Komplexität von Suchproblemen und Beweissystemen

Anton Ehrmanntraut

29. September 2023

Inhaltsverzeichnis

1 Einleitung

2 Zur Konzeptionalisierung und Ordnung von Suchproblemen

2.1 Suchprobleme und Levin-Reduktionen

Definition 2.1 (NP-Relation)**.** Eine *NP-Relation* ist eine zweistellige Relation $R \subseteq \Sigma^* \times \Sigma^*$, sodass diese

(1) in Polynomialzeit entscheidbar ist, d.h., $R \in \mathrm{P}$, und

(2) ein Polynom q existiert, sodass

$$(x, y) \in R \implies |y| \leq q(|x|) \quad \text{für alle } x, y \in \Sigma^*. \tag{2.1}$$

Die Wörter der ersten Komponente nennen wir *Probleminstanzen* oder *Instanzen* oder emphProbleme von R, die Wörter der zweiten Komponente nennen wir die *Zertifikate* von R. Wir sagen dann für $(x, y) \in R$, dass y *ein Zertifikat für* x ist. In diesem Sinne sagt (2.1) aus, dass Zertifikate y für x nicht superpolynomiell länger als x sein dürfen. Das Polynom q nennen wir auch die *Zertifikatsschranke* zu R.

Für eine NP-Relation definieren wir

$$\mathrm{Proj}(R) = \{x \mid \exists y \in \Sigma^*, (x, y) \in R\} \in \mathrm{NP}$$

Die Menge $\mathrm{Proj}(R)$ ist also die Menge der Probleminstanzen, für welche ein zugehöriges Zertifikat existiert; damit entspricht $\mathrm{Proj}(R)$ derjenigen Menge, die üblicherweise bei algorithmischen Entscheidungsproblemen betrachtet wird. Die Zugehörigkeit $\mathrm{Proj}(R) \in \mathrm{NP}$ folgt unmittelbar aus den Punkten (1) und (2).

Wir definieren

$$R(x) = \{y \mid y \in \Sigma^*, (x, y) \in R\}$$

als die Menge aller Zertifikate y zu x. Damit gilt unmittelbar

$$x \in \mathrm{Proj}(R) \iff R(x) \neq \emptyset. \qquad \lhd$$

Definition 2.2 (Levin-Reduzierbarkeit)**.** Seien Q, R zwei NP-Relationen. Wir sagen dass Q *sich auf* R *(Polynomialzeit-)Levin-reduzieren lässt*, bzw. $Q \leq_{\mathrm{L}}^{\mathrm{p}} R$ wenn zwei Funktionen $f, g \in \mathrm{FP}$ existieren sodass

(1) $x \in \mathrm{Proj}(Q) \iff f(x) \in \mathrm{Proj}(R)$,

(2) $(f(x), y) \in R \implies (x, g(x, y)) \in Q$.

Punkt (1) sagt also nur aus, dass f eine Many-one-Polynomialzeit-Reduktion zwischen den entsprechenden Entscheidungsproblemen ist. Punkt (2) sagt nun aus, dass wenn y ein Zertifikat für die Instanz $f(x)$ aus R ist, dann lässt sich aus y wieder ein Zertifikat $g(x, y)$ für die originale Instanz x berechnen.

Die Funktion f nennen wir *Reduktionsfunktion*, die Funktion g nennen wir *Translationsfunktion*.

Wir schreiben $Q \leq^{\mathrm{p}}_{\mathrm{L},1} R$ falls f zusätzlich injektiv ist. Wir schreiben $Q \leq^{\mathrm{p}}_{\mathrm{L},1,\mathrm{inv}} R$ falls f zusätzlich injektiv und p-invertierbar ist. Klar ist:

$$Q \leq^{\mathrm{p}}_{\mathrm{L},1,\mathrm{inv}} R \implies Q \leq^{\mathrm{p}}_{\mathrm{L},1} R \implies Q \leq^{\mathrm{p}}_{\mathrm{L}} R \implies \mathrm{Proj}(Q) \leq^{\mathrm{p}}_{\mathrm{m}} \mathrm{Proj}(R).$$

Wir sagen dass $R \leq^{\mathrm{p}}_{\mathrm{L}}$-*vollständig* ist, wenn $Q \leq^{\mathrm{p}}_{\mathrm{L}} R$ für alle NP-Relationen Q gilt. Die $\leq^{\mathrm{p}}_{\mathrm{L},1}$- und $\leq^{\mathrm{p}}_{\mathrm{L},1,\mathrm{inv}}$-Vollständigkeit ist analog definiert. ◁

Satz 2.3. *Die kanonische NP-Relation*

$$\texttt{rKAN} = \{((N, x, 1^n), \alpha) \mid \alpha \textit{ ist ein akz. Rechenweg auf } N(x) \textit{ und } |\alpha| \leq n\}$$

ist $\leq^{\mathrm{p}}_{\mathrm{L},1,\mathrm{inv}}$*-vollständig.*

Beweis. Sei R eine beliebige NP-Relation mit Zertifikatsschranke r, i.e. $(x, y) \in R \implies |y| \leq r(|x|)$. Sei M die PTM welche R entscheidet, mit Laufzeitschranke p. Sei N eine NPTM welche auf Eingabe x zunächst ein Zertifikat $y, |y| \leq r(|x|)$ rät, und dann testet ob $M(x, y)$ akzeptiert. Die Laufzeit von N ist beschränkt auf $p(|(x, y)|) \in O(p(r(|x|)))$ (hier nutzen wir die effiziente Listencodierung von **??** aus). Sei daher q ein Polynom, welches die Laufzeit von N beschränkt.

Definiere die Reduktionsfunktion $f(x) = (N, x, 1^{q(|x|)})$. Wir zeigen zunächst dass

$$x \in \mathrm{Proj}(R) \iff f(x) \in \mathrm{Proj}(\texttt{rKAN}).$$

Wenn $x \in \mathrm{Proj}(R)$, dann existiert ein $y, |y| \leq r(|x|)$ sodass $(x, y) \in R$. Dann wird auch $N(x)$ akzeptieren, nämlich auf jenem Pfad welcher y rät. Es existiert also ein Rechenweg α mit $|\alpha| \leq q(|x|)$ sodass $N(x)$ auf α akzptiert. Dann gilt aber auch $(f(x), \alpha) = ((N, x, 1^{q(|x|)}), \alpha) \in \texttt{rKAN}$. Die Rückrichtung $x \notin \mathrm{Proj}(R) \implies f(x) \notin \mathrm{Proj}(R)$ folgt analog. Es ist klar, dass f injektiv ist, dass f Polynomialzeit-berechenbar und -invertierbar ist.

Es lässt sich außerdem einfach eine Translationsfunktion $g \in \mathrm{FP}$ angeben, die für $g(f(x), \alpha) = y$ aus α das entsprechende geratene Zertifikat y aus α berechenen kann. □

2.2 Zur gemeinsamen Struktur von vollständigen Suchproblemen

Beobachtung 2.4 (Buhrman, Kadin und Thierauf 1998)**.** *Sei L eine beliebige Menge und sei R eine $\leq^{\mathrm{p}}_{\mathrm{L}}$-vollständige NP-Relation. Gilt $L \leq^{\mathrm{p}}_{1,\mathrm{inv}} \mathrm{Proj}(R)$, dann existiert eine $\leq^{\mathrm{p}}_{\mathrm{L}}$-vollständige NP-Relation R mit $\mathrm{Proj}(R) = L$.* TODO: Das kann zu universellem R verstärkt werden!

Beweis. Nach Voruassetzung haben wir eine p-invertierbare Funktion $h \in \mathrm{FP}$ mit $x \in L \iff h(x) \in \mathrm{Proj}(R)$. Definiere nun

$$R_L = \{(x, w) \mid x \in L, (h(x), w) \in R\}.$$

Es ist leicht zu sehen, dass R_L eine NP-Relation ist. Es ist auch leicht zu sehen dass $\mathrm{Proj}(R_L) = L$.

Wir zeigen nun, dass R_L auch $\leq^{\mathrm{p}}_{\mathrm{L}}$-vollständig ist. Sei hierfür Q eine beliebige NP-Relation. Nachdem R ja $\leq^{\mathrm{p}}_{\mathrm{L}}$-vollständig ist, existieren Reduktions- und Translationsfunktionen f, g die $Q \leq^{\mathrm{p}}_{\mathrm{L}} R$ realisieren. Definiere nun

$$f'(x) = h^{-1}(f(x)).$$

Damit gilt zum einen für f'

$$x \in \mathrm{Proj}(Q) \iff f(x) \in \mathrm{Proj}(R) \iff h(\underbrace{h^{-1}(f(x))}_{f'(x)}) \in \mathrm{Proj}(R) \iff f'(x) \in \mathrm{Proj}(R_L),$$

und zum anderen gilt

$$(f'(x), w) \in L_R \implies (h(h^{-1}(f(x))), w) \in R \implies (f(x), w) \in R \implies (x, g(x, w)) \in Q.$$

Damit erfüllen also f' und g die Voraussetzungen an eine Reduktions- bzw. Translationsfunktion und $Q \leq^{\mathrm{p}}_{\mathrm{L}} R_L$, wie gewünscht. □

Damit haben (im unrelativierten Fall) insbesondere alle zu SAT p-isomorphen Mengen eine entsprechende NP-Relation, auch wenn hierbei die Zertifikate nicht „natürlich“ sind.

Definition 2.5 (Sparsame Reduktionen)**.** Seien Q, R NP-Relationen. Wir sagen dass sich Q auf R (in Polynomialzeit) *sparsam* („*parsimonious*“[1]) reduzieren lässt, bzw. $Q \leq^{\mathrm{p}}_{\mathrm{pars}} R$ wenn eine Funktion $f \in \mathrm{FP}$ existiert mit

$$x \in \mathrm{Proj}(Q) \iff f(x) \in \mathrm{Proj}(R) \quad \text{und} \quad |Q(x)| = |R(f(x))|.$$

In anderen Worte, f realisiert eine Many-one-Reduktion von Q auf R, und haben sowohl die originale Q-Instanz x als auch die reduzierte R-Instanz $f(x)$ die gleiche Anzahl an Lösungen. Definiere $Q \leq^{\mathrm{p}}_{\mathrm{pars}}$-Vollständigkeit entsprechend. ◁

1. vgl. Rothe (2008).

Definition 2.6 (Strukturerhaltende Reduktion; Lynch und Lipton 1978)**.** Seien Q, R NP-Relationen. Wir sagen dass sich Q auf R (in Polynomialzeit) *strukturerhaltend reduzieren lässt*, bzw. $Q \leq^{\mathrm{p}}_{\mathrm{st}} R$, zwei Funktionen $f, g \in \mathrm{FP}$ existieren, und

(1) $(x, y) \in Q \implies (f(x), g(x, y)) \in R$ (Vorwärts-Translation von Zertifikaten),

(2) $(f(x), z) \in R \implies \exists y.\, (x, y) \in R \wedge g(x, y) = z$ (g ist quasi “surjektiv”),

(3) Falls $y_1, y_2 \in Q(x)$ und $y_1 \neq y_2$, dann ist auch $g(x, y_1) \neq g(x, y_2)$ (g ist quasi “injektiv”).

Definiere $Q \leq^{\mathrm{p}}_{\mathrm{st}}$-Vollständigkeit entsprechend. ◁

Definition 2.7 (Zertifikats-Isomorphie; Fischer, Hemaspaandra und Torenvliet 1995)**.** Seien Q, R NP-Relationen. Wir sagen dass sich Q auf R (in Polynomialzeit) *zertifikats-isomorph reduzieren lässt*, bzw. $Q \leq^{\mathrm{p}}_{\mathrm{wi}} R$, wenn zwei Funktionen $f, g \in \mathrm{FP}$ existieren, die p-invertierbar (also auch injektiv) sind, und

TODO: das steht so direkt aber nicht bei FHT…

(1) $(x, y) \in Q \implies g(x, y) = (f(x), z) \in R$ (Vorwärts-Translation von Zertifikaten),

(2) $(f(x), z) \in R \implies g^{-1}(f(x), z) = (x, y) \in R$ (g ist quasi “surjektiv“ und implementiert eine effiziente Rückwärts-Translation),

(3) Falls $y_1, y_2 \in Q(x)$ und $y_1 \neq y_2$, dann ist auch $g(x, y_1) \neq g(x, y_2)$, das heißt, mit $g(x, y_1) = (f(x), z_1), g(x, y_2) = (f(x), z_2)$, dass $z_1 \neq z_2$ (g ist quasi “injektiv”)).

Definiere $Q \leq^{\mathrm{p}}_{\mathrm{wi}}$-Vollständigkeit entsprechend. ◁

TODO: Brauchen wir die wi-Isomorphie?

TODO: An dieser Stelle die Definition von Fischer et al. mit der von Lynch et al. gegenüberstellen. Zeige insbesondere dass beide Definionen im Wesentlichen „gleich“ sind, nur dass Lynch/Lipton keine Invertierbarkeit fordert.

Definition 2.8 (Universelle Relationen; Agrawal und Biswas 1992)**.** Sei R eine NP-Relation mit Zertifikatsschranke q. Wir nennen R *streng* wenn für R gilt, dass $(x, y) \in R \implies |y| = q(|x|) > 0$. In anderen Worten, jedes Zertifikat y für x ist nicht ε und hat genau die Länge $q(|x|)$.

Eine Funktion $f \in \mathrm{FP}$ ist eine *projektive Levin-Reduktion* einer strengen Relation Q zu einer zweiten strengen Relation R wenn diese die folgenden Bedingungen erfüllen

(1) $f(x) = (z, \alpha)$ wobei $x, z \in \Sigma^*$ und $\alpha \in \mathbb{N}_{>0}^{q(|x|)}$ ist eine Sequenz von positiven paarweise verschiedenen Indizes der Länge $q(|x|)$.

(2) $\{y[\alpha] \mid y \in R(z)\} = Q(x)$

Wir nennen eine strenge Relation R *universell* wenn sie vollständig bezüglich projektiven Levin-Reduktionen ist. In anderen Worten, wenn für jede strenge Relation Q eine projektive Levin-Reduktion von Q auf R existiert. $\lhd$

Lemma 2.9. *(1) Seien Q, R strenge NP-Relationen. Ist Q auf R reduzierbar über eine projektive Levin-Reduktion, dann ist $Q \leq_{\mathrm{L}}^{\mathrm{p}} R$.*

(2) Ist R universell, dann ist R auch $\leq_{\mathrm{L}}^{\mathrm{p}}$-vollständig. Damit gilt insbesondere auch $Q \leq_{\mathrm{L}}^{\mathrm{p}} R$ für NP-Relationen Q die nicht *streng sind.*

Definition 2.10 (Agrawal und Biswas 1992)**.** Sei R eine NP-Relation mit Zertifikatsschranke q, wobei zusätzlich für R gilt, dass $(x, y) \in R \implies |y| = q(|x|)$. In anderen Worten, jedes Zertifikat y für x hat genau die Länge $q(|x|)$. Wir definieren nun bezüglich einer solchen Relation R:

(1) Die Relation R hat einen *building block*, wenn es ein Element $block \in \mathrm{Proj}(R)$ gibt, sowie paarweise verschiedene $b_1, b_2, b_3 \in \mathbb{N}_{>0}$ sodass

$$\{y[b_1 b_2 b_3] \mid y \in R(block)\} = \Sigma^3 - \{000\}$$

(2) Die Relation R ist *joinable* wenn es eine Funktion $join \in \mathrm{FP}$ gibt sodass

$$join(x_1, \ldots, x_n) = (z, \alpha) \text{ wobei } x_1, \ldots, x_n, z \in \Sigma^* \text{ und } \sum_{k=1}^{n} q(|x_k|) = |\alpha| \leq q(|z|),$$

wobei $\alpha \in \mathbb{N}_{>0}^*$ eine Sequenz von *paarweise verschiedenen* Indizes ist, und

$$\{y'[\alpha] \mid y' \in R(z)\} = \{y_1 \circ y_2 \circ \cdots \circ y_n \mid (\forall k \leq n).\, y_k \in R(x_k)\}.$$

(3) Die Relation R ist *coupable* wenn es eine Funktion $cpl \in \mathrm{FP}$ gibt sodass

$$cpl(x, (i_1, \ldots, i_n), (j_1, \ldots, j_n)) = (z, \alpha) \text{ wobei } x \in \Sigma^*, \; 1 \leq i_1, \ldots, i_n, j_1, \ldots, j_n \leq q(|x|) \text{ und } |\alpha| = q(|x|),$$

wobei wieder $\alpha \in \mathbb{N}_{>0}^*$ eine Sequenz von *paarweise verschiedenen* Indizes ist, und

$$\{y'[\alpha] \mid y' \in R(z)\} = \{y \mid y \in R(x) \text{ und } (\forall k \leq n)(y[i_k] \neq y[j_k])\}.$$

$\lhd$

Satz 2.11. *Sei R eine strenge NP-Relation. Folgende Aussagen sind äquivalent:*

(1) R ist eine universelle Relation.

(2) R hat einen building block*, ist* joinable *und ist* coupable*.*

Diese Äquivalenz gilt nur im unrelativierten Fall.

3 Suchprobleme und die Hypothese Q im Kontext des Pudlákschen Programms

- Will Q in den Pudlák-Baum einordnen: dafür ist es notwendig, diese ordentlich zu relativieren. Insb. will ich zeigen, dass einige bisherige Resultate natürlicherweise auf „Standardbeweissysteme“ vollständiger Mengen übertragen (nicht nur das Standardbeweissystem für SAT).

Definition 3.1 (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.) $\lhd$

Definition 3.2 (Standardbeweissystem)**.** Sei R eine NP-Relation. Wir definieren bezüglich R das *Standardbeweissystem* std_R für $\mathrm{Proj}(R)$ wie folgt:

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

Beobachtung 3.3. *Für jede NP-Relation R ist das Standardbeweissystem std_R ehrlich.*

Beweis. Sei q die Zertifikatsschranke von R, und sei $w = (x, y)$ gegeben sodass $std_R(x, y) = x$. An dieser Stelle müssen wir auf die konkrete Codierung von Beweisen $w = (x, y)$ eingehen. Wie in **??** beschrieben, codieren wir Tupel in einer solchen Weise sodass

$$|w| = |(x, y)| = 2(|x| + |y| + 2) = 2|x| + 2|y| + 4.$$

Da $(x, y) \in R$ gilt für y auch $|y| \leq q(|x|)$. Damit also

$$|w| \leq 2|x| + 2q(|x|) + 4 \leq q'(|x|) = q'(|std_R(w)|).$$

für ein geeignetes Polynom q', wie gewünscht. $\square$

Folgendes Lemma ist eine Generalisierung von Messner (2001, Thm. 5.2)

Lemma 3.4. *Sei R eine NP-Relation die Levin-paddable ist. Folgende Aussagen sind äquivalent:*

(1) Das Standardbweissystem std_R bzgl. R ist p-optimal.

(2) Für alle NTM N (ohne Laufzeitbeschränkung) mit $L(N) = \mathrm{Proj}(R)$ lassen sich akzepierende Rechenwege von N in Zertifikate umrechnen: es existiert eine Funktion $h \in \mathrm{FP}$ sodass

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

(3) Für alle NPTM N mit $L(N) = \mathrm{Proj}(R)$ lassen sich akzepierende Rechenwege von N in Zertifikate umrechnen: es existiert eine Funktion $h \in \mathrm{FP}$ sodass

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

Beweis. (1)⇒(2): Für NTM f_N können wir das assoziierte Beweissystem

$$f_N(x,\alpha) = \begin{cases} x & N(x) \text{ akz. mit Rechenweg } \alpha \\ \bot & \text{sonst} \end{cases}$$

angeben. Es ist klar, dass f_N ein Beweissystem für Proj(R) ist. Aus der p-Optimalität von std_R gilt nun $std_R \leq^{\mathrm{p}} f_N$, bzw. p-simuliert das Standardbeweissystem das Beweissystem f_N. Damit existiert eine Funktion $h \in \mathrm{FP}$ sodass

$$std_R(h(x,\alpha)) = f_N(x,\alpha).$$

Diese Funktion h erfüllt genau die Eigenschaften von (2): Wir haben

$$\begin{aligned} & N(x) \text{ akz. mit Rechenweg } \alpha \implies h(x,\alpha) = x \\ \implies & std_R(h(x,\alpha)) = x \\ \implies & (x, h(x,\alpha)) \in R, \end{aligned}$$

wie gewünscht.

(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. 3.1(3)).

Wir wollen nun zeigen, dass std_R auch p-optimal ist. Sei hierfür f ein beliebiges Beweissystem für Proj(R). Wir zeigen nun, dass $std_R \leq^{\mathrm{p}} f$. 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' ehrlich ist: es ist ehrlich für Eingaben $0z$, denn das Standardbeweissystem std_R ist ehrlich nach Beobachtung 3.3. 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 Polyom 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) gibt es also nun eine Funktion $h \in \mathrm{FP}$ sodass

$$N_{f'}(x) \text{ akz. mit Rechenweg } \alpha \implies (x, h(x,\alpha)) \in R. \tag{3.1}$$

Jetzt können wir $std_R \leq^{\mathrm{p}} f$ zeigen: 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 α_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

$$\begin{aligned} & N_{f'}(x') \text{ akz. mit } \alpha_z \implies (x', \underbrace{h(x', \alpha_z)}_{y'}) \in R \text{ nach (3.1)} \\ \implies & (pad(x, 1^{|1z|}), y') \in R \text{ mit } y' = h(x', \alpha_z) \text{ und obiger Def. von } x' \\ \implies & (x, \underbrace{padsol(x, 1^{|1z|}, y')}_{y}) \in R \\ \implies & std(x,y) = x \text{ mit } y = padsol(x, 1^{|1z|}, y') \end{aligned}$$

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. □

Folgendes Lemma ist eine Generalisierung von Fenner u. a. (2003, Thm. 2)

Lemma 3.5. *Sei R eine $\leq_{\mathrm{L}}^{\mathrm{p}}$-vollständige NP-Relation, mit der zusätzlichen Eigenschaft dass für die jeweilige entsprechende Problem-Reduktionsfunktion $f\colon Q \to R$ für $Q \leq_{\mathrm{L}}^{\mathrm{p}} R$ immer gilt, dass f ehrlich ist. Folgende Aussagen sind äquivalent:*

(1) Für alle NPTM N mit $L(N) = \mathrm{Proj}(R)$ lassen sich akzepierende Rechenwege von N in Zertifikate umrechnen: es existiert eine Funktion $h \in \mathrm{FP}$ sodass

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

(2) Für alle NPTM N mit $L(N) = \Sigma^*$ lassen sich aus Eingabe x Rechenwege von $N(x)$ effizient bestimmen: es existiert $r \in \mathrm{FP}$ sodass $N(x)$ auf Rechenweg $r(x)$ akzeptiert. (Das ist die Aussage Q.*)*

Beweis. (2)⇒(1): Sei R eine beliebige NP-Relation mit Zertifikatsschranke q, und sei N eine beliebige NPTM mit $L(N) = \mathrm{Proj}(R)$. Definiere nun die NPTM $N'(w)$ wie folgt:

```
1 wenn w nicht von der Form (x, α) dann akzeptiere
2 (x, α) ← w
3 wenn N(x) akzeptiert nicht auf Rechenweg α dann akzeptiere
4 sonst
    (Ab hier gilt x ∈ Pr(R), also auch R(x) ≠ ∅)
5   Rate nichtdeterministisch y ∈ Σ^{≤q(|x|)}
6   Akzeptiere genau dann wenn (x, y) ∈ A.
```

Es ist nun leicht zu sehen dass $L(N') = \Sigma^*$. Nach Voraussetzung (2) existiert eine Funktion $r \in \mathrm{FP}$ sodass für alle x die Maschine $N(w)$ auf Rechenweg $r(w)$ akzeptiert. Nun gilt

$$\begin{aligned} &N(x) \text{ akz. mit Rechenweg } \alpha \\ &\implies N'(x,\alpha) \text{ akz. in Z. 6} \\ &\implies N'(x,\alpha) \text{ akz. mit Rechenweg } r(x,\alpha) \text{ in Z. 6,} \end{aligned}$$

und aus diesem Rechenweg $r(x,\alpha)$ kann effizient der geratene Zeuge $y \in R(x)$ aus Z. 5 ausgelesen werden. Da $r \in \mathrm{FP}$ existiert also auch ein $h \in \mathrm{FP}$ sodass $h(x,\alpha)$ genau diesen geratenen Zeugen y berechnet. Wir haben dann also

$$\implies (x, h(x,\alpha)) \in R,$$

wie gewünscht.

(1)⇒(2): Sei R eine $\leq_{\mathrm{L}}^{\mathrm{p}}$-vollständige NP-Relation unter ehrlichen Problem-Reduktionsfunktionen, und Zertifikatsschranke p. Sei nun N eine NPTM mit $L(N) = \Sigma^*$. Betrachte die entsprechende NP-Relation

$$R_N = \{(x,\alpha) \mid N(x) \text{ akz. mit Rechenweg } \alpha\}$$

Da R ja vollständig ist, gilt $R_N \leq_{\mathrm{L}}^{\mathrm{p}} R$ via $f, g \in \mathrm{FP}$ 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 ∈ Σ^{≤q(|w|)}
2 wenn f(x) = w dann akzeptiere
  (Ab hier kann man x wegwerfen)
3 Rate nichtdeterministisch y ∈ Σ^{≤p(|w|)}
4 Akzeptiere genau dann wenn (w, y) ∈ R.
```

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

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

wie gewünscht.

Nach Voraussetzung (1) gilt nun also, dass eine Funktion $h \in \mathrm{FP}$ 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 α_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 (2) zu zeigen müssen wir aus $x \in \Sigma^*$ effizient einen akzeptierenden Rechenweg für N bestimmen. Wir haben

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

mit $r \in \mathrm{FP}$, $r(x) = g(h(f(x), \alpha_x))$, wie gewünscht. □

Lemma 3.6. *Die in Lemma 3.4 und 3.5 genannten Voraussetzungen an die NP-Relation R werden von allen solchen R erfüllt, die $\leq_{\mathrm{L}}^{\mathrm{p}}$-vollständig sind und Levin-paddable sind.*

Beweis. Es ist sofort klar, dass R die Voraussetzungen von Lemma 3.4 erfüllt. Es bleibt nur zu zeigen, dass für jede NP-Relation Q eine $\leq_{\mathrm{L}}^{\mathrm{p}}$-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 $Q \leq_{\mathrm{L}}^{\mathrm{p}} R$; 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

$$f'(x) = pad(f(x), 1^{|x|}).$$

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

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

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. □

3.1 Welche Suchprobleme sind paddable?

Beobachtung 3.7. *Die kanonische Levin-vollständige NP-Relation* `rKAN` *ist Levin-paddable.*

Beobachtung 3.8. *(1) Gilt* `rKAN` $\leq_{\mathrm{L}}^{\mathrm{p}} R$*, und ist die zugehörige Reduktionsfuktion f ehrlich, dann ist R Levin-paddable*

(2) Jede $\leq_{\mathrm{L,inv}}^{\mathrm{p}}$-vollständige NP-Relation R ist auch Levin-paddable.

Korollar 3.9. *Jede $\leq^{\mathrm{P}}_{\mathrm{L,inv}}$-vollständige Relation R erfüllt die in Lemma 3.4 und 3.5 genannten Voraussetzungen an die NP-Relation R.*

Das sind im unrelativierten Fall u.a. ᴦSAT, ᴦSETCOVER, ᴦVERTEXCOVER, ᴦCLIQUE, ᴦ3COLORABILITY.

So das Textbook von Goldreich (2008).

Beweis zu Beobachtung 3.8. Aussage (2) folgt unmittelbar aus (1): Wir haben ᴦKAN $\leq^{\mathrm{P}}_{\mathrm{L,inv}}$ R und damit ist die entsprechende Reduktionsfunktion f p-invertierbar, und damit ehrlich.

Für (1) nutzen wir die Levin-Paddability von ᴦKAN aus: übersetze Instanz x von R nach ᴦKAN, padde dort hoch, und überetze 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 ᴦKAN $\leq^{\mathrm{P}}_{\mathrm{L}}$ R bezeugen, und seinen analog f', g' jene Funktionen, welche $R \leq^{\mathrm{P}}_{\mathrm{L}}$ ᴦKAN bezeugen. Erstere existieren nach Voraussetzung, zweitere existieren weil ᴦKAN $\leq^{\mathrm{P}}_{\mathrm{L}}$-vollständig ist. Nach Voraussetzung ist f ehrlich. Und nach Beobachtung 3.7 existieren für ᴦKAN Padding-Funktionen $pad_{\text{ᴦKAN}}$, $padsol_{\text{ᴦKAN}}$. Sei q ein entsprechendes Polynom mit $q(|pad_{\text{ᴦKAN}}(x, 1^n)|) \geq n$, $q(|f(x)|) \geq |x|$.

Definiere nun

$$pad_R(x, 1^n) = f(pad_{\text{ᴦKAN}}(f'(x), 1^n)).$$

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

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

Ferner gilt

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

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 $p = pad_{\text{ᴦKAN}}(f'(x), 1^n)$, dann gilt

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

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

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

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

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

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

Beobachtung 3.10. *Jede NP-Relation mit einem* building block *und die* joinable *ist, ist auch Levin-paddable.*

Korollar 3.11. *Im unrelativierten Fall erfüllt jede universelle Relation R die in Lemma 3.4 und 3.5 genannten Voraussetzungen an die NP-Relation R.*

Das sind u.a. ᴦSAT, ᴦHAM, ᴦINDSET, ᴦKNAPSACK, ᴦMAXCUT.

Beweis zu Beobachtung 3.10. Sei R eine NP-Relation, mit zugehörigem Polynom q, welches die Zertifikatsgröße spezifiziert. Zur Erinnerung, dieses Polynom ist streng monoton steigend, und aus $(x, y) \in R$ folgt $|y| = q(|x|)$. 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 Voraussetzung hat die Relation R einen *building block block*. Es lässt sich leicht aus der Definition eines *building block* ableiten, dass $|block| > 0$ und $block \in \text{Proj}(R)$. Damit gilt auch dass die Zertifikate y zu $block$ die Länge $l = q(|block|) \geq |block| \geq 1$ haben.

Es sieht nicht danach aus, dass wir über die Anzahl an Zertifikaten für x' die Länge abschätzen können: ist $x \notin \text{Proj}(R)$ dann hätte auch x' keine Zertifikate, und könnte sich erlauben entsprechend kurz zu sein.

Nach Voraussetzungen ist die Relation R auch *joinable*, das heißt wir haben eine Funktion $join \in \text{FP}$. Sei

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

Wir werden nun über die Länge $|\delta|$ auf die Länge von Zertifikaten zu x' schließen, und damit $|x'|$ beschränken. Nach Definition ?? gilt

$$|\delta| = q(|x|) + q(n) \cdot q(|block|) = q(|x|) + q(n) \cdot l \geq n.$$

Beob. dass unter Definition ?? alle Zertifikate y' für x' die feste Länge $q(|x'|)$ haben. Zur Erinnerung: wir haben

$$\{y'[\delta] \mid y' \in \Sigma^{q(|x'|)}, (x', y') \in R\} = \{yy_1y_2 \cdots y_n \mid y \in \Sigma^{q(|x|)}, y_1, y_2, \dots \in \Sigma^l, \\ (x, y), (block, y_1), (block, y_2), \dots \in R\} \quad (3.2)$$

Die Sequenz δ besteht nach Definition aus paarweise verschiedenen Indizes, daher können wir argumentieren, dass auch alle Zertifikate y' (mit vorgegebener Länge $q(|x'|)$) mindestens die Länge $|\delta|$ haben. Damit gilt

$$q(|x'|) \geq |\delta| \geq n$$

wie gewünscht.

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

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

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: Gilt $x \notin \text{Proj}(R)$, dann ist die rechte Menge in (3.2) 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 weiters y_i für *block*. 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 δ leicht möglich:

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

Wir verifizieren: Sei $(pad(x, 1^n), y') \in R$, dann ist nach (3.2) $y'[\delta] = yy_1y_2 \cdots$ wobei $y \in \Sigma^{q(|x|)}$, $(x, y) \in R$. Wir haben

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

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

3.2 Hypothese Q und die Vollständigkeit von Suchproblemen

Satz 3.12 (Äquivalente Formulierungen der Hypothese Q; Fenner u. a. 2003; Messner 2001)**.** *Folgende Aussagen sind äquivalent:*

(1) Hypothese Q*: Für jede NPTM N mit $L(N) = \Sigma^*$ existiert eine Funktion*

$g \in \mathrm{FP}$ *sodass für alle* x *das Bild* $g(x)$ *eine akzeptierende Berechnung von* $N(x)$ *ist.*

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

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

(4) Jede surjektive ehrliche Funktion $f \in \mathrm{FP}$ *ist p-invertierbar.*

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

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

(6) Für jedes Paar von NP-Relationen A, B *und jede Funktion* $f \in \mathrm{FP}$ *gilt:*

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

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

(8) Es existiert eine $\leq^{\mathrm{p}}_{\mathrm{L}}$*-vollständige Levin-paddable NP-Relation* R *sodass für alle NPTM* N *mit* $L(N) = \mathrm{Proj}(R)$ *gilt: es existiert eine Funktion* $h \in \mathrm{FP}$ *mit*

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

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

(10) Es existiert eine $\leq^{\mathrm{p}}_{\mathrm{L,1,inv}}$*-vollständige NP-Relation* R *sodass für jede Menge* $S \in \mathrm{P}$ *mit* $S \subseteq \mathrm{Proj}(R)$ *gilt: es existiert eine Funktion* $g \in \mathrm{FP}$ *sodass*

$$x \in S \implies (x, g(x)) \in R.$$

Beweis. 1. (1) $\iff$ (2) $\iff$ (3) $\iff$ (4) $\iff$ (5): nach Fenner u. a. (2003, Thm. 2).

2. (1) $\iff$ (8) $\iff$ (9): nach Lemma 3.5 und 3.4.

3. (5) $\implies$ (10): Wir zeigen eine stärkere Variante von (10), welche sich über *alle* NP-Relationen R estreckt (und damit auch über $\leq^{\mathrm{p}}_{\mathrm{L,1,inv}}$-vollständige `rKAN`, wie von (10) gefordert). Sei R eine beliebige NP-Relation, wobei Polynom q die Zertifikatsgröße beschränkt. Sei nun $S \subseteq \mathrm{Proj}(R)$ mit $S \in \mathrm{P}$. Definiere die NPTM N, welche auf Eingabe x folgendes leistet: teste zuerst ob $x \in S$; falls nicht, lehne sofort ab. Rate dann ein $y \in \Sigma^{\leq q(|x|)}$ und akzeptiere genau dann wenn $(x, y) \in R$.

Klar ist, dass $L(N) = S$. Nach (5) existiert nun eine Funktion $h \in \mathrm{FP}$, die für $x \in S$ einen akzeptierenden Rechenweg $h(x)$ von $N(x)$ ausgibt. Wir können sogar aus $h(x)$ das geratene Zertifikat y extrahieren. Es ist daher leicht eine Funktion $g \in \mathrm{FP}$ anzugeben für die $(x, g(x)) \in R$ für alle $x \in S$.

4. (10) $\implies$ (5): Sei $L \in \mathrm{P}$ und sei N eine NPTM mit $L(N) = L$, wobei das Polynom q die Laufzeit beschränkt. Wir wollen eine Funktion $h \in \mathrm{FP}$ definieren sodass $h(x)$ ein akzeptierender Rechenweg von $N(x)$ für $x \in L$ ist. Definiere die NP-Relation

$$Q = \{(x, y) \mid N(x) \text{ akzeptiert mit Rechenweg } y \in \Sigma^{\leq q(|x|)}\}.$$

Nachdem (10) gilt, haben wir eine $\leq^{\mathrm{p}}_{\mathrm{L,1,inv}}$-vollständige NP-Relation R. Damit gilt $Q \leq^{\mathrm{p}}_{\mathrm{L}} R$ mittels Reduktions- bwz. Translationsfunktion $f, k \in FP$. Insbesondere existiert eine Inverse $f^{-1} \in \mathrm{FP}$ zu f.

Sei $S = f(L)$ die Bildmenge der Elemente aus L, also

$$S = \{f(x) \mid x \in L\}.$$

Es ist leicht zu sehen dass $S \subseteq \text{Proj}(R)$. Außerdem ist $S \in \text{P}$: teste $z \in S$ indem getestet wird ob $f^{-1}(z) = x \neq \perp$ und ob $x \in L$.

Damit sind die Voraussetzungen von (10) erfüllt, und es existiert eine Funktion $g \in \text{FP}$ sodass $(z, g(z)) \in R$ für alle $z \in S$. Damit gilt

$$\begin{aligned} & x \in L \implies f(x) \in S \implies (f(N, x), g(f(x))) \in R \\ & \implies ((x), k(g(f(x)))) \in Q \\ & \implies N(x) \text{ akz. mit Rechenweg } \underbrace{k(g(f(x)))}_{h(x)}. \end{aligned}$$

Definiere nun die gesuchte Funktion $h \in \text{FP}$ mit $h(x) = k(g(f(x)))$. Damit gilt für alle $x \in L$ dass $N(x)$ mit Rechenweg $h(x)$ akzeptiert, wie gewünscht.

5. (1) $\implies$ (6): Die Richtunng von rechts nach links ist klar. Für die andere Richtung sei $\text{Proj}(A) \leq^{\text{p}}_{\text{m}} \text{Proj}(B)$ 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 $f \in \text{FP}$ die Funktion, welche die Reduktion $\text{Proj}(A) \leq^{\text{p}}_{\text{m}} \text{Proj}(B)$ realisiert.

Definiere folgende NPTM N, die wie folgt auf Eingabe w arbeitet:

1 **wenn** w nicht von der Form (x, y') **dann** akzeptiere
2 $(x, y') \leftarrow w$
3 **wenn** $(f(x), y') \notin B$ **dann** akzeptiere
4 **sonst**
  (Ab hier gilt $f(x) \in \text{Pr}(B)$ und $x \in \text{Pr}(A)$)
5 Rate nichtdeterministisch $y \in \Sigma^{q(|x|)}$
6 Akzeptiere genau dann wenn $(x, y) \in A$.

Es ist leicht zu sehen dass $L(N) = \Sigma^*$. Nach (1) existiert nun also eine Funktion g sodass, für alle w, $g(w)$ eine akzeptierender Rechwenweg von $N(w)$ ist.

Damit lässt die Levin-Reduktion von A auf B angeben: wähle f als Reduktionsfunktion, und definiere g' als Translationsfunktion, welche aus dem akzeptierenden Rechenweg $g(x, y')$ das geratene Zertifikat y von Zeile 5 ausliest. Dann gilt

$$\begin{aligned} & (f(x), y') \in B \implies N(x, y') \text{ akz. auf einem Rechenweg in Z. 6, ratet } y \\ & \implies (x, y) = (x, g'(x, y')) \in A \end{aligned}$$

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

6. (6) $\implies$ (8): Sei R eine beliebige $\leq^{\text{p}}_{\text{L}}$-vollständige und Levin-paddable NP-Relation (diese existiert immer) und sei N eine NPTM N mit $L(N) = \text{Proj}(R)$, wobei das Polynom q die Laufzeit von N beschränkt. Definiere

$$Q = \{(x, y) \mid N(x) \text{ akzeptiert mit Rechenweg } y \in \Sigma^{\leq q(|x|)}\}.$$

Es ist klar, dass $\text{Proj}(R) \leq^{\text{p}}_{\text{m}} \text{Proj}(Q) = L(N) = \text{Proj}(R)$ über die Identiätsfunktion. Nach (6) gilt nun auch $R \leq^{\text{p}}_{\text{L}} Q$. mit Identitätsfunktion als Reduktionsfunktion und $h \in \text{FP}$ als Translationsfunktion. Damit gilt

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

wie gewünscht.

7. (2) $\implies$ (7): 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 haben wir $g \leq h$, das heißt es existiert eine (nicht notwendigerweise effiziente) Funktion f sodass $g(w) = h(f(w))$, und gleichzeitig ist $|f(w)| \leq q(|w|)$ für ein geeignetes Polynom q.

Betrachte folgende Multifunktion f':

$$f'(w) \mapsto y \iff \exists y \in \Sigma^{\leq q(|w|)}, g(w) = h(y).$$

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

Nach (2) gilt also $f' \in \text{NPMV}_t \subseteq_c \text{FP}$, also existiert eine Funktion $f'' \in$ 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

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

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

8. (7) $\Longrightarrow$ (9): klar, denn ʀKAN ist $\leq^{\text{p}}_{\text{L}}$-vollständig, ist Levin-paddable, und das Standardbeweissystem $\mathit{std}_{\text{ʀKAN}}$ ist (wie jedes Standardbeweissystem einer NP-Relation) optimal. Zusammen mit (7) ist es also auch p-optimal. □

Satz 3.13 (Formulierung Hypothese Q durch NP-Relationen, ∀-Variante)**.** *Folgende Aussagen sind äquivalent:*

(1) Hypothese Q

(8′) Für jede $\leq^{\text{p}}_{\text{L}}$-vollständige Levin-paddable NP-Relation R, und für alle NPTM N mit $L(N) = \text{Proj}(R)$ gilt: es existiert eine Funktion $h \in$ FP mit

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

(9′) Für jede $\leq^{\text{p}}_{\text{L}}$-vollständige Levin-paddable NP-Relationen R ist das Standardbeweissystem std_R p-optimal.

(10′) Für jede NP-Relation P und jede Menge $S \in \text{P}$ mit $S \subseteq \text{Proj}(P)$ gilt: es existiert eine Funktion $g \in$ FP sodass

$$x \in S \implies (x, g(x)) \in P.$$

Beweis. 1. (8′) $\Longrightarrow$ (1), (9′) $\Longrightarrow$ (1), (10′) $\Longrightarrow$ (1): Die NP-Relation ʀKAN ist $\leq^{\text{p}}_{\text{L,1,inv}}$-vollständig (und damit auch Levin-paddable). Gilt also (8′), dann auch die existentielle Variante (8) von vorigem Satz 3.12, und damit (1). Beweise der anderen Implikationen sind analog.

2. (1) $\Longrightarrow$ (8′): Folgt aus Lemma 3.5.

3. (8′) $\Longrightarrow$ (9′): Sei R eine beliebige $\leq^{\text{p}}_{\text{L}}$-vollständige Levin-paddable NP-Relation. Nach Voraussetzung können wir für jede NPTM N, $L(N) = \text{Proj}(R)$ eine Funktion $h \in FP$ angeben sodass

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

Das ist genau die erste der der äquivalenten Aussagen in Lemma 3.4. Damit gilt auch bezüglich *diesem* gewählten R auch die zweite der äquivalenten Aussagen, nämlich dass std_R p-optimal ist.

4. (1) $\Longrightarrow$ (10′): Im Beweis von Satz 3.12 wurde (1) $\Longrightarrow$ (5) $\Longrightarrow$ (10) gezeigt. Beachte insbesondere dass im Beweis zur zweiten Implikation sogar eine stärkere Aussage bewiesn wurde, welche die Aussage (10) für alle NP-Relationen (und nicht nur vollständige) zeigt. Das entspricht genau der hier aufgestellten Aussage (10′), wie gewünscht.

□

3.3 Karp-Vollständigkeit vs. Levin-Vollständigkeit

Vermutung 3.14 (Karp-vs-Levin-Vermutung; KvL)**.** *Es existiert eine NP-Relation R sodass* $\mathrm{Proj}(R)$ $\leq_{\mathrm{m}}^{\mathrm{p}}$*-vollständig für* NP *ist, aber R ist nicht* $\leq_{\mathrm{L}}^{\mathrm{p}}$*-vollständig (für alle NP-Relationen).*

Satz 3.15. $\mathsf{KvL} \implies \neg\mathsf{Q}$.

> *Beweis.* Wir zeigen die Kontraposition, und starten mit der Voraussetzung Q. Wir wollen nun $\neg$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 3.12 gilt also auch die Aussage 3.12(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 $\neg$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 $\neg$Q, also genau die Umkehrung von Satz 3.15. Betrachten wir hier exemplarisch den Fall für Relationen, die SAT bezeugen.

Starten wir mit $\neg$Q, dann haben wir über Satz 3.12 auch die Negation von Aussage 3.12(8). Nachdem rSAT eine $\leq_{\mathrm{L}}^{\mathrm{p}}$-vollständige Levin-paddable NP-Relation ist, muss auch eine NPTM N existiere, für die $L(N) =$ SAT, aber für alle Funktionen $h \in \mathrm{FP}$ gilt

$$N(\varphi) \text{ akz. mit Rechenweg } w \implies (\varphi, h(\varphi, w)) \in \mathsf{rSAT}. \tag{3.3}$$

In anderen Worten: es existiert zwar eine NPTM N welche die ($\leq_{\mathrm{m}}^{\mathrm{p}}$-vollständige Menge) SAT entscheidet, aber aus den akzeptierenden Rechenwegen w von $N(x)$ auf $x \in$ 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 3.3 so verstanden werden, dass $\mathsf{rSAT} \not\leq_{\mathrm{L}}^{\mathrm{p}} R_N$ *falls die Reduktionsfunktion f die Identitätsfunktion ist.* An dieser Stelle muss erneut hervorgehoben werden, dass im Allgemeinen $\mathsf{rSAT} \leq_{\mathrm{L}}^{\mathrm{p}} R_N$ mit Funktionen f, g gelten kann, notwendig hierfür ist aber dass $f \neq \mathrm{id}$.

Gleichzeitig wäre die Existenz einer solchen Reduktion überraschend. Angenommen $\mathsf{rSAT} \leq_{\mathrm{L}}^{\mathrm{p}} R_N$ wird von f, g ($f \neq \mathrm{id}$) realisiert, dann haben wir nach Definition

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

Einerseits ist es also nicht möglich, aus w effizient eine akzeptierende Belegung für $f(\varphi) \neq \varphi$ zu bestimmen. Andererseits reicht der „Beweis“ w aber aus, um (zusammen mit der Information φ) effizient wieder eine erfüllende Belegung für φ zu berechnen.

Ich vermute, dass solche Funktionen f, g nicht jeweils für alle NPTM N mit $L(N) =$ SAT existieren können. Tatsächlich können wir die eben formulierte Vermutung auch in der Theorie der Beweissystemen formulieren. Wir definieren zunächst eine abgeschwächte Variante der p-Simulation.

Definition 3.16. Seien h, h' Beweissysteme für L. Das Beweissystem h *p-simuliert effektiv* h' falls Funktionen $f, g \in \mathrm{FP}$ existieren sodass

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

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

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

Nicht vergessen: es ist offenbar unklar, wie das Symbol $\leq$ bzgl. Simulation gebraucht wird. Dose/Glaßer würden in der Def. das Ordnungszeichen spiegeln, Krajíček/Pudlák dagegen genau so wie hier.

In anderen Worten, falls $h \leq^{p}_{\mathrm{eff}} h'$, 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.

Klar ist: p-Simulation impliziert effektive p-Simulation impliziert Simulation unter Beweissystemen.

Vermutung 3.17 (KvL formuliert unter Beweissystemen)**.** *Das Standardbeweissystem sat für* SAT *kann nicht alle anderen optimalen Beweissysteme für* SAT *effektiv p-simulieren.*

In anderen Worten, es existiert optimales Beweissystem h sodass std $\not\leq^{\mathrm{p}}_{\mathrm{eff}} h$.

Dass die Formulierung der Vermutungen 3.14 und 3.17 äquivalent sind, zeigt folgende Beobachtung:

Beobachtung 3.18. *Folgende Aussagen sind äquivalent:*

(1) Jede NP-Relation R mit $\leq^{\mathrm{p}}_{\mathrm{m}}$-vollständigem $\mathrm{Proj}(R)$, ist auch $\leq^{\mathrm{p}}_{\mathrm{L}}$-vollständig.

(2) Für alle optimalen Beweissysteme h für SAT *gilt std $\leq^{\mathrm{p}}_{\mathrm{eff}} h$.*

Beweis. (1)⇒(2): Wir zeigen, dass *sat* jedes andere optimale Beweissystem h effektiv p-simulieren kann. Nachdem h optimal ist, hat es auch kurze Beweise: für jedes $\varphi \in \mathtt{SAT}$ einen h-Beweis w mit $|w| \leq q(|\varphi|)$. Definiere

$$R_h = \{(\varphi, w) \mid |w| \leq q(|\varphi|), h(w) = \varphi\}.$$

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

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

$$(f(\varphi), w) \in R_h \implies (\varphi, g(\varphi, w)) \in \mathtt{rSAT}.$$

Nach Definition gilt also

$$h(w) = f(\varphi) \implies sat(g(\varphi, w) = \varphi,$$

und damit ist $sat \leq^{\mathrm{p}}_{\mathrm{eff}} h$.

(2)⇒(1): Sei R eine NP-Relation wobei $\mathrm{Proj}(R) \leq^{\mathrm{p}}_{\mathrm{m}}$-vollständig ist. Wir zeigenen nun, dass R auch $\leq^{\mathrm{p}}_{\mathrm{L}}$-vollständig ist. Aus der $\leq^{\mathrm{p}}_{\mathrm{m}}$-Vollständigkeit folgt unmittelbar die Existenz einer Reduktionsfunktion f mit

$$\varphi \in \mathtt{SAT} \iff f(\varphi) \in \mathrm{Proj}(R).$$

Definiere

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

Wir zeigen, dass h ein Beweissystem für SAT ist. Es ist offenbar dass $h \in \mathrm{FP}$. Die Funktion h ist korrekt: wenn $h(x, y, \varphi) = \varphi$ dann ist $f(\varphi) = x \in \mathrm{Proj}(R)$ und nach Eigenschaft von f auch $\varphi \in \mathtt{SAT}$. Die Funktion h ist vollständig: Sei

$\varphi \in \mathtt{SAT}$. Dann ist schon $f(\varphi) \in \mathrm{Proj}(R)$ und es gibt ein y mit $(f(\varphi), y) \in R$. Also ist $(f(\varphi), y, \varphi)$ ein h-Beweis für φ.

Außerdem ist klar, dass h ehrlich ist. Definiere

$$R_h = \{(\varphi, w) \mid h(w) = \varphi\},$$

diese Relation ist damit eine NP-Relation. Wir wollen nun zeigen dass $\mathtt{rSAT} \leq^{\mathrm{p}}_{\mathrm{L}} R_h \leq^{\mathrm{p}}_{\mathrm{L}} Q$, womit dann Q auch $\leq^{\mathrm{p}}_{\mathrm{L}}$-vollständig ist, wie gewünscht.

Wir starten mit der zweiten Reduktion. Es gilt $R_h \leq^{\mathrm{p}}_{\mathrm{L}} Q$, denn es gilt

$$(f(\varphi), y) \in Q \implies h(\underbrace{f(\varphi), y, \varphi}_{g(\varphi, y)}) = \varphi \implies (\varphi, g(\varphi, y)) \in R_h,$$

wobei $g(\varphi, y) = (f(\varphi), y, \varphi)$.

Für die erste Reduktion nutzen wir die Voraussetzung. Es gilt nach Voraussetzung $std \leq^{\mathrm{p}}_{\mathrm{eff}} h$. Damit existieren also Funktionen $f', g' \in \mathrm{FP}$ mit

$$\varphi \in \mathtt{SAT} \iff f'(\varphi) \in \mathtt{SAT}$$
$$h(w) = f'(\varphi) \implies sat(g'(\varphi, w)) = \varphi.$$

Jetzt ist aber auch klar, dass f', g' die Reduktion $\mathtt{rSAT} \leq^{\mathrm{p}}_{\mathrm{L}} R_h$ realisieren, denn nun gilt

$$(f'(\varphi), w) \in R_h \implies (\varphi, g'(\varphi, w)) \in \mathtt{rSAT}.$$

□

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

Vermutung 3.19 ($\mathsf{SAT}^{\mathsf{eff}}$)**.** *Kein optimales Beweissystem für* SAT *kann alle anderen optimalen Beweissysteme für* SAT *effektiv p-simulieren. In anderen Worten, für jedes optimales Beweissystem h existiert ein optimales Beweissysteme h' sodass $h \not\leq^{\mathrm{p}}_{\mathrm{eff}} h'$.*

Satz 3.20. *(1)* $\mathsf{SAT}^{\mathsf{eff}} \implies \mathsf{SAT}$

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

Beweis. Zu (1): Klar aus Kontraposition. Wenn ein p-optimales Beweissystem h für SAT existiert, dann kann dieses (optimale) h auch alle anderen Beweissysteme p-simulieren, und damit insbesondere auch alle optimalen Beweissyste h' effektiv p-simulieren.

Zu (2): Wieder klar aus Kontraposition. Unter $\neg\mathsf{KvL}$ folgt mit der Formulierung aus Vermutung 3.17 dass das (optimale) Standardbeweissystem *sat* alle optimalen Beweissysteme effektiv p-simulieren kann. Dann existiert also auch *ein* optimales Beweissystem welches dies leistet. □

3.4 Bekannte Implikationen, Offene Orakel

Satz 3.21. *Es gelten die in Abbildung 3.1 abgebildeten Implikationen und Äquivalenzen.*

Beweis. 1. $\mathsf{DisjNP} \Rightarrow \mathsf{CON}^N$ nach Köbler, Messner und Torán (2003).

2. $\mathsf{UP} \Rightarrow \mathsf{TAUT}$ nach Köbler, Messner und Torán (2003).

3. $\mathsf{CON}^N \Rightarrow \mathrm{NEE} \neq \mathrm{coNEE}$ nach Köbler, Messner und Torán (2003).

4. $\mathrm{NP} \cap \mathrm{coNP} \neq \mathrm{P} \Rightarrow \neq \mathsf{Q}' \Rightarrow \mathrm{NPMV_t} \not\subseteq_c \mathrm{TFNP} \Rightarrow \neq \mathsf{Q}$ nach Fenner u. a. (2003).

5. $\neg\mathsf{Q} \Rightarrow \exists$ NP-Relation die nicht auf Entscheidung reduzierbar ist, denn unter $\neg\mathsf{Q}$ gilt mit Satz 3.12 auch die Negation von 3.12(1), also eine NPTM

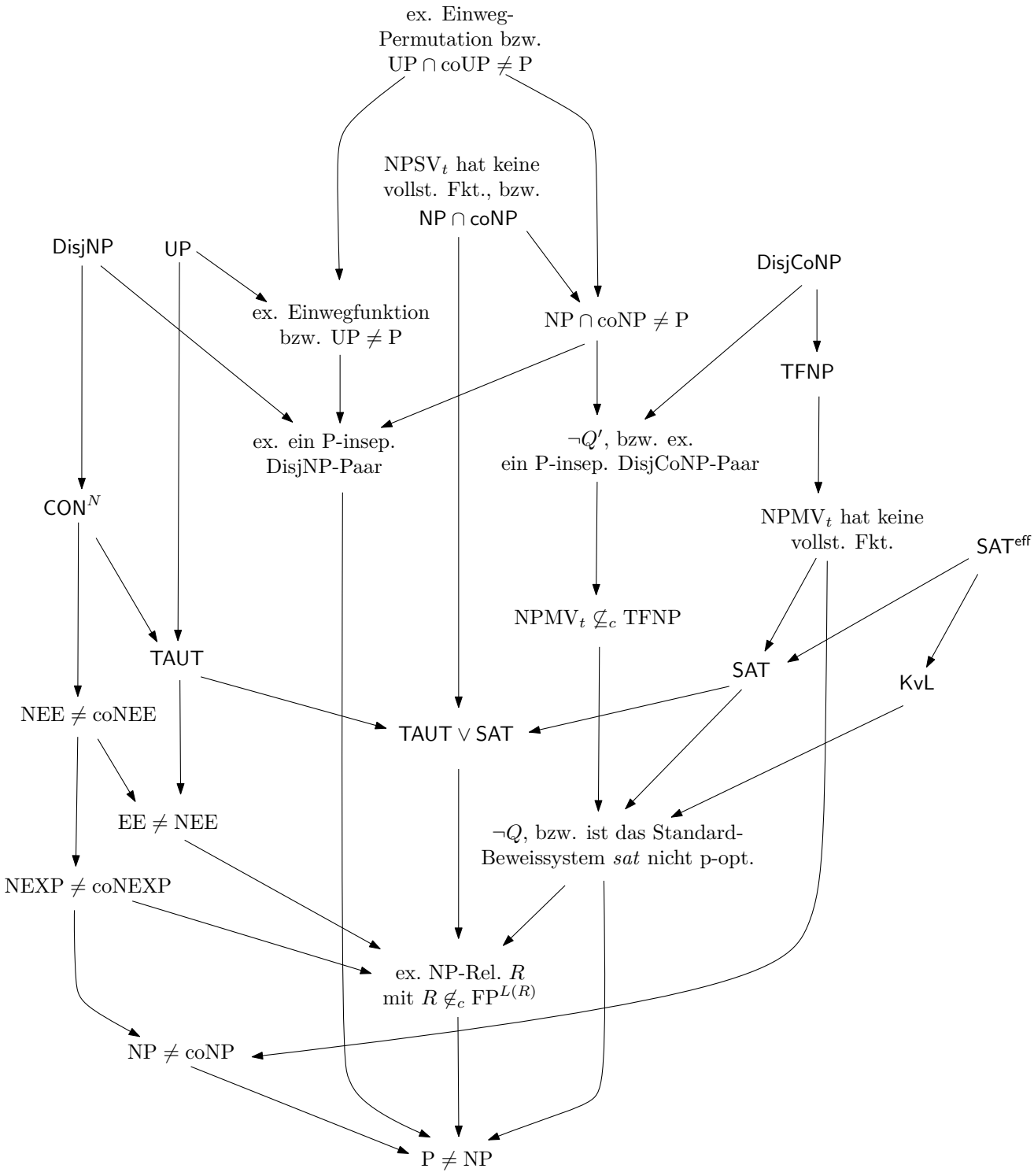

Abbildung 3.1: Bekannte (relativierenden) Implikationen zwischen den betrachteten Hypothesen und weiteren. Satz 3.21 gibt Belegstellen für jede dieser Implikationen an.

N mit $L(N) = \Sigma^*$ wobei keine Funktion $g \in \mathrm{FP}$ 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 α existiert. Nun gilt nach Vorigem auch $R \notin_c \mathrm{FP} = \mathrm{FP}^{\Sigma^*} = \mathrm{FP}^{L(R)}$.

6. EE $\neq$ NEE $\Rightarrow \exists$ NP-Relation die nicht auf Entscheidung reduzierbar ist, nach Bellare und Goldwasser (1994).

7. EXP $\neq$ NEXP $\Rightarrow \exists$ NP-Relation die nicht auf Entscheidung reduzierbar ist, nach Impagliazzo und Sudan (private Kommunikation berichtet von Bellare und Goldwasser 1994, Abschn. 1.5.4).

8. $\mathsf{NP} \cap \mathsf{coNP} \Rightarrow \mathsf{TAUT} \vee \mathsf{SAT}$ nach Beyersdorff, Köbler und Messner (2009).

9. NPMV_t hat keine vollständige Funktion $\Rightarrow \mathsf{SAT}$ nach Beyersdorff, Köbler und Messner (2009).

10. NPMV_t hat keine vollständige Funktion $\Rightarrow$ NP $\neq$ coNP nach Satz **??**.

11. $\mathsf{NP} \cap \mathsf{coNP} \Rightarrow \mathsf{TFNP} \Rightarrow \mathrm{NPMV}_\mathrm{t}$ hat keine vollständig Funktion, nach Pudlák (2017).

12. NP $\cap$ coNP $\neq$ P $\Rightarrow \exists$ P-inseparierbares DisjNP-Paar, denn wenn alle DisjNP-Paare P-separierbar, dann ist auch für jede Menge $L \in \mathrm{NP} \cap \mathrm{coNP}$ jeweils das DisjNP-Paar $(L, \overline{L})$ P-separierbar und damit $L \in \mathrm{P}$. □

Literatur

Agrawal, Manindra und Somenath Biswas. 1992. "Universal relations". In: *Proceedings of the Seventh Annual Structure in Complexity Theory Conference*. Seventh Annual Structure in Complexity Theory Conference. Juni 1992, S. 207–220. DOI: 10.1109/SCT.1992.215395.

Bellare, Mihir und Shafi Goldwasser. 1994. "The Complexity of Decision Versus Search". In: *SIAM Journal on Computing* 23.1 (Feb. 1994), S. 97–119. DOI: 10.1137/S0097539792228289.

Beyersdorff, Olaf, Johannes Köbler und Jochen Messner. 2009. "Nondeterministic functions and the existence of optimal proof systems". In: *Theoretical Computer Science* 410.38 (6. Sep. 2009), S. 3839–3855. DOI: 10.1016/j.tcs.2009.05.021.

Buhrman, H., J. Kadin und T. Thierauf. 1998. "Functions Computable with Nonadaptive Queries to NP". In: *Theory of Computing Systems* 31.1 (1. Feb. 1998), S. 77–92. DOI: 10.1007/s002240000079.

Fenner, Stephen A., Lance Fortnow, Ashish V. Naik und John D. Rogers. 2003. "Inverting onto functions". In: *Information and Computation* 186.1 (Okt. 2003), S. 90–103. DOI: 10.1016/S0890-5401(03)00119-6.

Fischer, Sophie, Lane Hemaspaandra und Leen Torenvliet. 1995. "Witness-isomorphic reductions and the local search problem". In: *Mathematical Foundations of Computer Science 1995*. Hrsg. von Jiří Wiedermann und Petr Hájek. Bd. 969. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, S. 277–287. DOI: 10.1007/3-540-60246-1_134.

Goldreich, Oded. 2008. *Computational Complexity: a Conceptual Perspective*. Cambridge: Cambridge University Press, 2008. 606 S. ISBN: 978-0-521-88473-0.

Köbler, Johannes, Jochen Messner und Jacobo Torán. 2003. "Optimal proof systems imply complete sets for promise classes". In: *Information and Computation* 184.1 (10. Juli 2003), S. 71–92. DOI: 10.1016/S0890-5401(03)00058-0.

Lynch, Nancy und Richard J. Lipton. 1978. "On Structure Preserving Reductions". In: *SIAM Journal on Computing* 7.2 (Mai 1978). Publisher: Society for Industrial and Applied Mathematics, S. 119–126. DOI: 10.1137/0207010.

Messner, Jochen. 2001. "On the simulation order of proof systems". Diss. University of Ulm, Germany, 2001.

Pudlák, Pavel. 2017. "Incompleteness in the finite domain". In: *The Bulletin of Symbolic Logic* 23.4 (2017), S. 405–441. DOI: 10.1017/bsl.2017.32.

Rothe, Jörg. 2008. *Komplexitätstheorie und Kryptologie: eine Einführung in Kryptokomplexität*. eXamen.Press. Berlin: Springer, 2008. ISBN: 978-3-540-79744-9.