten* $f(\texttt{SAT})$ P-invertieren: gegeben $w \in f(\texttt{SAT})$, berechne erst eine zweite Instanz $w' = pad(w, 1^n) \in \text{Proj}(Q)$ mit hinreichend langem $n$ sodass $w' \neq w$. Frage dann an das Orakel und erhalte $(x', z') \in \textit{set-}Q(w')$. Dann gilt $(x, z) = padsol(w, 1^n, (x', z'))$ mit $f(x) = w$, i.e. $x$ ist das gesuchte Urbild von $w$. Wir können also auf der Bildmenge $f(\texttt{SAT})$ die Einwegfunktion $f$ invertieren. Diese Menge ist tatsächlich nicht dünn: unabhängig der gewählten Codierung von SAT folgt aus der Existenz der Einwegfunktion $f$ schon P $\neq$ NP, und damit ist insbesondere die $\leq_{\text{m}}^{\text{p}}$-vollständige Menge $f(\texttt{SAT})$ eine nicht-dünne Menge nach dem Satz von Mahaney (1982). Das widerspräche nun den Eigenschaften von $f$, also ist $Q$ nicht Levin-paddable. (Diese Argumentation relativiert, wenn anstelle rSAT eine relativierbare vollständige Menge gewählt wird, die z.B rKAN.)

Dennoch bleibt die allgemeine Frage zwischen $\leq_{\text{L}}^{\text{p}}$-Vollständigkeit und Levin-Paddability offen, die wir im Folgenden nicht weiter bearbeiten werden:

**Frage 1.20.** *Ist jede $\leq_{\text{L}}^{\text{p}}$-vollständige NP-Relation $R$ auch Levin-paddable? Existiert ggf. ein Gegenbeispiel in einer geeigneten relativierten Umgebung?*

Unabhängig von dieser Frage können wir nun aber abschließend die vorigen Ergebnisse zur Beziehung zwischen Suchproblemen und der Hypothese Q in folgendem Satz zusammenfassen. Beachte dass diese Charakterisierungen relativieren. Die Äquivalenz zu Aussage (8) ist hierbei eine einfache relativierbare Generalisierung von Beweisen durch Messner (2000, Thm. 5.3).

**Satz 1.21** (Äquivalente Formulierungen der Hypothese Q)**.** *Folgende Aussagen sind äquivalent:*

*(1) Hypothese* Q*: Für jede totale NPTM $N$ existiert eine Funktion $g \in \text{FP}$ sodass für alle $x$ das Bild $g(x)$ ein akzeptierender Rechenweg von $N(x)$ ist.*

*(2)* $\text{TFNP} \subseteq_{\text{c}} \text{FP}$

*(3)* $\mathrm{NPMV}_t \subseteq_c \mathrm{FP}$

*(4)* $\mathrm{P} = \mathrm{NP} \cap \mathrm{coNP}$ *und* $\mathrm{NPMV}_t \subseteq_c \mathrm{NPSV}_t$

*(5) Jede surjektive ehrliche Funktion* $f \in \mathrm{FP}$ *ist* P*-invertierbar, heißt die Umkehrrelation* $f^{-1}$ *hat eine Verfeinerung in* FP*.*

*(6) Für jede Menge* $L \in \mathrm{P}$ *und jede NPTM* $N$ *mit* $L(N) = L$ *existiert eine Funktion* $h \in \mathrm{FP}$ *mit*

$$x \in L \implies N(x) \text{ akz. mit Rechenweg } h(x).$$

*(7) Für jedes Paar von NP-Relationen* $A, B$ *gilt:*

$$\mathrm{Proj}(A) \leq^{\mathrm{p}}_{\mathrm{m}} \mathrm{Proj}(B) \iff A \leq^{\mathrm{p}}_{\mathrm{L}} B.$$

*(8) Für jedes Beweissystem* $h$ *gilt:* $h$ *ist optimal* $\iff$ $h$ *ist* P*-optimal.*

*(9) Es existiert eine* $\leq^{\mathrm{p}}_{\mathrm{L}}$*-vollständige Levin-paddable NP-Relation* $R$ *sodass für alle NPTM* $N$ *mit* $L(N) = \mathrm{Proj}(R)$ *auch* $std_N \leq^{\mathrm{p}}_{\mathrm{m}} std_R$ *gilt.*

*(10) Es existiert eine* $\leq^{\mathrm{p}}_{\mathrm{L}}$*-vollständige Levin-paddable NP-Relation* $R$ *für welche das Standardbeweissystem* $std_R$ P*-optimal ist.*

*Beweis.* 1. (1) $\iff$ (2) $\iff$ (4) $\iff$ (5) $\iff$ (6): nach Fenner u. a. (2003, Thm. 2).

2. (1) $\iff$ (3): nach Beobachtung **??**.

3. (1) $\iff$ (7): nach Lemma 1.1.

4. (1) $\iff$ (9) $\iff$ (10): nach Lemma 1.13 und 1.16.

5. (2) $\implies$ (8): Die Richtung von rechts nach links ist klar. Sei für die andere Richtung $h$ ein optimales Beweissystem für eine Menge $L$. Wir wollen zeigen, dass $h$ auch P-optimal ist. Sei dafür $g$ ein weiteres Beweissystem für $L$. Nach Voraussetzung kann $h$ das Beweissystem $g$ simulieren, das heißt es existiert eine (nicht notwendigerweise effiziente) Funktion $\pi$ sodass $g(w) = h(\pi(w))$, und gleichzeitig ist $|\pi(w)| \leq q(|w|)$ für ein geeignetes Polynom $q$.

Betrachte folgende Multifunktion $f'$:

$$\textit{set-}f'(w) \stackrel{\mathrm{df}}{=} \{y \mid \exists y \in \Sigma^{\leq q(|w|)}, g(w) = h(y)\}.$$

Es lässt sich leicht zeigen, dass $f' \in \mathrm{NPMV}$, über einen geeigneten NPTM-Transduktor. Es ist sogar $f' \in \mathrm{NPMV}_t$, denn für jedes $w$ mindestens $\pi(w) \in \textit{set-}f'(w)$.

Nach (2) gilt also $f' \in \mathrm{NPMV}_t \subseteq_c \mathrm{FP}$, also existiert eine Funktion $f'' \in \mathrm{FP}$ welche eine Verfeinerung von $f'$ ist. Diese Funktion übersetzt $g$-Beweise $w$ für $x$ effizient in $h$-Beweise für $x$: Sei $g(w) = x$, dann gilt

$$f''(w) = y \quad \text{mit } y \in \textit{set-}f'(w), \text{ also gilt } y \in \Sigma^{\leq q(|w|)}, x = g(w) = h(y).$$

Damit ist $h(f''(w)) = x$ bzw. $f''(w)$ ein $h$-Beweis für $x$, wie gewünscht.

6. (8) $\implies$ (10): klar, denn $\mathtt{rKAN}$ ist $\leq^{\mathrm{p}}_{\mathrm{L}}$-vollständig, ist Levin-paddable, und das Standardbeweissystem $std_{\mathtt{rKAN}}$ ist (wie jedes Standardbeweissystem einer NP-Relation) optimal. Zusammen mit (7) ist es also auch P-optimal. □

Analysiert man die Beweise bezüglicher der Äquvalenz von Aussage Q zu (9) und (10) können wir sogar feststellen, dass die Wahl der Relation $R$ beliebig ist. Wir können daher Q über universell quantifizierte Varianten von (9) und (10) charakterisieren.

**Satz 1.22.** *Entweder gelten die Aussagen (1), (9), (10) oder die Aussagen (1'), (9'), (10'):*

*(1)* Q.

*(9)* *Für alle $\leq_L^p$-vollständigen Levin-paddable NP-Relationen $R$, alle NPTM $N$ mit $L(N) = \mathrm{Proj}(R)$ gilt $std_N \leq_m^p std_R$.*

*(10)* *Für alle $\leq_L^p$-vollständigen Levin-paddable NP-Relationen $R$ ist das Standardbeweissystem $std_R$ P-optimal.*

*(1′)* $\neg$Q.

*(9′)* *Es existiert keine $\leq_L^p$-vollständige Levin-paddable NP-Relation $R$, sodass für alle NPTM $N$ mit $L(N) = \mathrm{Proj}(R)$ auch $std_N \leq_m^p std_R$ gilt.*

*(10′)* *Es existiert keine $\leq_L^p$-vollständige Levin-paddable NP-Relation $R$ ist das Standardbeweissystem $std_R$ P-optimal.*

*Beachte dass (9′) nicht die negierte Version von (9) ist, für (10) gilt dies analog.*

## 1.3 *Bekannte Implikationen und Orakel, offene Trennungen*

Im letzten Abschnitt dieses Kapitels werden wir nun die in Abbildung 1 abgebildeten Implikationen und Äquivalenzen nachweisen. Damit werden insbesondere auch die Hypothesen Q und KvL in das Pudláksche Programm eingeordnet. Zum Schluss wird noch angegeben, welche der Hypothesen im (vergrößertem) Pudlákschen Programm durch ein Orakel separiert sind, und welche Separierungen noch offen sind.

Zunächst führen wir noch eine abgeschwächte Variante von Q ein, die von Fenner u. a. (2003) vorgeschlagen wurde.

**Vermutung 1.23** (Q′, Fenner u. a., 2003)**.** *Für jede totale NPTM $N$ existiert eine Funktion $g \in$ FP sodass für alle $x$ das Bild $g(x) \in \{0,1\}$ das erste Bit eines akzeptierenden Rechenwegs von $N(x)$ ist.*

Jetzt können wir auch die in Abbildung 1 abgebildeten Implikationen und Äquivalenzen nachweisen.

**Satz 1.24.** *Es gelten die in Abbildung 1 abgebildeten Implikationen und Äquivalenzen.*

*Beweis.* Es gelten die notierten Äquivalenzen:
1. $\neg$Q $\Leftrightarrow$ $\exists$ optimales Beweissystem was nicht P-optimal ist $\Leftrightarrow$ TFNP $\not\subseteq_c$ FP, nach Satz 1.21.
2. $\neg$Q′ $\Leftrightarrow$ $\exists$ P-inseparierbares DisjCoNP-Paar, nach Fortnow und Rogers (1993, Lemma 2.12, vgl. Appendix).
3. NP $\cap$ coNP $\neq$ P $\Leftrightarrow$ NPSV$_t \not\subseteq$ FP, nach Fenner u. a. (2003, Prop. 1).
4. UP $\neq$ P $\Leftrightarrow$ $\exists$ Einwegfunktionen, nach Grollmann und Selman (1988, Thm. 10).
5. UP $\cap$ coUP $\neq$ P $\Leftrightarrow$ $\exists$ Einwegpermutationen, nach Homan und Thakur (2003).
6. NP $\cap$ coNP $\Leftrightarrow$ NPSV$_t$ hat keine vollständige Funktion, nach Beyersdorff, Köbler und Messner (2009, Prop. 3).
7. DisjNP $\Leftrightarrow$ NPSV hat keine vollständige Funktion, nach Glaßer, Selman und Sengupta (2005, Thm. 9).

Es gelten die eingezeichneten Implikationen:
1. DisjNP $\Rightarrow$ TAUT$^N$ nach Köbler, Messner und Torán (2003, Cor. 6.1).
2. UP $\Rightarrow$ TAUT nach Köbler, Messner und Torán (2003, Cor. 4.1).
3. TAUT$^N$ $\Rightarrow$ NEE $\neq$ coNEE nach Köbler, Messner und Torán (2003, Cor. 7.1).
4. NP $\cap$ coNP $\neq$ P $\Rightarrow$ $\neg$Q′ $\Rightarrow$ NPMV$_t \not\subseteq_c$ TFNP $\Rightarrow$ $\neg$Q nach Fenner u. a. (2003, Prop. 9, Thm. 6).
5. E $\neq$ NE $\Rightarrow$ $\exists$ NP-Relation die nicht auf Entscheidung reduzierbar ist, nach Impagliazzo und Sudan (1991).
6. UP $\neq$ P $\Rightarrow$ $\exists$ P-inseparierbares DisjNP-Paar, nach Grollmann und Selman (1988, Thm. 5).
7. NP $\cap$ coNP $\Rightarrow$ TAUT $\vee$ SAT nach Köbler, Messner und Torán (2003, Cor. 5.1).

8. $\mathrm{NPMV_t}$ hat keine vollständige Funktion $\Rightarrow$ SAT nach Beyersdorff, Köbler und Messner (2009, Thm. 25). Es ist leicht zu sehen, dass der Beweis auch auf unsere relativierte Variante von SAT generalisiert.
9. $\mathrm{NPMV_t}$ hat keine vollständige Funktion $\Rightarrow$ NP $\neq$ coNP nach Satz 1.25.
10. $\mathsf{SAT}^{\mathsf{eff}} \Rightarrow$ SAT, $\mathsf{SAT}^{\mathsf{eff}} \Rightarrow$ KvL, nach Satz 1.11.
11. KvL $\Rightarrow \neg$Q, nach Satz 1.6.
12. $\neg$Q $\Rightarrow \exists$ NP-Relation die nicht auf Entscheidung reduzierbar ist, denn unter $\neg$Q gilt mit Satz 1.21 auch die Negation von 1.21(1), also eine NPTM $N$ mit $L(N) = \Sigma^*$ wobei keine Funktion $g \in$ FP existiert, welche für alle $x$ durch $g(x)$ einen akzeptierenden Rechenweg von $N(x)$ bestimmt. Definiere die NP-Relation $R_N$ mit $(x, \alpha) \in R_N$ genau dann wenn $N(x)$ mit Rechenweg $\alpha$ existiert. Nun gilt nach Vorigem auch $R \notin_{\mathrm{c}} \mathrm{FP} = \mathrm{FP}^{\Sigma^*} = \mathrm{FP}^{L(R)}$.
13. DisjCoNP $\Rightarrow$ TFNP $\Rightarrow$ $\mathrm{NPMV_t}$ hat keine vollständig Funktion, nach Pudlák (2017, Prop. 5.6, 5.10).
14. NP $\cap$ coNP $\neq$ P $\Rightarrow \exists$ P-inseparierbares DisjNP-Paar, denn wenn alle DisjNP-Paare P-separierbar, dann ist auch für jede Menge $L \in$ NP $\cap$ coNP jeweils das DisjNP-Paar $(L, \overline{L})$ P-separierbar und damit $L \in$ P.
15. DisjNP $\Rightarrow \exists$ P-inseparierbares DisjNP-Paar; ist klar, denn wenn alle DisjNP-Paare P-separierbar wären, dann wären auch alle Paare trivialerweise $\leq_{\mathrm{m}}^{\mathrm{pp}}$-vollständig.
16. DisjCoNP $\Rightarrow \exists$ P-inseparierbares DisjCoNP-Paar; ist aus selben Gründen klar.
17. $\mathsf{TAUT}^{\mathsf{N}} \Rightarrow$ TAUT klar, weil aus P-Optimalität auch Optimalität folgt.
18. SAT $\Rightarrow \neg$Q klar: wen Q, dann ist nach Satz 1.21 jedes optimale Beweissystem auch P-optimal. Dann gilt auch $\neg$SAT: jede Menge $L \in$ NP hat ein optimales Beweissystem $h$ (Beobachtung **??**) und das ist nach Voraussetzung P-optimal.
19. UP $\Rightarrow$ UP $\neq$ P klar.
20. NP $\cap$ coNP $\Rightarrow$ NP $\cap$ coNP $\neq$ P klar.
21. NP $\cap$ coNP $\Rightarrow$ NP $\neq$ coNP klar, denn wenn NP $=$ coNP dann ist NP $\cap$ coNP $=$ NP und damit existiert auch eine vollständige Menge.
22. $\exists$ P-inseparierbares DisjNP-Paar $\Rightarrow$ P $\neq$ NP klar.
23. UP $\cap$ coUP $\neq$ P $\Rightarrow$ UP $\neq$ P, UP $\cap$ coUP $\Rightarrow$ NP $\cap$ coNP $\neq$ P klar.
24. NEE $\neq$ coNEE $\Rightarrow$ NE $\neq$ coNE $\Rightarrow$ NP $\neq$ coNP $\Rightarrow$ P $\neq$ NP klar.
25. NEE $\neq$ coNEE $\Rightarrow$ EE $\neq$ NEE $\Rightarrow$ E $\neq$ NE klar. □

Der verbleibende Beweis ist eine Generalisierung von Dingel (2022).

**Satz 1.25.** *Wenn* NP $=$ coNP *dann existiert eine* $\leq_{\mathrm{m}}^{\mathrm{p}}$*-vollständige Multifunktion* $f$ *für* $\mathrm{NPMV_t}$.

*Beweis.* Nach Voraussetzung können wir in NP testen, ob ein Wort $x$ im Urbild einer beliebigen NPMV-Multifunktion liegt. Es gilt $\mathtt{KAN} \in$ NP und damit $\mathtt{KAN} \in$ coNP. Insbesondere ist dann die Menge

$$U \stackrel{\mathrm{df}}{=} \{(T, x, 1^n) \mid T \text{ ist ein NPTM-Transduktur und akz. } x \text{ auf keinem Rechenweg der Länge} \leq n\} \in \mathrm{NP},$$

und wird von der NPTM $N_u$ in Laufzeit $q(|(T, x, 1^n)|)$ entschieden.

Betrachte nun die Multifunktion $f$, die durch folgenden nichtdeterministischen Transduktor $T'(T, x, 1^n)$ berechnet wird:

**wenn** $T$ kein Transduktor ist **dann** Gebe $\varepsilon$ aus
Rate nichtdeterministisch einen Rechenweg $\alpha$ von $T$ der Länge $\leq n$
Rate nichtdeterministisch einen Rechenweg $\beta$ von $N_u$ der Länge $\leq q(|(T, x, 1^n)|)$
**wenn** $T(x)$ auf $\alpha$ nicht terminiert, heißt ein weiterer Rechenschritt ist möglich **dann** Gebe $\varepsilon$ aus
**sonst wenn** $T(x)$ mit $\alpha$ akzeptiert **dann**
    $y \leftarrow$ Ausgabe von $T(x)$ auf $\alpha$
    Gebe $y$ aus
**sonst wenn** $N_u(i, x, 1^n)$ mit $\beta$ akzeptiert **dann** Gebe $\varepsilon$ aus
**sonst** Lehne ab

Es ist leicht zu sehen dass $T'$ in Polynomialzeit arbeitet. Wir charakterisieren nun die Outputs von $T'$ in Abhängigkeit der Eingabe $(T, x, 1^n)$. Es gilt nun:

- Falls ein Rechenweg von $T(x)$ mit $> n$ Schritten existiert, dann terminiert $T$ auf mindestens einem Rechenweg in in Z. 6 und wir haben $\textit{set-}f(T, x, 1^n) \subseteq \{\varepsilon\}$.
- Falls $\textit{set-}T(x) \neq \emptyset$ und die Laufzeit von $T(x)$ auf $n$ Schritte beschränkt ist, dann existiert für jedes $y \in \textit{set-}T(x)$ ein akzeptierender Rechenweg $\alpha$ der Länge $\leq n$ auf $T$ der $y$ ausgibt. Damit wird auch $f$ dieses $y$ in Z. 9 ausgeben. Gleichzeitig ist damit $(T, x, 1^n) \notin U$ und Z. 11 niemals erreicht. Ebenso ist jeder geratene Rechenweg $\alpha$ ein terminierender Rechenweg auf $T(x)$, alsowird auch Z. 6 niemals erreicht. Es gilt also $\textit{set-}f(T, x, 1^n) = \textit{set-}T(x)$.
- Oder es gilt $\textit{set-}T(x) = \emptyset$. Dann wird jeder Rechenweg der Länge $\leq n$ von $T(x)$ terminieren und ablehnen, und $f$ definitiv nicht in Z. 6 oder Z. 8 akzeptieren. Andererseits gilt dann $(T, x, 1^n) \in U$ und Z. 11 wird auf mindestens einem Rechenweg von $f$ erreicht. Es gilt also $\textit{set-}f(T, x, 1^n) = \{\varepsilon\}$.

Damit ist klar, dass $f \in \mathrm{NPMV}_t$. Wir zeigen nun, dass $f$ auch $\mathrm{NPMV}_t$-vollständig ist. Sei hierfür $g$ eine beliebige Multifunktion aus $\mathrm{NPMV}_t$. Dann existiert auch ein NPTM-Transdutkor $T_g$ sodass dieser $g$ in berechnet, und dabei terminiert $T_g(x)$ in $\leq p(|x|)$ vielen Schritten für geeignetes Polyom $p$.

Nun gilt nach obiger Beobachtung schon dass

$$\textit{set-}g(x) = \textit{set-}T_g(x) \neq \emptyset \implies \textit{set-}f(\underbrace{T_g, x, 1^{p(|x|)}}_{h(x)}) = \textit{set-}T(x) = \textit{set-}g(x)$$

und $h(x) = (T_g, x, 1^{p(|x|)})$ realisiert die Reduktion von $g$ auf $f$, wie gewünscht. □

Abbildung 2 zeigt, welche Hypothesen unter relativierbaren Beweisen durch ein Orakel voneinander getrennt sind. Beachte, dass im Gegensatz zur Abbildung 1 aus Übersichtlichkeit einige Hypothesen ausgelassen wurden, nämlich jene der Exponentialzeitklassen, und jene der Reduzierbarkeit von Such- auf Entscheidungsprobleme. Das blau hervorgehobene Orakel $O$ wird im folgenden Kapitel 2 konstruiert, vgl. Satz 2.1.

Für viele Paare von Hypothesen A, B haben wir damit entweder eine relativierende Implikation $\mathsf{A} \Rightarrow \mathsf{B}$ oder es existiert ein Orakel welches A und B trennt, also ein Orakel relativ zu diesem $\mathsf{A} \wedge \neg\mathsf{B}$ gilt, und damit einen relativierenden Beweis für diese Implikation ausschließen.

Wir wollen hierbei die Stellung von Q hervorheben: mittels Orakelkonstruktionen erkennen wir eine weitestgehende Unabhängigkeit zwischen der Hypothese $\neg$Q auf der einen Seite und den anderen Hypothesen des Pudlákschen Programms. Zum einen wissen wir über ein Orakel von Fenner u. a. (2003, Thm. 12.3, Nr. 8 in der Abb.), dass die Annahme von $\mathrm{UP} \neq \mathrm{P} \wedge \mathrm{NP} \neq \mathrm{coNP}$ unter relativierenden Beweisen nicht ausreicht, um $\neg$Q zu zeigen, also diese Annahme auch nicht ausreicht um KvL zu zeigen. Auf ähnliche Weise ergibt sich aus dem in Kapitel 2 konstruierten Orakel ($O$ in der Abb.), dass auch die Annahme DisjNP$\wedge$UP nicht ausreicht, um $\neg$Q zu zeigen. Symmetrisch sehen wir über zwei Orakel von Dose (2020a, Cor. 3.3, 2020b, Thm. 3.2, siehe Nr. 5 u. 6 in der Abb.) dass die Annahme $\neg$Q (bzw. sogar die stärkere Annahme $\neg$Q′) nicht ausreicht, um TAUT bzw. SAT zu zeigen, also auch nicht um die stärkeren ursprünglichen Pudlákschen Hypothesen (DisjNP, UP, DisjCoNP, usw.) zu beweisen.

Teile dieser Beobachtung übertragen sich entsprechend auch auf die Verstärkung KvL von $\neg$Q. Weder $\mathrm{UP} \neq \mathrm{P} \wedge \mathrm{NP} \neq \mathrm{coNP}$ noch DisjNP $\wedge$ UP reicht als Annahme aus, um relativierend KvL zu berweisen. Damit wissen wir zumindest schon, dass KvL (wieder unter relativierenden Beweisen) nicht äquivalent zu einer der Aussagen „$\mathrm{UP} \neq \mathrm{P}$“, „$\mathrm{NP} \neq \mathrm{coNP}$“, DisjNP, UP ist. Andererseits wären einige weitere Orakel wünschenswert, um KvL besser zu situieren. Existiert ein Orakel relativ zu diesem KvL (also relativierende Beweise für $\neg$KvL ausschließt)? Existiert ein Orakel relativ zu diesem KvL $\wedge$ Q (und damit KvL von Q trennt)?

In diesem Sinne können wir auch allgemein fragen, für welche Paare A, B von Hypothesen sowohl unbekannt ist, ob $A \Rightarrow B$ über einen relativierbaren Beweis, noch ob ein Orakel existiert relativ zu diesem $\mathsf{A} \wedge \neg\mathsf{B}$. Das sei im Folgenden nun abschließend noch zusammengefasst (vgl. Tabelle 1.

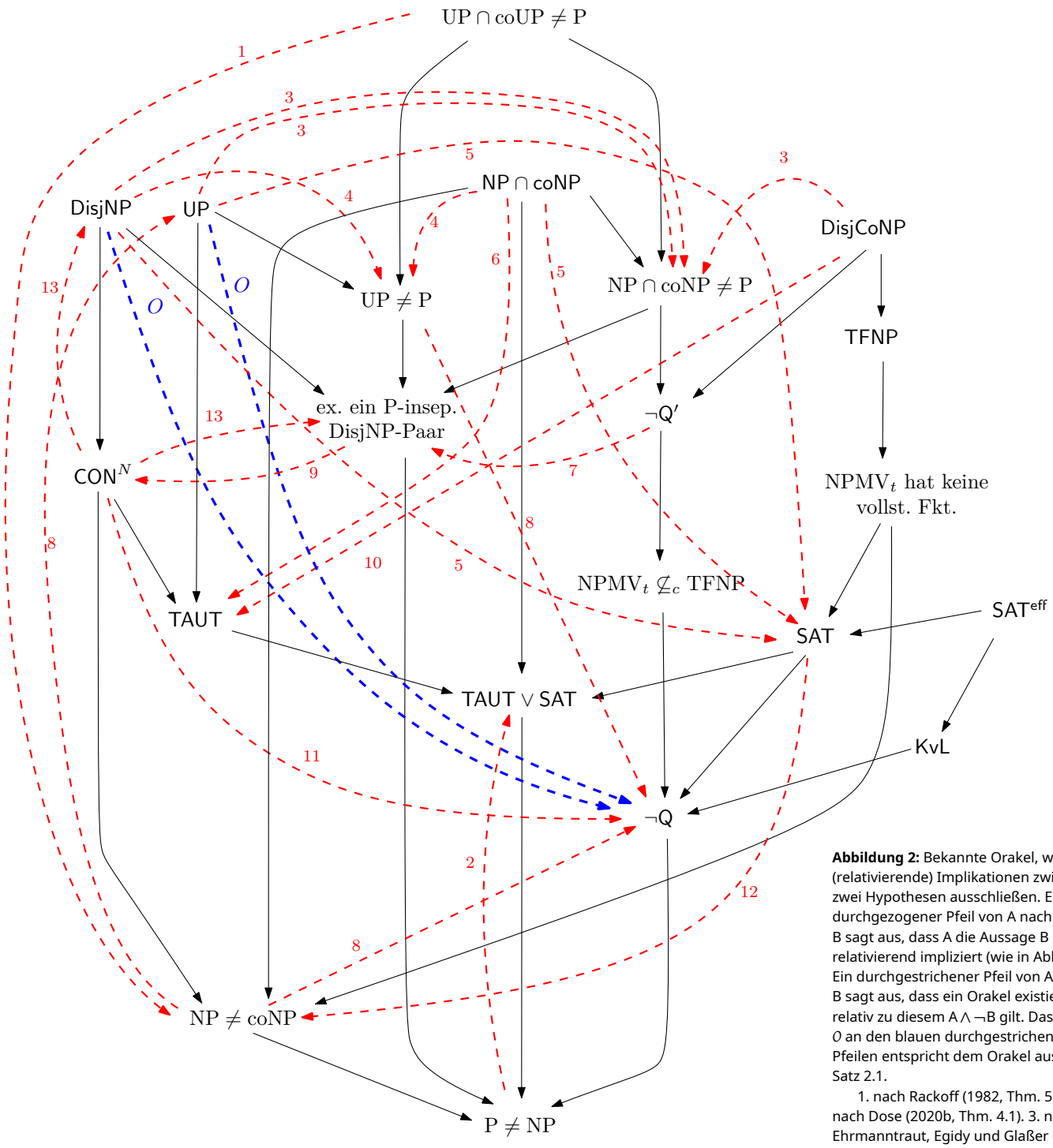



**Abbildung 2:** Bekannte Orakel, welche (relativierende) Implikationen zwischen zwei Hypothesen ausschließen. Ein durchgezogener Pfeil von A nach B sagt aus, dass A die Aussage B relativierend impliziert (wie in Abb. 1). Ein durchgestrichener Pfeil von A nach B sagt aus, dass ein Orakel existiert, relativ zu diesem $A \wedge \neg B$ gilt. Das Orakel $O$ an den blauen durchgestrichenen Pfeilen entspricht dem Orakel aus Satz 2.1.

1. nach Rackoff (1982, Thm. 5). 2. nach Dose (2020b, Thm. 4.1). 3. nach Ehrmanntraut, Egidy und Glaßer (2022, Thm. 9). 4. nach Dose und Glaßer (2019, Thm. 4.1). 5. nach Dose (2020a, Cor. 3.3). 6. nach Dose (2020b, Thm. 3.2). 7. nach Fortnow und Rogers (2002, Thm. 3.2). 8. nach Fenner u. a. (2003, Thm. 12.3). 9. nach Glaßer, Selman, Sengupta und Zhang (2004, Cor. 6.6). 10. nach Khaniki (2022, Thm. 5.1). 11. nach Khaniki (2022, Thm. 5.2). 12. nach Dingel (2022, Satz 3.12). 13. nach Glaßer, Selman, Sengupta und Zhang (2004, Cor. 6.34).

- Unter dem ursprünglichen Hypothesen des Pudlákschen Programms (SAT, TAUT, $\mathsf{CON}^{\mathsf{N}}$, Vollständigkeit von DisjNP, DisjCoNP, UP, NP $\cap$ coNP, TFNP, $\mathrm{NPMV}_t$, Kollaps NP $=$ coNP, NP $\cap$ coNP $=$ P; die zusammengesetzte Hypothese SAT $\vee$ TAUT diskutieren wir hier dagegen noch nicht) kennen wir für fast alle Paare an Hypothesen eine relativierende Implikation oder ein entsprechendes Orakel, relativ zu diesem die Implikation nicht gilt. Offen bleiben nur diese neun Paare:

  (i) TAUT $\stackrel{?}{\Rightarrow}$ $\mathsf{CON}^{\mathsf{N}}$,
  (ii) TAUT $\stackrel{?}{\Rightarrow}$ NP $\neq$ coNP,
  (iii) UP $\stackrel{?}{\Rightarrow}$ $\mathsf{CON}^{\mathsf{N}}$,
  (iv) UP $\stackrel{?}{\Rightarrow}$ DisjNP,
  (v) UP $\stackrel{?}{\Rightarrow}$ NP $\neq$ coNP,
  (vi) „$\mathrm{NPMV}_t$ hat keine vollst. Fkt.“ $\stackrel{?}{\Rightarrow}$ TFNP,
  (vii) TFNP $\stackrel{?}{\Rightarrow}$ DisjCoNP,
  (viii) „$\mathrm{NPMV}_t$ hat keine vollst. Fkt.“ $\stackrel{?}{\Rightarrow}$ DisjCoNP.

  Ein Orakel für (ii) wäre insbesondere auch ein Orakel für (iii)–(vi); ein Orakel für (vi) oder (vii) wäre insbesondere auch ein Orakel für (viii).

- Erweitern wir den Blick um Q und verwandte Hypothesen Q′, „$\mathrm{NPMV}_t \not\subseteq_c$TFNP“, so entstehen einige neue Paare A, B, für die unbekannt ist ob ein Orakel diese trennt oder ob ein Beweis einer relativierbare Implikation existiert, z.B. TFNP $\stackrel{?}{\Rightarrow} \neg$Q′. Beachte aber, dass für jedes dieser offenen Paare A, B (mit A oder B in {Q, Q′, „$\mathrm{NPMV}_t \not\subseteq_c$TFNP“}) die Konstruktion eines Orakes *O* mit A $\wedge \neg$B höchstwahrscheinlich sehr schwierig ist: für jedes offene Paar A, B lässt sich verifizieren, dass relativ zu einem trennenden Orakel *O* auch Q′ $\wedge \neg$Q gilt. Damit trennt *O* insbesondere Q und Q′ unter relativierenden Beweisen, und würde eine seit 28 Jahren offene Frage von Fenner u. a. (2003, vgl. auch 1996) beantworten. Das entspricht genau jenen offenen Orakelkonstruktionen, die in Tabelle 1 mit † markiert sind.

- Ergänzen wir weiter mit dem Kollaps „UP $=$ P“ und der P-Separierbarkeit von DisjNP-Paaren entstehen weiter neue offenen Paare A, B von Hypothesen, unter anderem

  (ix) DisjCoNP $\stackrel{?}{\Rightarrow}$ „DisjNP inseparierbar“,
  (x) $\mathsf{CON}^{\mathsf{N}} \stackrel{?}{\Rightarrow}$ „DisjNP inseparierbar“,
  (xi) UP $\neq$ P $\stackrel{?}{\Rightarrow}$ TAUT

  Dies sind die drei „stärksten“ Implikationen bzw. diejenigen Paare an Hypothesen, deren Orakelkonstruktionen gegen diese Implikationen am „schwierigsten“ ist. Gemeint ist, dass sämtliche anderen offenen Paare A, B mit A oder B in {„UP $\neq$ P“, „DisjNP insep.“} dann auch durch eines dieser Orakel getrennt wird, die (ix), (x), und (xi) trennen.

- Ergänzen wir nun abschließend mit den hier neu definierten Hypothesen KvL und $\mathsf{SAT}^{\mathsf{eff}}$ entstehen wieder neue Paare A, B für die offen ist, ob A die Hypothese B impliziert, oder ob ein Orakel gegen diese Implikation existiert. Das gilt für so gut wie alle möglichen Paare zwischen KvL bzw. $\mathsf{SAT}^{\mathsf{eff}}$ und den übrigen betrachteten Hypothesen. Besonders im Hinblick auf den Schwerpunkt dieser Arbeit auf Suchprobleme und auf die Hypothese KvL sind die folgenden Paare interessant:

  (xii) KvL $\stackrel{?}{\Rightarrow}$ $\mathsf{SAT}^{\mathsf{eff}}$,
  (xiii) KvL $\stackrel{?}{\Rightarrow}$ SAT (oder stärker SAT $\vee$ TAUT),
  (xiv) DisjCoNP $\stackrel{?}{\Rightarrow}$ KvL (oder schwächer $\neg$Q $\stackrel{?}{\Rightarrow}$ KvL).

  Diese Fragen werden im Folgenden nicht weiter untersucht. Stattdessen seien sie hier als zukünftige Forschungsdesiderata formuliert: zeige dass eine der obigen Implikationen gilt, gebe ein Gegenbeispiel an, oder konstruiere ein Orakel relativ zu diesem eine der obigen Implikationen nicht gilt.

- Schließlich gehen wir noch auf die zusammengesetzte Hypothese TAUT $\vee$ SAT ein. Zur Erinnerung: diese Hypothese besagt (in Verbindung mit Korollar **??**), dass eine Menge

$L \in \mathrm{NP} \cup \mathrm{coNP}$ existiert für die kein P-optimales Beweissystem existiert. Trotz der zusammengesetzten Natur dieser Hypothese lässt sich zeigen, dass $\mathsf{TAUT} \vee \mathsf{SAT}$ äquivalent zu weiteren natürlichen Hypothesen ist. Zum einen zeigt Khaniki (2022, Thm. 3.2) die Äquivalenz zur Hypothese $\mathsf{RFN}_1$ betreffend der Beweisbarkeit endlicher Widerspruchsfreiheit (Pudlák, 2017, vgl.). Zum anderen geben Egidy, Glaßer und Herold (2023) eine Verbesserung der ersten genannten Charakterisierung an, hierbei bezogen auf die Mengen der Boolschen Hierarhie (BH, vgl. Cai und Hemachandra, 1986; Cai, Gundermann u. a., 1988, 1989). Aufbauend auf Ergebnissen von Köbler, Messner und Torán (2003) ergibt sich, dass $\mathsf{TAUT} \vee \mathsf{SAT}$ genau dann gilt wenn sogar eine Menge $L \in \mathrm{BH} \supseteq \mathrm{NP} \cup \mathrm{coNP}$ existiert für die es kein P-optimales Beweissystem gibt.

Auf diese beiden Charakterisierungen soll hier aber nicht weiter eingegangen werden. Trotzdem sei hier noch knapp die Beziehung der Hypothese zu den anderen (unter relativierbaren Beweisen) erläutert. Einerseits existieren Orakel, sodass $(\mathsf{TAUT} \vee \mathsf{SAT}) \wedge \neg \mathsf{A}$ für alle bisher genannten Hypothesen A (außer $\mathrm{P} \neq \mathrm{NP}$, was trivialerweise eine notwendige Bedingung ist) . Andererseits bleibt für viele Hypothesen noch offen, ob diese hinreichend für $\mathsf{TAUT} \vee \mathsf{SAT}$ sein könnten. Insbesondere sind folgende Paare noch offen:

(xv) $\mathrm{UP} \cap \mathrm{coUP} \neq \mathrm{P} \stackrel{?}{\Rightarrow} \mathsf{TAUT} \vee \mathsf{SAT}$,
(xvi) $\mathsf{KvL} \stackrel{?}{\Rightarrow} \mathsf{TAUT} \vee \mathsf{SAT}$.

Hiermit wollen wir die Diskussion über die Beziehungen der Hypothesen des erweiterten Pudlákschen Programms abschließen. Im folgenden Kapitel werden wir nun noch das angekündigte Orakel $O$ konstruieren.

| Antezendent A \ Konsequent B | TAUT | $\mathsf{CON}^{\mathsf{N}}$ | DisjNP | UP | SAT | $\mathrm{NPMV_t}$ unvollst. | TFNP | DisjCoNP | NP ∩ coNP | NP ≠ coNP | NP ∩ coNP ≠ P | ¬Q | ¬Q′ | $\mathrm{NPMV_t} \not\subseteq_{\mathrm{t}}$ TFNP | UP ≠ P | DisjNP unsep. | KvL | $\mathsf{SAT}^{\mathsf{eff}}$ | TAUT ∨ SAT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| TAUT | | ? | 13 | 4 | 0 | 0 | 0 | 0 | 0 | ? | 0 | 0 | 0 | 0 | 4 | 13 | 0 | 0 | |
| $\mathsf{CON}^{\mathsf{N}}$ | | | 13 | 4 | 0 | 0 | 0 | 0 | 0 | | 0 | 0 | 0 | 0 | 4 | ***13*** | 0 | 0 | |
| DisjNP | | | | 4 | 0 | 0 | 0 | 0 | 0 | | 0 | ***0*** | 0 | 0 | ***4*** | | 0 | 0 | |
| UP | | ? | ? | | 0 | 0 | 0 | 0 | 0 | ? | 0 | ***0*** | 0 | 0 | | | 0 | 0 | |
| SAT | 10 | 10 | 10 | 10 | | 12 | 12 | 12 | 3 | ***12*** | 3 | | † | † | ? | ? | ? | ? | |
| $\mathrm{NPMV_t}$ unvollst. | 10 | 10 | 10 | 10 | | | ? | ? | 3 | | 3 | | † | † | ? | ? | ? | ? | |
| TFNP | 10 | 10 | 10 | 10 | | | | ? | 3 | | 3 | | † | † | ? | ? | ? | ? | |
| DisjCoNP | ***10*** | 10 | 10 | 10 | | | | | 3 | | ***3*** | | | | ? | ? | ? | ? | |
| NP ∩ coNP | ***6*** | 6 | 6 | 4 | ***5*** | 5 | 5 | 5 | | | | | | | ***4*** | | ? | 5 | |
| NP ≠ coNP | 6 | 6 | 6 | 4 | 0 | 0 | 0 | 0 | 0 | | 0 | 0 | 0 | 0 | 4 | 13 | 0 | 0 | ? |
| NP ∩ coNP ≠ P | 6 | 1 | 1 | 4 | 5 | 1 | 1 | 1 | 1 | 1 | | | | | 4 | | ? | 5 | ? |
| ¬Q | 6 | 1 | 1 | 4 | 5 | 1 | 1 | 1 | 1 | 1 | 3 | | † | † | 4 | 7 | ? | 5 | ? |
| ¬Q′ | 6 | 1 | 1 | 4 | 5 | 1 | 1 | 1 | 1 | 1 | 3 | | | | 4 | ***7*** | ? | 5 | ? |
| $\mathrm{NPMV_t} \not\subseteq_{\mathrm{t}}$ TFNP | 6 | 1 | 1 | 4 | 5 | 1 | 1 | 1 | 1 | 1 | 3 | | † | | 4 | 7 | ? | 5 | ? |
| UP ≠ P | ? | 1 | 1 | ? | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | | | 0 | 0 | ? |
| DisjNP unsep. | 6 | 1 | 1 | 4 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 4 | | 0 | 0 | ? |
| KvL | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | | † | † | ? | ? | | ? | ? |
| $\mathsf{SAT}^{\mathsf{eff}}$ | ? | ? | ? | ? | | ? | ? | ? | ? | ? | ? | | † | † | ? | ? | | | |
| TAUT ∨ SAT | 6 | 6 | 6 | 4 | 0 | 0 | 0 | 0 | 0 | 12 | 0 | 0 | 0 | 0 | 4 | 13 | 0 | 0 | |

**Tabelle 1:** Überblick über Orakel, welche Impliationen $\mathsf{A} \Rightarrow \mathsf{B}$ zwischen den betrachteten Hypothesen unter relativierbaren Beweisen trennen, in dem Sinn dass ein Orakel existiert relativ zu diesem $\mathsf{A} \wedge \neg \mathsf{B}$ gilt. Jede Zelle entspricht hierbei einer solchen Implikation. Die Hypothese A links ist hierbei der Antezendent, die Hypothese B oben der Konsequent.

Leere Zellen bedeuten, dass kein Orakel mit $\mathsf{A} \wedge \neg \mathsf{B}$ existiert, enn es existiert nein relativierender Beweis für $\mathsf{A} \Rightarrow \mathsf{B}$.

Eine Zahl (bzw. $O$) in der Zelle bedeutet, dass relativ zu einem Orakel $\mathsf{A} \wedge \neg \mathsf{B}$ gilt, also ein Orakel gegen die Impliakation $\mathsf{A} \Rightarrow \mathsf{B}$. Die Zahl gibt hierbei an, um welches Orakel es sich aus Abb. 2 handelt, das Label $O$, dass es sich um das konstruierte Orakel aus Kapitel 2 handelt. Ist die Zahl (bzw. $O$) fett gedruckt, dann entspricht das Orakel genau dem Eingezeichneten, ansonsten folgt die behauptete Eigenschaft aus relativierbaren Implikationen zwischen den Hypothesen.

Ein rotes ? bedeutet, dass unbekannt ist, ob ein solches Orakel existiert.

Ein rotes † bedeutet, dass auch unbekannt ist, ob ein solches Orakel $D$ existiert. Hierbei ist aber die Konstruktion besonders schwierig: wenn nämlich ein solches Orakel existiert, also $\mathsf{A} \wedge \neg \mathsf{B}$ relativ zu $D$ gilt, dann muss auch $\mathsf{Q}' \wedge \neg \mathsf{Q}$ relativ zu $D$ gelten.

# 2 *Orakel mit* DisjNP, UP *und* Q

Ziel dieses Kapitels ist die Konstruktion eines Orakels $O$, relativ zu dem einerseits die Hypothesen DisjNP und UP gilt, andererseits auch die Hypothese Q gilt. Damit wird ausgeschlossen, dass ¬Q nicht mit relativierenden Mitteln beweisen werden kann, selbst unter Annahme der starken, aber wahrscheinlichen Annahme DisjNP ∧ UP. Dies verbessert auch ein Ergebnis von Dose (2020a, Cor. 3.3), welcher ein ähnliches Orakel konstruiert, relativ zu diesem DisjNP ∧ UP ∧ ¬SAT gilt.

Präzise werden wir folgenden Satz beweisen:

**Satz 2.1.** *Es existiert ein Orakel $O$ sodass folgende Aussagen gelten:*

*(1) Für jede totale NPTM $N$ existiert eine Funktion $g \in \mathrm{FP}^O$ sodass $g(x)$ ein akzeptierender Rechenweg von $N^O(x)$ ist (was äquivalent zu* Q *relativ zu $O$ ist).*

*(2) Es existiert kein $\leq_m^{\mathrm{pp},O}$-hartes Paar in $\mathrm{DisjNP}^O$ für $\mathrm{DisjUP}^O$ (was* DisjNP *relativ zu $O$ impliziert).*

*(3) Es existiert keine $\leq_m^{\mathrm{p},O}$-vollständige Menge für $\mathrm{UP}^O$ (was äquivalent zu* UP *relativ zu $O$ ist).*

Die Orakelkonstruktion bedient sich zwei zentralen Ideen. Die erste Idee besteht darin, von einem PSPACE-vollständigem Orakel $E$ auszugen und dieses zu modifizeren, um die gewünschten Eigenschaften zu erhalten. Durch geschicktes Rückgreifen auf das ursprüngliche Orakel lassen sich dann gewisse nichttriviale Berechnungen effizient umsetzen. Diese Idee geht auf Baker, Gill und Solovay (1975) zurück.

Die zweite Idee betrifft vor allem die Konstruktion. Wir wenden hierbei ein Verfahren von Dose und Glaßer (2019) an, welche sich als ein starkes Framework erwiesen hat, schrittweise Orakel zu konstruieren, die simultan mehrere Eigenschaften erfüllen. Dieses Framework baut maßgeblich auf drei Zutaten auf: erstens, partiell definierten Orakeln, zweitens, ein Begriff von Gültigkeit, und drittens, eine stufenweise nicht-konstruktive Definitionsvorschrift des Orakels. Das werden wir später beim Einsatz in der Konstruktion näher erläutern.

Wir starten mit einem groben Überblick über die Orakelkonstruktion: Startpunkt der Konstruktion ist ein PSPACE-vollständiges Orakel $E$, wobei $E$ so gewählt wird dass gewisse „Ebenen“ leer bleiben. Gemeint ist, dass keine Wörter der Länge $2, 4, 8, \ldots$ in $E$ enthalten sind. Wir werden nun in diese leeren Ebenen geschickt einige wenige Wörter einsetzen und erreichen so das Orakel $O \supseteq E$. Diese Wörter können wir so wählen, dass für jede $\mathrm{UP}^O$-Maschine und jeden $\mathrm{FP}^O$-Transduktor die Reduktion auf eine gewisse Zeugensprache $C \in \mathrm{UP}^O$ ausgeschlossen wird. Das läuft über ein klassisches Diagonalargument, und kann analog für DisjNP umgesetzt werden.

Nun zur Aussage Q. Trivialerweise gilt relativ zu $E$ auch Q. Hätten wir die Möglichkeit, effizient die Differenz $O - E$ auszurechnen, hätten wir auch Q relativ zu $O$. Das ist zwar nicht möglich, aber für totale NPTM $N$ ist es zumindest möglich, eine relevante Portion von $O - E$ zu berechnen, sodass sich auch ein akzeptierender Rechenweg von $N$ mithilfe des PSPACE-vollständigen Orakel $E$ berechnen lässt.

Im folgenden Abschnitt 2.1 spezifizieren wir noch einige spezielle Notationen, die wir zur Orakelkonstruktion benötigen. Aufbauend auf der obigen Skizzze können wir anschließend in Abschnitt 2.2 die konkrete Konstruktionsvorschrift des Orakels formulieren. In Abschnitt 2.3 wird dann abschließend nachgewiesen, dass diese Konstruktionsvorschrift zum einen wohldefiniert ist, und zum anderen dass sich hieraus die gewünschten Eigenschaften wie in Satz 2.1 ergeben.

## 2.1 *Notation zur Orakelkonstruktion*

Zunächst seien $\{M_i\}_{i\in\mathbb{N}}$, $\{N_i\}_{i\in\mathbb{N}}$, $\{F_i\}_{i\in\mathbb{N}}$ sogenannte *Standardaufzählungen* der Orakel-PTMs, Orakel-NPTMs, bzw. Orakel-PTM-Tranduktoren, welche folgende Eigenschaften hat:

1. Die Mengen $\{M_i \mid i \in \mathbb{N}\}$, $\{N_i \mid i \in \mathbb{N}\}$, $\{F_i \mid i \in \mathbb{N}\}$ sind in Polynomialzeit entscheidbar,

heißt es ist effizient entscheidbar, ob der gegebene Maschinencode einer TM der Standardaufzählung entspricht.

2. Für jedes Orakel $D$ terminiert $M_i^D(x)$ nach höchstens $p_i(|x|) \stackrel{\text{df}}{=} |x|^i + i$ Schritten; analog für $N_i$ und $T_i$.
3. Für jede Orakel-PTM $M$ existiert ein $i$ sodass $L(M_i^D) = L(M^D)$, für jede Orakel-NPTM $N$ existiert ein $i$ sodass $L(N_i^D) = L(N^D)$, und für jeden Orakel-PTM-Transduktor $T$ existiert ein $i$ sodass $T^D(x) = T_i^D(x)$.
   Insbesondere kann jeder akzeptierender Rechenweg $\alpha$ Berechnung $N_i(x)$ in einen akzeptierenden Rechenweg $\alpha'$ der Berechnung $N(x)$ effizient übersetzt werden.

Solche Standardaufzählungen existieren. Eine Möglichkeit, diese zu konstruieren ist beispielsweise, jede nichtdeterministische TM mit einem Timer auszustatten, die nach polynomieller Laufzeit die Berechnung abbricht. Konkret: gegeben $i$, sei zunächst $N$ die nichtdeterministische TM mit Codierung $i$. Die TM $N_i$ führt dann auf Eingabe $x$ parallel zur Rechnung $N(x)$ auf jedem Rechenweg einen Timer aus, der nach $> |x|^i + i$ Schritten den Rechenweg ablehnend abbricht. Damit ist die Laufzeit von $N_i$ polynomiell beschränkt auf $p_i$.

Wie bereits angesprochen werden wir ein Konstruktionsverfahren von Dose und Glaßer anwenden. Die erste wesentliche Zutat dieses Framekworks ist der Begriff von „partiell definierten“ Orakeln, bei denen also für gewisse $x$ noch nicht endgültig festgelegt ist, ob $x \in O$ oder $x \notin O$ gelten soll. Diese werden mittels finiten Wörtern $w \in \Sigma^*$ formalisiert: ein finites Wort $w \in \Sigma^*$ können wir im Folgenden auch als die Menge $\{i \mid i < |w|, w[i] = 1\}$ verstehen (aber $|w|$ immer als die Länge von $w$). Die intendierte Interpretation ist, dass gegenüber der *Menge* $w$ die Zugehörigkeit aller Zahlen (bzw. äquivalent Wörtern) $x$ mit $x < |w|$ final speizifiziert ist, nicht dagegen für $x \geq |w|$ (und nur ersatzweise $x \notin w$ gilt).

Diese Inerpretation von finiten Wörtern $w$ als Orakel macht es einfacher, unsere Orakelkonstruktionen präzise und knapp zu beschreiben. Üblicherweise werden wir $w$ so erweitern, dass die Zugehörigkeit des kleinsten $x \in \mathbb{N}$ spezifiziert wird, welche noch nicht final spezifiziert ist. Dieses $x$ ist genau $|w|$ und wir legen die Zugehörigkeit final fest, indem wir an $w$ entweder 0 anhängen (und $x$ ist final nicht im Orakel $w0$) oder 1 anhängen (und $x$ ist final im Orakel $w1$).

Wir können relativ partiell definierten Orakeln auch rechnen. Für $w \in \Sigma^*$ definieren $M^w(x)$ wir entsprechend als $M^{\{i|w(i)=1\}}(x)$ (heißt, Orakel-Anfragen, für die $w$ nicht definiert ist, werden negativ beantwortet). Dies ermöglicht es uns auch, folgenden Begriff zu definieren: Wir sagen, dass NPTM $M^w(x)$ *definit* ist, wenn alle Anfragen auf allen Rechenwegen $< |w|$ sind (oder äquivalent: $w[q]$ ist für alle Anfragen $q$ auf allen Rechenwegen definiert); wir sagen, dass $M^w(x)$ *definitiv akzeptiert* (bzw. *definitiv ablehnt*), wenn $M^w(x)$ definit ist und akzeptiert (bzw. ablehnt). Intuitiv beschreibt der Begriff „definit“ Berechnungen, die sich nicht ändern, wenn das jeweilige partiell definierte Orakel erweitert wird, denn die Anfragen sind zu kurz.

**Beobachtung 2.2.** *(1) Wenn $M^w(x)$ eine definite Berechnung ist und $v \sqsupseteq w$ ist, dann ist $M^v(x)$ definit. Die Berechnung $M^v(x)$ akzeptiert genau dann, wenn $M^w(x)$ akzeptiert.*

*(2) Wenn $w$ für alle Wörter der Länge $p_i(|x|) = |x|^i + i$ definiert ist, dann ist $M_i^w(x)$ definit.*

*(3) Wenn $M^w(x)$ auf einem Rechenweg mit der Menge der Orakel-Anfragen $Q$ akzeptiert, und $w, v$ auf $Q$ übereinstimmen, dann akzeptiert $M^v(x)$ auf dem gleichen Rechenweg und mit der gleichen Menge der Anfragen $Q$.*

Für ein partielles Orakel $w$, einen PTM-Transduktor $F$ und eine (N)PTM $M$ schreiben wir manchmal $M^w(F^w(x))$ als die *eine* Berechnung der (N)PTM $M \circ F$ auf Eingabe $x$ relativ zu $w$. Entsprechend sagen wir dann auch, dass $M^w(F^w(x))$ definit ist (bzw. definitiv akzeptiert, oder definitiv ablehnt) when $M \circ F$ definit auf Eingabe $x$ relativ zu $w$ ist (bzw. definitiv akzeptiert, defitiv ablehnt). Sollte es aus dem Kontext klar hervorgehen, lassen wir üblicherweise auch den Zusatz „partiell“ weg, wenn wir z.B. von einem (partiellen) Orakel $w \in \Sigma^*$ sprechen.

Vor der Konstruktion machen wir nun noch folgende bekannte kombinatorische Aussage:

**Lemma 2.3.** *Sei $G$ ein gerichteter bipartiter Graph mit den Knotenmengen $A$ und $B$. Das heißt, jede Kante in $G$ führt entweder von einem Knoten in $A$ zu einem Knoten in $B$ oder umgekehrt. Sei $\Delta$ eine obere Schranke für den Ausgangsgrad jedes Knotens in $G$.*

*Wenn $|A|, |B| > 2\Delta$ gilt, dann gibt es ein $a \in A$ und $b \in B$, sodass weder $(a, b)$ noch $(b, a)$ eine Kante in $G$ ist.*

*Beweis.* Sei $n = \min\{|A|, |B|\} > 2\Delta$. Entfernen Knoten aus $A$ und $B$, bis beide Knotenmengen jeweils genau $n$ Knoten haben, um einen gerichteten bipartiten Graphen $G'$ mit den Knotenmengen $A'$ und $B'$ zu bilden. Sei $G''$ der zugrunde liegende ungerichtete Graph von $G'$. In $G'$ gibt es $\leq |A'| \cdot \Delta + |B'| \cdot \Delta < n^2$ viele ungerichtete Kanten, aber $n^2$ viele ungerichtete Kanten im vollständigen bipartiten ungerichteten Graphen $K_{n,n}$.

Das bedeutet, dass es $a \in A' \subseteq A$, $b \in B' \subseteq B$ gibt, die in $G''$ nicht adjazent sind; damit sind sowohl $(a, b) \notin E(G')$ als auch $(b, a) \notin E(G')$ im induzierten gerichteten bipartiten Teilgraphen $G'$. Also gilt für den ursprünglichen Graphen $G$ sowohl $(a, b) \notin E(G)$ als auch $(b, a) \notin E(G)$, wie gewünscht. □

## 2.2 *Definition*

Wie zum Teil anfangs des Kapitels skizziert, möchten wir in unseren Orakelonstruktion abzählbar unendlich viele *Ebenen* $n$, das heißt, Wörter gleicher Länge $n$, für eine abzählbar unendliche Familie von Zeugensprachen mit zunehmend großen Lücken injektiv reservieren und zuordnen. Hierfür sei $e(0) \stackrel{\text{df}}{=} 2$, $e(i) \stackrel{\text{df}}{=} 2^{e(i-1)}$. Es gibt eine polynomialzeit-berechenbare, polynomialzeit-invertierbare injektive Funktion $f$, die von $(m, h) \in \mathbb{N} \times \mathbb{N}$ auf $\mathbb{N}$ abbildet. Definiere nun $H_m \stackrel{\text{df}}{=} \{e(f(m, h)) \mid h \in \mathbb{N}\}$ als die Menge der für die Zeugensprache $m$ reservierten Ebenen. Diese Definition stellt nun Folgendes sicher:

**Beobachtung 2.4.** *(1) Die Menge $H_m$ ist abzählbar unendlich, eine Teilmenge der geraden Zahlen, und alle $H_0, H_1, \ldots$ sind paarweise disjunkt.*

*(2) Die Folge $\min H_0, \min H_1, \ldots$ ist nach oben unbegrenzt.*

*(3) Wenn $n \in H_m$, dann gilt für jedes $a \in \mathbb{N}$: $n < a < 2^n \implies a \notin H_0, H_1, \ldots$.*

*(4) Jede Menge $H_m \in \mathrm{P}$ für alle $m \in \mathbb{N}$.*

Wir starten nun die Orakelkonstruktion mit einer PSPACE-vollständiger Menge $C$ welche keine Wörter der Länge $e(0), e(1), e(2), \ldots$ enthält. Damit sind also die oben definierten Ebenen in $C$ leer, wir haben also $\Sigma^n \cap E = \emptyset$ für alle $n \in H_m$.

Wie bereits angesprochen, werden wir in der Konstruktion Wörter der Länge $n \in H_m$ in das Orakel $C$ einsetzen und $O \supseteq C$ erhalten, sodass $O$ die gewünschten Eigenschaften hat. Hierzu definieren wir folgende Zeugensprachen, welche vom Inhalt der Ebenen abhängig sind. Sei hierfür $m \in \mathbb{N}$ und $w \in \Sigma^* \cup \Sigma^\omega$ beliebig:

$$A_m^w \stackrel{\text{df}}{=} \{0^n \mid n \in H_m, \text{existiert } x \in \Sigma^n \text{ mit } x \in w \text{ und } x \text{ endet mit } 0\}$$
$$B_m^w \stackrel{\text{df}}{=} \{0^n \mid n \in H_m, \text{existiert } x \in \Sigma^n \text{ mit } x \in w \text{ und } x \text{ endet mit } 1\}$$
$$C_m^w \stackrel{\text{df}}{=} \{0^n \mid n \in H_m, \text{existiert } x \in \Sigma^n \text{ mit } x \in w\}$$

Sind die Ebenen der Höhe $H_m$ in $w$ auf geeignete Weise gefüllt, lässt sich leicht sehen dass diese entsprechenden Zeugensprachen in $\mathrm{DisjUP}^w$ bzw. $\mathrm{UP}^w$ fallen:

**Behauptung 2.5.** *Sei $w \in \Sigma^* \cup \Sigma^\omega$ ein beliebiges Orakel.*

*(1) Wenn $|w \cap \Sigma^n| \leq 1$ für alle $n \in H_m$, dann $(A_m^w, B_m^w) \in \mathrm{DisjUP}^w$.*

*(2) Wenn $|w \cap \Sigma^n| \leq 1$ für alle $n \in H_m$, dann $C_m^w \in \mathrm{UP}^w$.*

### *Idee und Vorschau der Konstruktion*

1. Erarbeitung (1), bzw. Q: Für alle $j \in \mathbb{N}$ versucht die Konstruktion die Stufen so einzurichten, dass $N_j$ nicht total ist. Falls dies nicht möglich ist, dann wird $N_j$ inhärent total

akzeptieren. Diese Eigenschaft können wir dann algorithmisch ausnutzen, um eine relevante Portion von $O - E$ zu bestimmen, und so einen akzeptierenden Rechenweg für $N_j(x)$ bestimmen.

2. Erarbeitung von (2), bzw. DisjNP: Für alle $a \neq b$ versucht die Konstruktion die Stufen so einzurichten, dass $N_a, N_b$ beide eine Eingabe $x$ akzeptieren, womit $x \in L(N_a) \cap L(N_b)$ und $(L(N_a), L(N_b)) \notin \text{DisjNP}$. Falls dies nicht möglich ist, ist $(N_a, N_b)$ inhärent ein disjunktes NP-Paar. In diesem Fall fixieren wir ein $m$, stellen sicher, dass $(A_m, B_m)$ ein disjunktes UP-Paar ist, und diagonalisieren gegen jeden PTM-Transduktor $F_r$, sodass $F_r$ die Reduktion $(A_m, B_m) \leq_{\text{m}}^{\text{pp}} (L(N_a), L(N_b))$ nicht realisiert. Dies wird folgendermaßen erreicht: (i) Für alle $n \in H_m$ fügen wir höchstens ein Wort der Länge $n$ in $O$ ein (und somit $(A_m, B_m) \in \text{DisjUP}$), und (ii) für jedes $r$ gibt es ein $n \in H_m$ so, dass $0^n \in A_m$, aber $N_a(F_r(0^n))$ ablehnt (oder analog $0^n \in B_m$, aber $N_b(F_r(0^n))$ ablehnt).
3. Erarbeitung von (3), bzw. UP: Für alle $a$ versucht die Konstruktion die Stufen so einzurichten, dass $N_a$ eine Eingabe $x$ auf zwei Rechenwegen akzeptieren, womit $L(N_a) \notin \text{UP}$. Falls dies nicht möglich ist, $L(N_a)$ inhärent eine UP-Sprache. In diesem Fall fixieren wir ein $m$, stellen sicher, dass $C_m$ eine Sprache in UP ist, und diagonalisieren gegen jeden PTM-Transduktor $F_r$, sodass $F_r$ die Reduktion $C_m \leq_{\text{m}}^{\text{pp}} L(N_a)$ nicht realisiert. Dies wird folgendermaßen erreicht: (i) Für alle $n \in H_m$ fügen wir höchstens ein Wort der Länge $n$ in $O$ ein (und somit $C_m \in \text{DisjUP}$), und (ii) für jedes $r$ gibt es ein $n \in H_m$ so, dass $0^n \in C_m$ genau dann wenn $N_a(F_r(0^n))$ ablehnt.

Wir weisen diesen Arbeitsschritten folgende Symbole zu, welche die einzelnen Tasks repräsentieren sollen: $\tau_j^1$, $\tau_{a,b}^2$, $\tau_{a,b,r}^2$, $\tau_a^3$, $\tau_{a,r}^3$. Symbol $\tau_j^1$ repräsentiert den (versuchsweisen) Ausschluss der Totalität von $N_j$. Symbol $\tau_{a,b}^2$ repräsentiert analog den Ausschluss der Disunktheit von $L(N_a), L(N_b)$, Symbol $\tau_{a,b,r}^2$ dann die Diagonalisierung dieses Paares gegen den Transduktor $F_r$. Analog für UP und $\tau_a^3, \tau_{a,r}^3$.

TODO: Idee skizzieren; Verweise darauf dass das Zutat Nr. 2 von Dose/Glaßer ist

Ein Orakel $w \in \Sigma^*$ ist $t$-gültig wenn $t \in \mathcal{T}$ und folgendes gilt:

V1 Wenn $x < |w|$ und $|x| \notin \text{img}(e)$, dann gilt $x \in w \iff x \in C$.
(Bedeutung: Orakel $w$ und $C$ stimmen auf Wörtern mit Länge $\neq e(\cdot)$ überein.)

V2 Für alle $i$ gilt $|w \cap \Sigma^{e(i)}| \leq 2$.
(Bedeutung: Orakel $w$ ist dünn auf den Ebenen der Länge $e(\cdot)$.)

V3 Wenn $t(\tau_j^1) = 0$, dann existiert ein $z$ sodass $N_j^w(z)$ definitiv ablehnt.
($L(N_j) \neq \Sigma^*$ relativ zum finalen Orakel.)

V4 Wenn $t(\tau_{a,b}^2) = 0$, dann existiert ein $z$ sodass $M_a^w(z)$ und $M_b^w(z)$ definitiv akzeptieren.
(Bedeutung: wenn $t(\tau_{a,b}^2) = 0$, dann $L(M_a) \cap L(M_b) \neq \emptyset$ relativ zum finalen Orakel.)

V5 Wenn $0 < t(\tau_{a,b}^2) = m$, dann gilt für alle $n \in H_m$ dass $|\Sigma^n \cap w| \leq 1$.
(Bedeutung: wenn $0 < t(\tau_{a,b}^2) = m$, dann $(A_m, B_m) \in \text{DisjNP}$.)

V6 Wenn $t(\tau_a^3) = 0$, dann existiert ein $z$ sodass $M_a^w(z)$ definitiv auf zwei Rechenwegen akzeptiert.
(Bedeutung: wenn $t(\tau_a^3) = 0$, dann $L(M_a) \notin \text{UP}$ relativ zum finalen Orakel.)

V7 Wenn $0 < t(\tau_a^3) = m$, dann gilt für alle $n \in H_m$ dass $|\Sigma^n \cap w| \leq 1$.
(Bedeutung: wenn $0 < t(\tau_a^3) = m$, dann $C_m \in \text{UP}$.)

### *Induktive Definition des Orakels*

Intuitiv gesprochen verläuft die Konstruktion nun wie folgt: wir starten mit einem partiell definierten Orakel $w$, und wollen dieses nun schrittweise erweitern. In jeder Erweiterung nehmen wir uns einen noch nicht bearbeiteten Task $\tau$, und werden die Erweiterung so wählen, dass $\tau$

relativ zu dieser Erweiterung erfüllt wird. Wir passen dabei auf, dass auch in zukünftigen Erweiterungen $\tau$ erhalten bleibt. Führen wir das nun unendlich oft durch, enden wir „im Limit“ mit einem $\omega$-langen Orakel, welcher alle unsere Tasks $\tau$ abgearbeitet hat.

Diese Idee formalisiern wir nun. Sei $T$ eine abzählbare Aufzählung der oben genannten Tasks sodass $\tau^2_{a,b,r}$ immer nach $\tau^2_{a,b}$ kommt, sowie $\tau^3_{a,r}$ immer nach $\tau^3_a$ kommt. Die Orakelkonstruktion erfolgt nun in abzähnlbar unendlich vielen *Stufen*. In jeder Stufe bearbeiten wir den kleinsten Task $\tau$ in der durch $T$ festgelegten Reihenfolge. Anschließend entfernen wir $\tau$ aus $T$, und entfernen möglicherweise zusätzlich höhere Tasks aus $T$. In der nächsten Stufe fahren wir mit dem nächsten Task fort, die noch nicht aus $T$ entfernt wurde. (In jeder Stufe existiert immer mindestens ein Task, die noch nicht entfernt wurde, da wir in keiner Stufe alle Tasks aus $T$ entfernen werden.)

Eine Stufe $s < \omega$ identifizieren wir hierbei mit einem Orakel $w_s \in \Sigma^*$, einer „Gültigkeits“-Funktion $t_s \in \mathcal{T}$, und einem Task (bzw. mehreren Tasks) welcher in dieser Stufe bearbeitet wurde. Wir werden die einzelen $w_0, w_1, \dots$ und $t_0, t_1, t_2, \dots$ so defineren, dass

$$w_0 \subsetneq w_1 \subsetneq w_2 \subsetneq \cdots,$$

und

$$t_0 \subseteq t_1 \subseteq t_2 \subseteq \cdots,$$

heißt insbesondere das $t_j$ eine Fortsetzung von $t_i$ ist, wenn immer $j \geq i$. Außerdem werden wir sichern, dass jedes $w_s$ ein $t_s$-gültiges Orakel ist. Es ist klar, dass jeder Task $\tau \in T$ letzlich in irgendeiner Stufe $s$ bearbeitet wird.

Nun zur Definition von $w_s, t_s$: wir werden die einzelnen Stufen induktiv definieren. Als Basisklausel setzen wir $w_0 = \varepsilon$ und $t_0 = \emptyset$. Für unsere induktive Klausel sei $s > 0$. Die Definition für $w_s, t_s$ ergibt sich nun aus der bereits definierten Funktion $t_{s-1} \in \mathcal{T}$, und dem bereits definierten $t_{s-1}$-gültigen Orakel $w_{s-1}$, sowie dem zu bearbeitenden kleinsten verbleibenden Task $\tau$ in $T$. Zur Erinnerung: dieser wird unmittelbar nach der Bearbeitung aus $T$ entfernt. In der Bearbeitung wird das Orakel strikt verlängert. Es gibt nun fünf Fälle, je nach dem welche Form der bearbeitete Task $\tau$ hat.

**Task $\tau^1_j$:** Setze $t' \stackrel{\text{df}}{=} t_{s-1} \cup \{\tau^1_j \mapsto 0\}$. Existiert ein $t'$-gültiges Orakel $v \supsetneq w_{s-1}$, dann setze $t_s \stackrel{\text{df}}{=} t'$ und $w_s \stackrel{\text{df}}{=} v$.

Ansonsten setze $t_s \stackrel{\text{df}}{=} t_{s-1}$ und setze $w_s \stackrel{\text{df}}{=} w_{s-1}y$ für geeignetes $y \in \{0,1\}$ sodass $w_s$ auch $t_s$-gültig ist. Das ist möglich nach Behauptung 2.6.

(Bedeutung: wenn das Orakel $w_s$ so eingerichtet werden kann, dass $N_j$ nicht mehr total arbeitet, dann erweitere genau so, vgl. V2.)

**Task $\tau^2_{a,b}$:** Setze $t' \stackrel{\text{df}}{=} t_{s-1} \cup \{\tau^2_{a,b} \mapsto 0\}$. Existiert ein $t'$-gültiges Orakel $v \supsetneq w_{s-1}$, dann setze $t_s \stackrel{\text{df}}{=} t'$ und $w_s \stackrel{\text{df}}{=} v$. Entferne außerdem alle Tasks der Form $\tau^2_{a,b,r}$ von $T$.

Ansonsten wähle ein hinreichend großes $m \notin \operatorname{img}(t_s)$ sodass $w_s$ kein Wort der Länge $\min H_m$ definiert. Setze $t_s \stackrel{\text{df}}{=} t_{s-1} \cup \{\tau^2_{a,b} \mapsto m\}$; damit ist $w_{s-1}$ auch $t_s$-gültig. Setze $w_s \stackrel{\text{df}}{=} w_{s-1}y$ für geeignetes $y \in \{0,1\}$ sodass $w_s$ auch $t_s$-gültig ist. Das ist möglich nach Behauptung 2.6.

(Bedeutung: wenn das Orakel $w_s$ so eingerichtet werden kann, dass $N_a, N_b$ nicht mehr disjunkt akzeptieren, dann erweitere genau so, vgl. V4. Ansonsten, falls das nicht möglich ist, wähle ein geeignetes frisches $m$ und setze ab dieser Stufe voraus, dass $(A_m, B_m) \in \text{DisjUP}$.)

**Task $\tau^2_{a,b,r}$:** Wir wissen dass $t_{s-1}(\tau^2_{a,b}) = m > 0$. Setze $t_s = t_{s-1}$ und wähle ein $t_s$-gültiges Orakel $w_s \supsetneq w_{s-1}$ sodass bezüglich einem $n \in \mathbb{N}$ eine der folgenden Aussagen gilt:

- $0^n \in A^v_m$ für alle $v \supseteq w_s$ und $M_a(F_r(0^n))$ lehnt relativ zu $w_s$ definitiv ab.
- $0^n \in B^v_m$ für alle $v \supseteq w_s$ und $M_b(F_r(0^n))$ lehnt relativ zu $w_s$ definitiv ab.

Das ist möglich nach Behauptung 2.7.

(Bedeutung: erweitere zu $w_s$, sodass $F_r$ nicht die Reduktion $(A_m, B_m) \leq_{\mathrm{m}}^{\mathrm{pp}} (L(N_a), L(N_b))$ realisiert.)

**Task $\tau_a^3$:** Setze $t' \stackrel{\mathrm{df}}{=} t_{s-1} \cup \{\tau_{a,b}^3 \mapsto 0\}$. Existiert ein $t'$-gültiges Orakel $v \sqsupsetneq w_{s-1}$, dann setze $t_s \stackrel{\mathrm{df}}{=} t'$ und $w_s \stackrel{\mathrm{df}}{=} v$. Entferne außerdem alle Tasks der Form $\tau_{a,b,r}^3$ von $T$.

Ansonsten wähle ein hinreichend großes $m \notin \mathrm{img}(t_s)$ sodass $w_s$ kein Wort der Länge $\min H_m$ definiert. Setze $t_s \stackrel{\mathrm{df}}{=} t_{s-1} \cup \{\tau_{a,b}^3 \mapsto m\}$; damit ist $w_{s-1}$ auch $t_s$-gültig. Setze $w_s \stackrel{\mathrm{df}}{=} w_{s-1}y$ für geeignetes $y \in \{0,1\}$ sodass $w_s$ auch $t_s$-gültig ist. Das ist möglich nach Behauptung 2.6.

(Bedeutung: wenn das Orakel $w_s$ so eingerichtet werden kann, dass $N_a$ auf mehr als einem Rechenweg akzeptiert, dann erweitere genau so, vgl. V6. Ansonsten, falls das nicht möglich ist, wähle ein geeignetes frisches $m$ und setze ab dieser Stufe voraus, dass $(C_m) \in \mathrm{UP}$.)

**Task $\tau_{a,r}^3$:** Wir wissen dass $t_{s-1}(\tau_a^3) = m > 0$. Setze $t_s \stackrel{\mathrm{df}}{=} t_{s-1}$ und wähle ein $t_s$-gültiges Orakel $w_s \sqsupsetneq w_{s-1}$ sodass bezüglich einem $n \in \mathbb{N}$ eine der folgenden Aussagen gilt:

- $0^n \in C_m^v$ für alle $v \sqsupseteq w_s$ und $M_a(F_r(0^n))$ lehnt relativ zu $w_s$ definitiv ab.
- $0^n \notin C_m^v$ für alle $v \sqsupseteq w_s$ und $M_a(F_r(0^n))$ akzeptiert relativ zu $w_s$ definitiv.

Das ist möglich nach Behauptung 2.10.

(Bedeutung: erweitere zu $w_s$, sodass $F_r$ nicht die Reduktion $(C_m) \leq_{\mathrm{m}}^{\mathrm{p}} (L(N_a))$ realisiert.)

Beobachte, dass $t_s$ immer als Element von $\mathcal{T}$ definiert ist. Beachte auch den „Existenzquantor“ in Task $\tau_j^1$ (bzw. ähnlich bei $\tau_{a,b}^2$, $\tau_a^3$), welcher in der Konstruktion „testet“, ob eine gültige Erweiterung des Orakels existiert, welche die Totalität der NPTM $N_j$ definitiv ausschließt. Hierzu zwei Bemerkungen: Erstens handelt es sich hierbei insbesondere um ein nicht-konstruktives Argument. Falls eine solche Erweiterung existieren sollte, dann können wir diese auch auswählen (z.B. indem die lexikographisch kleinste gewält wird), ohne dass diese in expliziter Weise angegeben wird. Zweitens, falls eine solche gültige Erweiterung nicht existiert, dann ist die NPTM $N_j$ sogar „besonders total“, in dem Sinn dass $N_j$ sogar unter *jeder* gülitgen Erweiterung total ist. Diese Konstruktionstaktik ist die dritte Zutat des Verfahrens von Dose und Glaßer.

Mit den oben genannten Tasks ist die die Definition der Stufe $s$ abgeschlossen, und somit die beiden Folgen $\{w_s\}_{s<\omega}$ $\{t_s\}_{s<\omega}$. Später werden wir das finale Orakel $O$ als $\bigcup_{s\in\mathbb{N}} w_s = \bigcup_{s\in\mathbb{N}}\{i \mid w_s[i] = 1, i < |w_s|\}$ definieren, heißt die Vereinigung über alle partiellen Orakel, oder äquivalent, der Grenzwert $\lim_{n\to\omega} w_s = O \in \Sigma^\omega$ der Folge von finiten Wörtern $w_0 \sqsubsetneq w_1 \sqsubsetneq \cdots$.

Wir müssen nun zwei Aussagen zeigen: erstens, dass diese Konstruktion tatsächlich möglich ist, indem wir die in der Definition angekündigten Lemmata angeben und beweisen. Zweitens müssen wir zeigen, dass die Konstruktion das leistet was wir uns wünschen, also dass $O$ die behaupteten Eigenschaften des Satzes 2.1 erfüllen. Beides werden wir nun im folgenden Abschnitt beweisen.

## 2.3 *Korrektheit*

### *Existenz*

Wir zeigen im Folgenden zunächst, dass die oben definierte induktive Definition tatsächlich wohldefiniert ist, in dem Sinne dass jeder Task umgesetzt werden kann und die induktive Definition nicht „abbricht“.

Zunächst beweisen wir, dass sich ein $t$-gültiges Orakel $w$ immer um ein Bit verlängern lassen kann, ohne Gültigkeit zu verletzen.

**Lemma 2.6.** *Sei $t \in \mathcal{T}$ und $w$ ein $t$-gültiges Orakel, und sei $z = |w|$. (Denke $z$ als das nächste Wort,*

*für welche wir die Zuordnung zum Orakel festlegen wollen, d.h. wahlweise $z \notin w0$ oder $z \in w1$.) Dann existiert ein $b \in \{0,1\}$ sodass $wb$ auch $t$-gültig ist. Insbesondere gilt*

*(1) Falls $|z| \notin \mathrm{img}(e)$, dann ist $w0$ $t$-gültig wenn $z \in C$, und $w1$ $t$-gültig wenn $z \notin C$.*

*(2) Ansonsten, falls ein $i$ existiert mit $|z| = e(i)$, dann ist $w0$ $t$-gültig.*

*Beweis.* Sei $z = |w|$. Beachte, dass wir mit $b$ kontrollieren, ob $z \in wb$ gilt. Angenommen, $wb$ ist nicht $t$-gültig, dann muss eine der Bedingungen V1–V7 verletzt sein.

Angenommen V3 ist verletzt, weil $N_j^{wb}(x)$ nicht definit ablehnt und gleichzeitig $t(\tau_j^1) = 0$. Da nach Voraussetzung $w$ aber $t$-gültig ist, wird $N_j^w(x)$ definitiv ablehnen. Nach Beobachtung 2.2(3) wissen wir aber, dass dann auch $N_j^{wb}(x)$ definitiv ablehnen wird. Widerspruch. Also kann V3 nicht verletzt sein. Mit analoger Argumentation sehen wir auch, dass V4 und V6 nicht verletzt sein können.

Angenommen V1 ist verletzt, weil für $x < |wb|, |x| \notin \mathrm{img}(e)$ die Äquivalenz von V1 nicht gilt, heißt $x \in wb \nleftrightarrow x \in C$. Dann kann $x$ nicht $< |w|$ sein, denn V1 gilt hier nach $t$-Gültigkeit von $w$. Also muss $x = z$. Damit auch $|z| \notin \mathrm{img}(e)$ und wir haben für Fall (2) schon einen Widerspruch zur Voraussetzung. Wir sind also in Fall (1) und können voraussetzen, dass $b = 1$ genau dann wenn $z \in C$. Dann gilt aber genau $x \in wb \leftrightarrow x \in C$ und wir haben einen Widerspruch.

Es kann also nur V2, V5, oder V7 verletzt sein. Angenommen V5 ist verletzt, weil für $n \in H_m$ gilt $|wb \cap \Sigma^n| > 1$. Nach Definition wissen wir, dass $wb$ und $w$ auf allen Wörtern $\neq z$ übereinstimmen. Wir unterscheiden nun zwei Fälle: $z \notin \Sigma^n$ und $z \in \Sigma^n$. Für den ersten Fall sei angenommen $z \notin \Sigma^n$. Dann stimmen $wb$ und $w$ sogar auf den Wörtern $\Sigma^n$ überein. Das bedeutet dass auch $|w \cap \Sigma^n| > 1$. Das widerspricht der $t$-Gültigkeit von $w$.

Für den zweiten Fall nehmen wir nun $z \in \Sigma^n$ an. Damit müssen wir auch nur Fall (2) prüfen, da Voraussetzung von Fall (1) nicht erfüllt sind. Hier gilt nun $b = 0$ und

$$|wb \cap \Sigma^n| = |w0 \cap \Sigma^n| = |w \cap \Sigma^n| > 1,$$

haben also wieder einen Widerspruch zur $t$-Gültigkeit von $w$.

Die Bedingung V5 kann also nicht verletzt sein. Auf analoge Weise wie eben bei V5 lässt sich auch zeigen, dass V2 und V7 nicht verletzt sein können. Insgesamt kann also keine Bedingung V1–V7 verletzt sein; $wb$ ist $t$-gültig wie gewünscht. □

Damit haben wir die ersten beiden Tasks aus der Definition schon gesichert. Nun zeigen wir, dass die Bearbeitung von $\tau^2_{a,b,r}$ möglich ist.

**Lemma 2.7.** *Die Bearbeitung eines Tasks $\tau^2_{a,b,r}$ ist möglich: gilt $t_s = t_{s-1}, t_s(\tau^2_{a,b}) = m > 0$, dann lässt sich $w_s$ so zu $t_s$-gültigem $w \sqsupseteq w_s$ erweitern, sodass eine der folgenden Aussagen gilt:*

*(1) $0^n \in A^v_m$ für alle $v \sqsupseteq w$ und $M_a(F_r(0^n))$ lehnt relativ zu $w$ definitiv ab.*

*(2) $0^n \in B^v_m$ für alle $v \sqsupseteq w$ und $M_b(F_r(0^n))$ lehnt relativ zu $w$ definitiv ab.*

*Skizze.* Widerspruchsbeweis. Erweitere $w_{s-1}$ so weit zu $u$, dass genau alle Wörter der Länge $< n = e(i) \in H_m$ definiert sind, wobei das $i$ hinreichend groß gewählt wird. Sei für jedes $X \subseteq \Sigma^n$ das Orakel $u(X) \sqsupsetneq w_{s-1}$ jenes Orakel was entsteht, wenn die Ebene $e(i)$ mit genau den Wörtern aus $X$ gefüllt wird, heißt $u(X)$ und $X$ stimmen auf $\Sigma^n$ überein. Beob. dass $u(X), |X| \leq 1$ auch $t_s$-gültig ist.

Nach Annahme gilt

- für $\alpha \in \Sigma^{n-1}0$ gilt $0^n \in A_m^{u(\{\alpha\})}$ und daher akzeptiert $M_a(F_r(0^n))$ relativ zu $u(\{\alpha\})$.
- für $\beta \in \Sigma^{n-1}1$ gilt $0^n \in B_m^{u(\{\alpha\})}$ und daher akzeptiert $M_b(F_r(0^n))$ relativ zu $u(\{\beta\})$.

Kombinatorische Standardmethoden zeigen dann, dass relativ zu $u(\{\alpha,\beta\})$ mit geeignetem $\alpha \in \Sigma^{n-1}0$, $\beta \in \Sigma^{n-1}1$ sowohl $M_a(F_r(0^n))$ also auch $M_b(F_r(0^n))$ relativ zu $u(\{\alpha,\beta\})$ akzeptieren. Damit wäre aber auch $u(\{\alpha,\beta\})$ ein geeignetes Orakel in der Bearbeitung von Task $\tau^2_{a,b}$ und wir hätten $t_s(\tau^2_{a,b}) = 0$. □

*Beweis.* Wir fixieren die Werte von $a$, $b$ und $r$ im gesamten Beweis dieses Satzes.

Sei $\hat{s} < s$ die Stufe, die $\tau^2_{a,b}$ behandelt hat. Eine solche Stufe existiert, da andernfalls $t_s(\tau^2_{a,b})$ undefiniert wäre. Wir haben $m = t_{\hat{s}}(\tau^2_{a,b}) = t_s tau^2_{a,b})$; fixiere auch $m$ für den Rest des Beweises.

Wir nehmen an, dass für alle $t_s$-gültigen $w \supsetneq w_{s-1}$ weder (1) noch (2) zutrifft. Daraus werden wir einen Widerspruch ableiten, indem wir ein geeignetes Orakel $u' \supsetneq w_{\hat{s}-1}$ konstruieren, das bezüglich $t' \stackrel{\text{df}}{=} t_{\hat{s}-1} \cup \{\tau^2_{a,b} \mapsto 0\}$ gültig ist. (Gemeint ist: relativ zu $u'$ wird $M_a$ und $M_b$ eine Eingabe definitiv akzeptieren.) Dann folgt nach Definition, dass $u'$ eine mögliche $t'$-gültige Erweiterung von $w_{\hat{s}-1}$ in Stufe $\hat{s}$ ist, daher hätte die Bearbeitung von $\tau^2_{a,b}$ eben $t_{\hat{s}} = t'$ gesetzt, damit auch $t_s tau^2_{a,b}) = t'(\tau^2_{a,b}) = 0$, was der Voraussetzung widerspricht.

Sei

$$\gamma(n) \stackrel{\text{df}}{=} \max(p_a(p_r(n)) + p_r(n), p_b(p_r(n)) + p_r(n))$$

das Polynom, das die Laufzeit von $M_a \circ F_r, M_b \circ F_r$ bezüglich der Eingabelänge $n$ relativ zu einem beliebigen Orakel beschränkt. Das bedeutet immer dann, wenn ein partielles Orakel $u'$ für alle Wörter der Länge $\leq \gamma(n)$ definiert ist, auch $M_a^{u'}(F_r^{u'}(x)), M_b^{u'}(F_r^{u'}(x))$ für alle Eingaben $x \in \Sigma^n$ definit sind. Sei $n \in \mathbb{N}$ eine geeignete Zahl sodass $n \in H_m$, und $w_{s-1}$ keine Wörter der Länge $\geq n$ definiert, und

$$2^n > \gamma(n), \quad 2^{n-1} > 2\gamma(n). \tag{2.1}$$

Die erste Ungleichung von (2.1) stellt sicher, dass kein Level $a$, $n < a \leq \gamma(n)$ für irgendeine Zeugensprache reserviert ist, das heißt, $a \notin H_0, H_1, \ldots$ (vgl. Beobachtung 2.4(3)). Die zweite Ungleichung stellt sicher, dass es genügend Wörter der Länge $n$ gibt, damit bestimmte kombinatorische Argumente funktionieren. Die Ungleichung stellt sicher, dass es genügend Wörter der Länge $n$ gibt, damit bestimmte kombinatorische Argumente funktionieren.

Für den restlichen Beweis fixieren wir zusätzlich $n$. Beachte, dass $\ell(Q) \leq \gamma(n)$ für $Q$ die Menge der Orakelqueries ist, die jeweils von der Berechnung $M_a(F_r(0^n))$ oder der Berechnung $M_b(F_r(0^n))$ gestellt werden. Wir definieren nun $u \supseteq w_{s-1}$ als ein $t_s$-gültiges partielles Orakel, das genau für alle Wörter bis zur Länge $< n$ definiert ist. Ein solches Orakel existiert nach Lemma 2.6, indem man $w_{s-1}$ bitweise erweitert, so dass es $t_s$-gültig (bzw. identisch $t_{s-1}$-gültig) bleibt.

Für unseren Beweis betrachten wir nicht alle $t_s$-gültigen $w$, sondern vielmehr eine ausreichende Teilmenge davon. Für $X \subseteq \Sigma^n, |X| \leq 2$ definieren wir ein partielles Orakel $u(X) \supsetneq u$ als

$$u(X)[x] \stackrel{\text{df}}{=} \begin{cases} u[x] & \text{falls } |x| \leq n \\ X[x] & \text{falls } |x| = n \\ C[X] & \text{falls } n < |x| \leq \gamma(n) \\ \bot & \text{sonst,} \end{cases}$$

das für alle Wörter bis zur Länge $\leq \gamma(n)$ definiert ist, und so dass $u(X) \cap \Sigma^n = X$, das heißt, $u(X)$ und $X$ stimmen in $\Sigma^n$ überein.

Im Wesentlichen entsteht also $u(X)$ aus $u$, indem die Ebene $n$ mit $X$ gefüllt wird, und dann in den höheren Ebenen mit dem PSPACE-Orakel $C$ weitergemacht wird. Es ist leicht zu sehen, dass für $|X| \leq 1$ das Orakel $u(X)$ sogar $t_s$-gültig ist, indem iterativ $u$ erweitert wird.

**Behauptung 2.8.** *Sei $|X| \leq 1$. Dann ist $u(X)$ ein $t_s$-gültiges Orakel.*

*Beweis.* Angenommen, es ist kein $t_s$-valies Orakel. Dann ist eine der Bedingungen V1–V7 verletzt. Wir zeigen, dass diese Annahme zu einem Widerspruch führt. Klar ist, dass V3, V4, V6 nicht verletzt sein können, denn jede definite Berechnung relativ zu $u$ ist auch eine definite Berechnung relativ zu $u(X)$ nach Beobachtung 2.2(1).

Angeommen, V1 ist verletzt. Dann muss ein $x$ mit $|x| \leq \gamma(n), |x| \neq e(\cdot)$ existieren, sodass $x \in u(X) \nleftrightarrow x \in C$. Klar ist, dass $|x| \geq n$ sein muss, da ansonsten schon $u$ nicht $t_s$-gültig wäre; das wäre ein Widerspruch zur Konstruktion von $u$. Also $n < |x| \leq \gamma(n)$. Dann wissen wir aber nach Definition von $u(X)$ dass $x \in u(X) \leftrightarrow x \in C$; Widerspruch zur Wahl von $x$.

Angenommen, V5 ist verletzt. Dann existiert ein $\tau'$ mit $t_s(\tau') = m' > 0$ und $n' \in H_{m'}$ und $|\Sigma^{n'} \cap u(X)| > 1$. Wieder klar ist, dass $n \leq n' \leq \gamma(n) < 2^n$ sein muss, ansonsten wäre schon $u$ nicht mehr $t_s$-gültig. Dann aber muss auch $n = n'$, denn ansonsten wäre $n' \notin H_{m'}$, nach Beobachtung 2.4. Jetzt haben wir aber $|\Sigma^{n'} \cap u(X)| = |\Sigma^n \cap u(X)| = |X| \leq 1$; das ist ein Widerspruch zur Annahme $|\Sigma^{n'} \cap u(X)| > 1$. Also kann V5 nicht verletzt sein.

Auf analoge Weise ist ersichtlich, dass auch V2 und V7 nicht verletzt sein können. Damit ist keine Bedingung verletzt, $u(X)$ muss also $t_s$-gültig sein. □

Wir haben angenommen, dass für $t_s$-gültige Orakel nicht (1) oder (2) gilt. Angewendet auf $u(X), |X| \leq 1$ bedeutet das

- Für $\alpha \in \Sigma^{n-1}0$ gilt $0^n \in A_m^{u(\{\alpha\})}$ und daher akzeptiert $M_a(F_r(0^n))$ definitiv relativ zu $u(\{\alpha\})$ auf einem Rechenweg mit Orakelmenge $Q_\alpha$.
- Für $\beta \in \Sigma^{n-1}1$ gilt $0^n \in B_m^{u(\{\alpha\})}$ und daher akzeptiert $M_b(F_r(0^n))$ definitiv relativ zu $u(\{\beta\})$ auf einem Rechenweg mit Orakelmenge $Q_\beta$.

Wir wollen nun ein Orakel $u'$ konstruieren, sodass sowohl $M_a$ als auch $M_b$ akzeptieren. Hierfür wollen wir die beiden jeweiligen akzeptierenden Rechenwege fixieren. Wir stellen das sicher, indem wir $u'$ so wählen, dass $u'$ mit $u(\{\alpha\})$ auf $Q_\alpha$ übereinstimmt, dann wird auch $M_a(F_r(0^n))$ relativ zu $u'$ akzeptieren. Symmetrisch stellen wir das auch für $M_b$ bzw. $\beta$ sicher, sodass auch $M_a(F_r(0^n))$ relativ zu $u'$ akzeptieren wird.

Hierzu müssen wir $\alpha \in \Sigma^{n-1}0$ und $\beta \in \Sigma^{n-1}1$ finden, die sich nicht gegenseitig „stören“. Ein Wort $\alpha \in \Sigma^{n-1}0$ stört $\beta \in \Sigma^{n-1}1$ falls $\alpha \in Q_\beta$, symmetrisch stört ein Wort $\beta \in \Sigma^{n-1}0$ ein Wort $\alpha \in \Sigma^{n-1}1$ falls $\beta \in Q_\alpha$.

Es existieren $\alpha \in \Sigma^{n-1}0$ und $\beta \in \Sigma^{n-1}1$ die sich nicht gegenseitig stören. Wir zeigen das über einen bipartiten „Störgraph“ $G$. Setze

$$A = \Sigma^{n-1}0, B = \Sigma^{n-1}1$$

als die zwei Knotenmengen von $G$. Setze nun

$$E = \{(\alpha, \beta) \mid \alpha \in \Sigma^{n-1}0, \beta \in \Sigma^{n-1}1, \alpha \in Q_\beta\} \cup \{(\beta, \alpha) \mid \alpha \in \Sigma^{n-1}0, \beta \in \Sigma^{n-1}1, \beta \in Q_\alpha\}$$

als Kantenmenge. Beachte, dass der Ausgangsgrad $\Delta$ von $G$ höchstens $\gamma(n)$ sein kann, denn ein Rechenweg auf $M_a(F_r(0^n))$ (bzw. $M_b(\cdots)$) ist auf $\leq \gamma(n)$ viele Schritte beschränkt.

Nach (2.1) wissen wir nun, dass $|A|, |B| > 2\Delta$. Mittels Lemma 2.3 exisieren also $\alpha \in A = \Sigma^{n-1}0$, $\beta \in B = \Sigma^{n-1}1$ sodass weder $(a, b) \in E$ noch $(b, a) \in E$. In anderen Worten, es gilt $\alpha \notin Q_\beta$ und $\beta \notin Q_\alpha$.

Betrachte nun $u' \stackrel{\text{df}}{=} u(\{\alpha, \beta\})$. Wir zeigen nun zwei Dinge: erstens, dass $M_a(F_r(0^n))$ und $M_b(F_r(0^n))$ definitiv relativ zu $u(\{\alpha, \beta\})$ akzeptieren. Zweitens anschließend, dass $u(\{\alpha, \beta\})$ auch $t'$-gültig ist.

Für die erste Aussage beobachten wir, dass $u(\{\alpha\})$ und $u(\{\alpha, \beta\})$ auf $Q_\alpha$ übereinstimmen. Angenommen sie stimmen nicht überein, dann müssen sie nach Konstruktion auf $\beta$ nicht übereinstimmen. Dann wäre aber $\beta \in Q_\alpha$, was ein Widerspruch zur Wahl von $\beta$ ist. Symmetrisch sehen wir, dass $u(\{\beta\})$ und $u(\{\alpha, \beta\})$ auf $Q_\beta$ ist. Also akzeptieren $M_a(F_r(0^n))$ und $M_b(F_r(0^n))$ definitiv relativ zu $u(\{\alpha, \beta\})$.

Nun zur zweiten Aussage. Zunächst zeigen wir $t_{\hat{s}-1}$-Gültigkeit.

**Behauptung 2.9.** *Das Orakel $u' = u(\{\alpha, \beta\})$ ist $t_{\hat{s}-1}$-gültig.*

*Beweis.* Angenommen, es ist kein $t_{\hat{s}-1}$-valies Orakel. Dann ist eine der Bedingungen V1–V7 verletzt. Wir zeigen, dass diese Annahme zu einem Widerspruch führt. Wieder klar ist, dass V3, V4, V6 nicht verletzt sein können, denn jede definite Berechnung relativ zu $t_{\hat{s}-1}$-gültigem $u$ ist auch eine definite Berechnung relativ zu $u'$ nach Beobachtung 2.2(1). Auch V1 kann nicht verletzt sein; das folgt aus dem gleichen Argument wie im Beweis von Behauptung 2.8.

Angenommen, V5 ist verletzt. Dann existiert ein $\tau'$ mit $t_{\hat{s}-1}(\tau') = m' > 0$ und $n' \in H_{m'}$ und $|\Sigma^{n'} \cap u(X)| > 1$. Wieder folgt $n = n'$. Insbesondere folgt daraus auch $m = m'$, denn $n$ ist nur in $H_m$ enthalten. Gleichzeitig haben wir $\tau' \neq \tau^2_{a,b}$, da $\tau^2_{a,b} \notin \text{dom}(t_{\hat{s}-1})$. Damit gilt aber $t_s(\tau') = t_{\hat{s}-1}(\tau') = m' = m = t_s(\tau^2_{a,b})$; Widerspruch zur Injektivität von $t_s \in \mathcal{T}$ auf dem

Support. Also kann V5 nicht verletzt sein. Auf analoge Weise ist ersichtlich, dass auch V7 nicht verletzt sein kann.

Angenommen, V2 ist verletzt. Dann existiert ein $i$ mit $|u' \cap \Sigma^{n'}| > 2$ für $n' = e(i)$. Wieder folgt $n = n'$. Jetzt haben wir aber $|\Sigma^{n'} \cap u'| = |\Sigma^n \cap u(\{\alpha, \beta\})| = |\{\alpha, \beta\}| = 2$; das ist ein Widerspruch zur Annahme $|\Sigma^{n'} \cap u'| > 2$. Also kann V2 nicht verletzt sein.

Damit ist keine Bedingung verletzt, $u'$ muss also $t_{\hat{s}-1}$-gültig sein. □

Wir erinnern uns daran dass $t' = t_{\hat{s}-1} \cup \{\tau^2_{a,b} \mapsto 0\}$. Nun ist es leicht zu sehen, dass $u' \stackrel{\text{df}}{=} u(\{\alpha, \beta\})$ auch $t'$-gültig ist. Das Orakel $u'$ ist nach voriger Behauptung $t_{\hat{s}-1}$-gültig, und bei der Erweiterung von $t_{\hat{s}-1}$ zu $t'$ kommt nur $\tau^2_{a,b} \mapsto 0$ hinzu. Das bedeutet, dass wir nur noch die Bedingung V4 bezüglich $a, b$ verifizieren müssen. Sei nun $y = F_r(0^n)$ relativ zu $u'$. Nach voriger Aussage oben wissen wir aber, dass $M_a(y)$ und $M_b(y)$ relativ zu $u'$ beide definitiv akzeptieren, wie von V4 verlangt.

Da nun also $u' \supsetneq u \supsetneq w_{\hat{s}-1}$ auch $t'$-gültig ist, sind wir fertig und erreichen einen Widerspruch, wie anfangs argumentiert: während der Bearbeitung von Task $\tau^2_{a,b}$ in Stufe $\hat{s}$ war das Orakel $u'$ eine mögliche $t'$-gültig Erweiterung von $w_{\hat{s}-1}$, denn es ist $t'$-gültig und $u' \supsetneq w_{\hat{s}-1}$. Also wäre nach Definition des Tasks $\tau^2_{a,b}$ dann $t_{\hat{s}} = t'$ gesetzt worden. Damit wäre dann auch $t_s(\tau^2_{a,b}) = t'(\tau^2_{a,b}) = 0$, was der Voraussetzung dieses Lemma 2.7 widerspricht. □

Ohne größeren Veränderungen lässt sich auf fast gleiche Weise auch zeigen, dass die Tasks $\tau^3_{a,r}$ bearbeitet werden können.

**Lemma 2.10.** *Die Bearbeitung eines Tasks $\tau^3_{a,r}$ ist möglich: gilt $t_s = t_{s-1}, t_s(\tau^3_a) = m > 0$, dann lässt sich $w_s$ so zu $t_s$-gültigem $w \supsetneq w_{s-1}$ erweitern, dass eine der folgenden Fälle eintritt:*

- *$0^n \in C^v_m$ für alle $v \sqsupseteq w$ und $M_a(F_r(0^n))$ lehnt relativ zu $w$ definitiv ab.*
- *$0^n \notin C^v_m$ für alle $v \sqsupseteq w$ und $M_a(F_r(0^n))$ akzeptiert relativ zu $w$ definitiv.*

*Beweis.* Wir verfahren wie im Beweis von Lemma 2.7. Um wieder einen Widerspruch abzuleiten, nehmen wir an, dass für alle $t_s$-gültigen $w \supsetneq w_{s-1}$ weder (1) noch (2) zutrifft. Definiere wieder identisch $u$ und $u(X)$. Wieder gilt nach Behauptung 2.8 dass $u(X)$ immer $t_s$-gültig ist wenn $|X| \leq 1$. Wir haben also:

- Die Berechnung $M_a(F_r(0^n))$ lehnt relativ zu $u(\emptyset)$ definitiv ab.
- Für $\xi \in \Sigma^n$ gilt $0^n \in C_m^{u(\{\xi\})}$ und daher akzeptiert $M_a(F_r(0^n))$ definitiv relativ zu $u(\{\xi\})$ auf einem Rechenweg mit Orakelmenge $Q_\xi$.

Beachte, dass $\xi \in Q_\xi$ ist, andernfalls stimmen $u(\emptyset)$ und $u(\{\xi\})$ auf $Q_\xi$ überein, damit folgt mit Beobachtung 2.2(3), dass $M_a(F_r(0^n))$ relativ zu $u(\emptyset)$ akzeptiert, was der Annahme widerspricht.

Wir fahren nun fort wie in Lemma 2.7. Seien $\alpha \in \Sigma^n$, $\beta \in \Sigma^n$ zwei unterschiedliche Wörter, die sich nicht gegenseitig stören. Das heißt, $\alpha \notin Q_\beta$, $\beta \notin Q_\alpha$. Diese zwei Wörter existieren nach dem gleichen kombinatorischen Argument wie bei Lemma 2.7.

Setze nun $u(\{\alpha, \beta\})$. Wir zeigen nun, dass $M_a(F^r(0^n))$ auf zwei unterschiedlichen Rechenwegen akzeptieren. Wieder haben wir, dass $u(\{\alpha\})$ und $u(\{\alpha, \beta\})$ auf $Q_\alpha$ übereinstimmen, und symmetrisch $u(\{\beta\})$ und $u(\{\alpha, \beta\})$ auf $Q_\beta$ übereinstimmen. Mittels Beobachtung 2.2(3) sehen wir also, dass es zwei Rechenwege von $M_a(F_r(0^n))$ relativ zu $u(\{\alpha, \beta\})$ gibt, welche definitiv akzeptieren: einer mit Orakelfragen $Q_\alpha$, und einer mit $Q_\beta$. Diese zwei Rechenwege sind tatsächlich unterschiedlich: einerseits gilt aus obiger Feststellung dass $\alpha \in Q_\alpha$, aber nach Wahl von $\beta$ ist $\alpha \notin Q_\beta$. Auf einem Rechenweg wird also $\alpha$ erfragt, auf dem anderen nicht; also sind die zwei Rechenwege unterschiedlich.

Wie im Beweis von Lemma 2.7 können wir jetzt $t' \stackrel{\text{df}}{=} t_{\hat{s}-1} \cup \{\tau^3_a \mapsto 0\}$ setzen. Wieder gilt nach Behauptung 2.9 dass $u' \stackrel{\text{df}}{=} u(\{\alpha, \beta\})$ auch $t_{\hat{s}-1}$-gültig ist. Dann lässt sich auch leicht sehen, dass $u'$ auch $t'$-gültig ist. Es kommt V6 bezüglich $a$ hinzu, aber wir haben ja eben gesehen, dass $M_a$ auf zwei unterschiedlichen Rechenwegen definitiv akzeptiert.

Da nun also $u' \supsetneq u \supsetneq w_{\hat{s}-1}$ auch $t'$-gültig ist, sind wir fertig und erreichen einen Widerspruch: während der Bearbeitung von Task $\tau^2_{a,b}$ in Stufe $\hat{s}$ war das Orakel $u'$ eine mögliche $t'$-gültige Erweiterung von $w_{\hat{s}-1}$. Also wäre nach Definition des Tasks $\tau^2_{a,b}$ dann $t_{\hat{s}} = t'$ gesetzt

worden. Damit wäre dann auch $t_s(\tau^2_{a,b}) = t'(\tau^2_{a,b}) = 0$, was der Voraussetzung dieses Lemma 2.10 widerspricht. □

Damit ist die Konstruktion möglich. Sei $O \stackrel{\text{df}}{=} \bigcup_{s\in\mathbb{N}} w_s$. Beachte dass $w_s \sqsubsetneq O$ für alle $w_s$.

Sei außerdem $t_\omega \stackrel{\text{df}}{=} \bigcup_{s\in\mathbb{N}} t_s$. Beachte, dass nach Definition von $t_0, t_1, \ldots$ auch $t_\omega$ eine (totale) Funktion ist. Beachte außerdem, dass $|w_0| < |w_1| < |w_2| < \ldots$ eine nach oben unbeschränkte Folge ist.

### *Eigenschaften des konstruierten Orakels*

Nun müssen wir noch verifizieren, dass $O$ tatsächlich alle gewünschten Eigenschaften erfüllt, die in Satz 2.1 behauptet wurden. Wir starten mit einer Beobachtung über den groben Aufbau von $O$, der sich sofort aus der Ebenen-Konstruktion und unserem Gültigkeitsbegriff ergibt.

**Behauptung 2.11.** *(1) Es gilt $C \subseteq O$ und $O$ und $C$ stimmen auf allen Wörtern der Länge $\neq e(\cdot)$ überein.*

*(2) Es gilt $|C \cup \Sigma^{e(i)}| \leq 2$ für alle $i$.*

*(3) Wenn $t_\omega(\tau^1_j) = 0$, dann gilt $L(N^O_j) \neq \Sigma^*$.*

*(4) Wenn $t_\omega(\tau^2_{a,b}) = m > 0$, dann gilt $|O \cap \Sigma^n| \leq 1$ für alle $n \in H_m$. Insbesondere gilt damit $(A^O_m, B^O_m) \in \text{DisjUP}^O$.*

*(5) Wenn $t_\omega(\tau^3_a) = m > 0$, dann gilt $|O \cap \Sigma^n| \leq 1$ für alle $n \in H_m$. Insbesondere gilt damit $(C^O_m) \in \text{UP}^O$.*

*Beweis.* Zu (1): Wir zeigen zunächst Übereinstimmung. Sei $x$ ein Wort mit $|x| \neq e(\cdot)$. Wir zeigen dass $x \in C$ genau dann wenn $x \in O$. Wähle ein $s$ sodass $x < |w_s|$, heißt $w_s$ wird von $x$ definiert. Nun ist $w_s$ auch $t_s$-gültig, und mit V1 gilt insbesondere $x \in w_s \iff x \in C$. Da nun $w_s \sqsubsetneq O$, gilt auch $x \in O \iff x \in w_s \iff x \in C$ und wir sind fertig.

Für die Inklusion $C \subseteq O$ sei $y \in C$ gegeben. Nach unserer Wahl von $C$ war $C \cap \Sigma^{e(i)} = \emptyset$ für alle $i$, heißt $y$ kann nicht die Länge $e(\cdot)$ haben. Damit gilt dann mit Übereinstimmung auch $y \in O$.

Zu (2): Beweis läuft analog wie bei (1), unter Berufung auf V2.

Zu (3): Nach Voraussetzung muss es ein $s$ geben, für das $t_s(\tau^1_j) = 0$. Insbesondere ist $w_s$ auch $t_s$-gültig, und mit V3 existiert ein $z$ sodass $N^{w_s}_j(z)$ definitiv ablehnt. Da $w_s \sqsubseteq O$, folgt mit Beobachtung 2.2(1), dass $N^O_j(z)$ auch definitiv ablehnen wird.

Zu (4): Angenommen, es existiert ein $n \in H_m$ für das $|O \cap \Sigma^n| > 1$. Wähle ein $s$ sodass $w_s$ alle Wörter der Länge $\leq n$ definiert. Dieses $w_s$ ist insbesondere $t_s$-gültig.

Nun gilt $t_s(\tau^2_{a,b}) = t_\omega(\tau^2_{a,b}) = m > 0$, und mit V5 gilt insbesondere $|w_s \cap \Sigma^n| \leq 1$. Da nun $w_s$ und $O$ auf $\Sigma^n$ übereinstimmen, haben wir auch $|O \cap \Sigma^n| \leq 1$. Das widerspricht der Annahme.

Also gilt $|O \cap \Sigma^n| \leq 1$ für alle $n \in H_m$. Dann folgt aus Beobachtung 2.5(1) auch schon sofort, dass $(A^O_m, B^O_m) \in \text{DisjUP}$.

Zu (5): Beweis läuft analog wie bei (4). □

Über die Definition von Task $\tau^2_{a,b}$ bzw. $\tau^3_{a,r}$ ist nun in Verbindung mit der vorigen Beobachtung auch ersichtlich, dass für DisjNP bzw. UP keine vollständigen Elemente existieren können.

**Behauptung 2.12.** *(1) Kein Paar aus $\text{DisjNP}^O$ ist $\leq^{\text{pp}}_{\text{m}}$-hart für $\text{DisjUP}^O$.*

*(2) Keine Menge aus $\text{UP}^O$ ist $\leq^{\text{p}}_{\text{m}}$-vollständig.*

*Beweis.* Wir zeigen hier nur (1), der Beweis für Aussage (2) folgt analog.

Angenommen es existiert ein solches $\leq^{\text{pp}}_{\text{m}}$-hartes Paar $(U_1, U_2) \in \text{DisjNP}^O$. Dann existieren über die Wahl der Standardenumeration auch zwei NPTM sodass $L(M^O_a) = U_1, L(M^O_b) = U_2$. Betrachte den Task $\tau^2_{a,b}$; dieser wurde in der Konstruktion von $O$ in Stufe $\hat{s}$ bearbeitet. Wir erinnern uns, dass $w_{\hat{s}} \sqsubsetneq O$ ein $t_{\hat{s}}$-gültiges Orakel ist.

Wenn $t_{\hat{s}}(\tau^2_{a,b}) = 0$ ist, dann besagt V4, dass eine Eingabe $x \in \Sigma^*$ existiert für die sowohl $M_a(x)$ als auch $M_b(x)$ definitiv relativ zu $w_{\hat{s}}$ akzeptieren. Da $w_{\hat{s}} \sqsubseteq O$ ist, akzeptieren $M_a(x)$ und $M_b(x)$ relativ zu $O$, nach Beobachtung 2.2(1). Das bedeutet aber $x \in U \cap U'$; Widerspruch zur Wahl von $U, U'$ als disjunkt.

Daher können wir annehmen, dass $m \stackrel{\text{df}}{=} t_{\hat{s}}(\tau^2_{a,b}) > 0$ ist. Insbesondere ist daher $t_\omega(\tau^2_{a,b}) > 0$ und nach voriger Behauptung 2.11(4) gilt dann auch $(A^O_m, B^O_m) \in \text{DisjUP}^O$. Also gilt nach Annahme auch $(A^O_m, B^O_m) \leq^{\text{pp}}_{\text{m}} (U_1, U_2)$ relativ zu $O$.

Sei nun $r$ so gewählt, dass diese Reduktion von $F^O_r$ realisiert wird, und betrachte Task $\tau^2_{i,j,r}$, welcher in einem bestimmten Schritt $s$ behandelt wird. Nach Definition dieses Task existiert ohne Beschränkung der Allgemeinheit ein $n \in \mathbb{N}$ sodass $0^n \in A^O_m$, und $M_a(F_r(0^n))$ definitiv relativ zu $w_s$ ablehnt. (Der andere Fall in dem $M_b$ ablehnt läuft symmetrisch.)

Mit Beobachtung 2.2(1) erhalten wir dann, dass $M_a(F_r(0^n))$ relativ zu $O$ ablehnt. Also auch $F^O_r(0^n) \notin U_1$. Dies widerspricht der Annahme, dass $F^O_r$ die Reduktion realisiert, denn wir haben ja $0^n \in A^O_m$. □

Damit erfüllt $O$ schon die Aussagen (1) und (2) von Satz 2.1. Die letzte Aussage (3) ist aufwändiger zu beweisen. Folgende Behauptung sagt aus, dass totale NPTM $N_j$ relativ zu $O$ „besonders total“ sind. Nimmt man (ab hinreichender Länge) Wörter der Länge $= e(\cdot)$ aus $O$ weg, und erhält $T \subseteq O$, bleibt die NPTM relativ zu $T$ immer noch total. Das ergibt auch Sinn, denn in der Bearbeitung von Task $\tau^1_j$ wurden sämtlichen geeigneten Erweiterungen ausprobiert, welche die Totalität von $N_j$ zerstören würden. Da keine solche Erweiterung existiert, wird auch $T$ nicht die Totalität von $N_j$ zerstören können.

**Behauptung 2.13.** *Sei $N_j$ eine totale NPTM, d.h. $L(N^O_j) = \Sigma^*$. Es existiert eine Länge $n$ mit folgender Eigenschaft: falls $T \subseteq O$ mit $O$ auf Wörtern der Länge $\neq e(\cdot)$ und Wörtern $\leq n$ übereinstimmt, dann $L(N^T_j) = \Sigma^*$.*

*Beweis.* Sei $s$ die Stufe bei der $\tau^1_j$ bearbeitet wurde, und setze $n = |w_s|$. Wir zeigen nun, dass dieses $n$ die behauptete Eigenschaft erfüllt. Angenommen, dies gilt nicht, dann existiert ein $T \subseteq O$ dass mit $O$ auf Wörtern der Länge $\neq e(\cdot)$ und Wörtern $\leq n$ übereinstimmt, aber für ein Wort $z$ lehnt $N^T_j(z)$ ab.

Sei $m \in \mathbb{N}$ so gewählt dass $m > n, p_j(|x|)$, und definiere das folgende partielle Orakel $v$, das genau für alle Wörter der Länge $\leq m$ definiert ist:

$$v[x] \stackrel{\text{df}}{=} \begin{cases} T[x] & \text{falls } |x| \leq m \\ \bot & \text{sonst.} \end{cases}$$

Es ist leicht zu sehen, dass $N^v_j(z)$ definitiv ablehnt, stimmen $v$ und $T$ ja auf allen Wörtern der Länge $\leq p_j(|x|)$ überein. Außerdem ist klar, dass $v \supsetneq w_s \supsetneq w_{s-1}$.

Sei $t' = t_{s-1} \cup \{\tau^1_j \mapsto 0\}$ Wir zeigen unten, dass $v$ auch $t_{s-1}$-gültig ist. Damit ist dann klar, dass $v$ auch $t'$-gültig ist: es kommt nur V3 bezüglich $N_j$ hinzu, aber wir haben ja bereits gesehen dass $N^v_j(z)$ definitiv ablehnt.

Insbesondere ist dann während der Bearbeitung von Task $\tau^1_j$ in Stufe $s$ das Orakel $v$ eine mögliche $t'$-gültige Erweiterung von $w_{s-1}$, denn es ist $t'$-gültig und $v \supsetneq w_{s-1}$. Also wäre nach Definition des Tasks $\tau^1_j$ dann $t_s = t'$ gesetzt worden, und wir hätten $t_s(\tau^1_j) = 0$. Dann wäre aber auch $t_\omega(\tau^1_j) = 0$, und nach voriger Behauptung 2.11(3) damit $L(N^O_j) \neq \Sigma^*$. Widerspruch zur Wahl von $N_j$.

Es bleibt zu zeigen dass $v$ auch $t_{s-1}$-gültig ist. Angenommen, $v$ ist nicht $t_{s-1}$-gültig, dann muss eine Bedingung V1–V7 verletzt sein. Zur Erinnerung: $v \supsetneq w_{s-1}$ und $w_{s-1}$ ist $t_{s-1}$-gültig. Wieder klar ist, dass V3, V4, V6 nicht verletzt sein können, denn jede definite Berechnung relativ zu $w_{s-1}$ ist auch eine definite Berechnung relativ zu $v$ nach Beobachtung 2.2(1).

Angenommen V1 ist verletzt. Dann existiert ein $x < |v|$ und $|x| \neq e(\cdot)$ und $x \in v \nleftrightarrow x \in C$.

Nach Voraussetzung dieser Behauptung stimmen aber $T$ und $O$ auf $x$ überein; wir haben daher

$$x \in v \leftrightarrow x \in T \leftrightarrow x \in O \leftrightarrow x \in C,$$

wobei letzte Äquivalenz aus Beobachtung 2.11(1) folgt. Widerspruch zur Annahme; V1 kann nicht verletzt sein.

Angenommen, V5 ist verletzt. Dann existiert ein $\tau'$ mit $t_{s-1}(\tau') = m' > 0$ und $n' \in H_{m'}$ und $|\Sigma^{n'} \cap v| > 1$. Insbesondere gilt $t_\omega(\tau') = m' > 0$. Außerdem muss $n' \leq m$ sein, da ansonsten $\Sigma^{n'}$ nicht durch $v$ definiert ist (und damit $v \cap \Sigma^{n'} = \emptyset$. Insbesondere stimmen damit $v$ und $T$ auf $\Sigma^{n'}$ überein. Damit gilt

$$|\Sigma^{n'} \cap v| = |\Sigma^{n'} \cap T| \leq |\Sigma^{n'} \cap O| \leq 1,$$

wobei die erste Ungleichung aus $T \subseteq O$ folgt, und die zweite Ungleichung aus voriger Behauptung 2.11(4) bzw. (5) folgt. Das widerspricht der Annahme $|\Sigma^{n'} \cap v| > 1$, also kann V5 nicht verletzt sein. Auf analoge Weise lässt sich zeigen, dass V2 und V7 nicht verletzt sein können.

Damit ist keine Bedingung verletzt, $v$ muss also $t_{s-1}$-gültig sein. □

Nun können wir für die Hypothese Q argumentieren. Hierfür müssen wir, gegeben eine totale NPTM $N_j$, effizient einen akzeptierenden Rechenweg von $N_j^O(x)$ bestimmen. Offensichtlich ist das zumindest relativ zu $C$ (anstelle $O$) möglich, da insbesondere $\mathrm{P}^C = \mathrm{NP}^C$ gilt. Beachte, dass wir $O$ als $C \cup D$ schreiben können, wobei

$$D = O - C = \{w \mid w \in O, \exists i.|w| = e(i)\},$$

und $C$ und $D$ sind insbesondere disjunkt. Beachte dass $C$ das ursprünglich gewählte PSPACE-vollständige Orakel ist, wobei die Ebenen der Höhe $e(\cdot)$ leer waren. Die Menge $D$ entspricht dann genau dem Inhalt dieser Lücken.

Hätten wir nun die Möglichkeit, effizient $D$ entscheiden zu können, dann wäre auch $\mathrm{P}^O = \mathrm{NP}^O$ und wir könnten einen akzeptierenden Rechenweg von $N_j^O(x)$ einfach ausrechnen. Nun können wir zwar $D$ nicht effizient entscheiden, aber wir können mittels $N_j$ und Behauptung 2.13 zunmindest iterativ eine relevante finite Approximation $D' \subseteq D$ von $D$ bestimmen. Das soll kurz skizziert werden: Gegeben unsere finite Approximation $D' \subseteq D$, können wir relativ zu $C \cup D'$ einen akzeptierenden Rechenweg $\alpha$ von $N_j(x)$ ausrechnen. Dieser existiert insbesondere nach Behauptung 2.13. Nun können wir die Orakelfragen auf $\alpha$ mit dem „echten“ $D$ abgleichen, und so überprüfen wo unsere Approximation fehlerhaft ist, und ggf. unsere Apprixmation aktualisieren. Nachdem $D$ dünn ist, enden wir spätestens nach polynomiell vielen Iterationen bei einer Approximation $D'$, die auf allen relevanten Wörtern mit $D$ übereinstimmt.

**Behauptung 2.14.** *Sei $N_j$ eine totale NPTM, d.h. $L(N_j^O) = \Sigma^*$. Dann existiert eine Funktion $g \in \mathrm{FP}^O$ sodass $g(x)$ einen akzeptierenden Rechenweg von $M_j^O(x)$ ausgibt. Damit gilt nach Definition die Hypothese* Q *relativ zu $O$.*

*Beweis.* Wir schreiben erneut $O$ als $C \cup D$, wobei $D \stackrel{\text{df}}{=} O \cap \{w \mid \exists i.|w| = e(i)\}$ Sei $n$ hinreichend groß, sodass diese vorige Behauptung 2.13 erfüllt ist. Damit gilt (mit $T = C \cup D'$)

$$\begin{aligned} &D' \subseteq D, D \text{ stimmt mit Wörtern der Länge} \leq n \text{ mit } D \text{ überein} \\ &\implies L(N_j^{C \cup D'}) = \Sigma^*. \end{aligned} \tag{2.2}$$

Wir betrachten nun folgenden formalen Algorithmus relativ zu $O$ auf Eingabe $x$:

1 $D' \leftarrow \{w \mid w \in O, |w| \leq n, \exists i.|w| = e(i)\}$ *(Konstante, muss nicht berechnet werden)*
2 **wiederhole** *(Invariante:* $D' \subseteq D = O \cap \{w \mid \exists i.|w| = e(i)\}$*)*
3 Sei $\alpha$ ein akzeptierender Rechenweg auf $N_j^{C \cup D'}(x)$ und $Q$ die Menge an Orakelfragen
4 **wenn** existiert eine Frage $q \in Q$ für die $q \in D$ aber $q \notin D'$ **dann**
5 $D' \leftarrow D' \cup \{q\}$
6 **sonst** *(für alle* $q \in Q$ *gilt:* $q \notin D \vee q \in D'$*)*
7 Gebe $\alpha$ aus

Korrektheit: Beobachte zunächst die Invariante dass $D' \subseteq D$. Damit gilt nach (2.2) auch $L(N_j^{C \cup D}) = \Sigma^*$ und insbesondere existiert dann auch ein akzeptierender Rechenweg auf $N_j^{C \cup D}(x)$. Damit ist Z. 3 wohldefiniert. Terminiert nun der Algorithmus mit einem Rechenweg $\alpha$ in Z. 7, dann stimmt aber $D'$ mit $D$ auf $Q$ überein: Falls $q \in D'$, dann auch $q \in D'$ (nach Invariante). Falls $q \notin D'$, dann $q \in D$ (nach Negation der If-Bedingung). Damit stimmen auch $C \cup D'$ und $C \cup D = O$ auf $Q$ überein. Also wird auch $N_j^O(x)$ mit Rechenweg $\alpha$ akzeptieren, nach Beobachtung 2.2(3).

Laufzeit: Wir zeigen dass der Algorithmus in polynomiell beschränkter deterministischer Zeit (abhängig von $|x|$) relativ zu $O$ arbeitet. Wir wissen, dass für jede Orakelfrage $q \in Q$ gilt, dass $|q| \leq p_j(|x|)$. Zusammen mit oben genannten Invariante gilt $D' \subseteq D \cap \{w \mid \exists i.|w| = e(i) \leq p_j(|x|)\}$. Nun ist aber $D$ dünn. Im Speziellen gilt mit Behauptung 2.11(2) dass

$$\ell(D') \leq \sum_{\substack{i \in \mathbb{N} \\ e(i) \leq p_j(|x|)}} \ell(D \cap \Sigma^{e(i)}) = \sum_{\substack{i \in \mathbb{N} \\ e(i) \leq p_j(|x|)}} e(i) \cdot |D \cap \Sigma^{e(i)}| \leq \sum_{\substack{i \in \mathbb{N} \\ e(i) \leq p_j(|x|)}} 2e(i) \leq 2p_j(|x|)^2.$$

Das heißt, dass nach polynomiell vielen Iterationen wird kein weiteres Wort zu $D'$ hinzugefügt und der Algorithmus terminiert.

Wir zeigen nun abschließend, dass Zeile 3 in polynomiell beschränkter deterministischer Zeit berechnet werden kann. Hierfür werden wir das finite $D'$ in $N_j$ „hineincodieren“. Gemeint ist, $D'$ in das „Programm“ $N_j$ hineincodieren, sodass für Queries $q$, $|q| = e(\cdot)$ nur getestet wird ob $q \in D'$ anstelle einer echten Orakelfrage. Es existiert also eine Orakel-NPTM $N_j'$, sodass $N_j'^C(x)$ äquivalent zu $N_j^{C \cup D'}(x)$ arbeitet. Und da $\mathrm{P}^C = \mathrm{PSPACE}^C$, können wir in $\mathrm{FP}^C$ auch einen akzeptierenden Rechenweg $\beta'$ von $N_j'^C(x)$ effizient bestimmen. Das geht dann auch in $\mathrm{FP}^O \supseteq \mathrm{FP}^C$. Also können wir auch einen akzeptierender Rechenweg von $N_j^{C \cup D'}(x)$ in $\mathrm{FP}^O$ berechnen. Beachte insbesondere, dass das Hineincodieren in Polynomialzeit möglich ist, ist ja $\ell(D')$ polynomiell in Abhängigkeit von $|x|$ beschränkt. □

Damit ist der Beweis von Satz 2.1 abgeschlossen: das Orakel $O$ erfüllt alle Eigenschaften. Relativ zu $O$ existiert nach Behauptung 2.12 (1) kein $\leq_{\mathrm{m}}^{\mathrm{pp}}$-hartes Paar in DisjNP für DisjUP, und (2) kein $\leq_{\mathrm{m}}^{\mathrm{p}}$-vollständige Menge für UP. Nach Behauptung 2.14 kann für jede totale NPTM $N_j$ eine Funktion $g \in \mathrm{FP}$ angegeben werden, für die $g(x)$ ein akzeptierender Rechenweg für $N_j(x)$ ist. Mit den Eigenschaften der Standardenumeration ist klar, dass dass auch für *alle* totalen NPTM $N$ gilt. (Übersetze $N$ in äquivalente Standard-NPTM $N_j$, übersetze dann den akzeptierenden Rechenweg $g(x) = \alpha$ von $N_j(x)$ in einen akzeptierenden Rechenweg $\alpha'$ von $N(x)$ zurück.) Damit gilt relativ zu $O$ also auch die Hypothese Q (3).

Wir schließen dieses Kapitel mit einer Zusammenfassung weiterer Eigenschaften von $O$, die sich unmittelbar aus relativierenden Implikationen ergeben.

**Korollar 2.15.** *Folgende Aussagen gelten relativ zum Orakel O:*

*(1)* $\mathrm{P} = \mathrm{UP} \cap \mathrm{coUP} = \mathrm{NP} \cap \mathrm{coNP} \subsetneq \mathrm{UP} \subsetneq \mathrm{NP}$.
*(2)* NP, UP, NE, NEE *sind nicht abgeschlossen unter Komplement.*
*(3)* P, E, EE *sind nicht abgeschlossen unter Nichtdeterminismus.*
*(4)* $\mathrm{UP} \not\subseteq \mathrm{coNP}$.

*(5)* $\mathrm{NPSV}_t \subseteq \mathrm{FP}$.
*(6)* $\mathrm{NP}b\mathrm{V}_t \subseteq_t \mathrm{NPSV}_t$.
*(7)* $\mathrm{NP}k\mathrm{V}_t \subseteq_t \mathrm{NPSV}_t$ *für alle* $k \geq 2$.
*(8)* $\mathrm{NPMV}_t \subseteq_t \mathrm{FP}$.
*(9)* $\mathrm{NPMV}_t \subseteq_t \mathrm{NPSV}_t$.
*(10)* $\mathrm{NPMV}_t \subseteq_t \mathrm{TFNP}$.
*(11)* $\mathrm{NPMV} \subseteq_t \mathrm{NPSV}$.
*(12)* $\mathrm{TFNP} \subseteq_t \mathrm{FP}$.
*(13) Es existiert eine NP-Relation* $R$ *mit* $\leq^p_m$*-vollständigem* $\mathrm{Proj}(R) \in \mathrm{NP}$ *und* $R$ *ist nicht* $\leq^p_L$*-vollständig.*
*(14)* $\mathrm{NP} \cap \mathrm{coNP}$ *hat keine* $\leq^p_m$*-vollständige Menge.*
*(15)* UP *hat keine* $\leq^p_m$*-vollständige Menge.*
*(16)* DisjNP *hat keine* $\leq^{pp}_m$*-vollständiges Paar.*
*(17)* $\mathrm{NPMV}_t$ *hat eine* $\leq^p_m$*-vollständige Multifunktion.*
*(18)* TFNP *hat eine* $\leq^p_m$*-vollständige Multifunktion.*
*(19)* DisjCoNP *hat ein* $\leq^{pp}_m$*-vollständiges Paar.*
*(20) Für keine* $\leq^p_m$*-vollständige Menge* $A \in \mathrm{NP}$ *existiert ein* P*-optimales Beweissystem.*
*(21) Für alle Mengen* $A \in \mathrm{coNP}$ *existiert ein* P*-optimales Beweissystem.*
*(22) Es existiert ein* P*-inseparables* DisjNP*-Paar.*
*(23) Jedes* DisjCoNP*-Paar ist* P*-separierbar.*
*(24) Weder* NP *noch* coNP *haben die* shrinking property.
*(25) Weder* NP *noch* coNP *haben die* separation property.

# 3 *Diskussion und Fazit*

**Korollar 3.1.** *Sei* $\mathsf{A} \in \{\mathsf{DisjNP}, \mathsf{UP}, \mathsf{CON}^{\mathsf{N}}, \mathsf{TAUT}, \mathsf{DisjCoNP}, \mathsf{TFNP}, \mathsf{SAT}\}$. *Für jede Wahl von* A, *jede Wahl von* $\mathsf{A}' \in \{\mathsf{A}, \neg\mathsf{A}\}$, *jede Wal von* $\mathsf{B} \in \{\mathsf{Q}, \neg\mathsf{Q}\}$ *existiert ein Orakel relativ zu diesem* $\mathsf{A}' \wedge \mathsf{B}$ *gilt, außer für die Fälle* $\mathsf{DisjCoNP} \wedge \mathsf{Q}$, $\mathsf{TFNP} \wedge \mathsf{Q}$, $\mathsf{SAT} \wedge \mathsf{Q}$ *(da das einer relativierenden Implikation wiederspricht).*