20.01.2022

- NEU: Orakel O_2 mit $\mathsf{DisjNP}, \mathsf{DisjCoNP}$ und $\mathrm{UP} = \mathrm{P}$ (DisjNP ist dazugekommen). Damit analog zu DG20 ($\mathsf{DisjNP} \wedge \mathsf{NP} \cap \mathsf{coNP} \wedge \mathrm{UP} = \mathrm{P}$).
- NEU: Orakel O_3 mit $\mathsf{DisjCoNP}$ und alle DisjNP-Paare sind P-separierbar. Das übernimmt schon ziemlich viele Orakel, welche sich durch die Einführung der Hypothese *„existiert ein P-inseparierbares DisjNP-Paar“* ergeben. Beob. dass diese das symmetrische Analog zu $\neg Q'$ ist (*„… P-inseparierbares DisjCoNP-Paar“*.
- Eine Variante von Titus' Orakel zeigt $\mathrm{UP} \cap \mathrm{coUP} \neq \mathrm{P} \wedge \neg\mathsf{TAUT} \wedge \neg\mathsf{SAT}$. Das übernimmt alle Orakel, welche sich durch die Einführung der Hypothese $\mathrm{UP} \cap \mathrm{coUP} \neq \mathrm{P}$ ergeben.
- Damit verbleiben nur noch wenige offene Orakel übrig (grüne Pfeile). Alle anderen Orakel sind mindestens so stark wie $Q' \wedge \neg Q$ oder $\mathsf{NPMV}_t \wedge \mathsf{DisjCoNP}$.

Exposé zur Masterarbeit (Anton Ehrmanntraut)

Die Masterarbeit beschäftigt sich grob mit Suchproblemen und hierzu zugehörigen komplexitätstheoretischen Hypothesen. Dabei wird der Begriff „Suchprobleme“ bewusst weit gefasst, um die verschiedenen Konzeptionen aus der Komplexitätstheorie abzudecken, die Probleme detaillierter betrachten als reine Entscheidungsprobleme. Dies umfasst (intuitiv zu Suchproblemen am nächsten) die Klasse TFNP (Beame et al.), aber auch Funktionenklassen wie NPMV (Selman), und allgemein eine Perspektivierung über Levin-Reduktionen (im Gegensatz zu den üblichen Cook-Reduktionen). Hypothesen bezüglich deren Vollständigkeit, Inklusionen, etc., (das umfasst auch die Hypothese Q, Fenner et al.) haben große Nähe zu Hypothesen über Beweissysteme (Cook, Reckhow).

Im ersten Beitrag will die Masterarbeit daher einen Überblick und Systematisierung dieser unterschiedlichen Konzepte von Suchproblemen liefern. Ein Schwerpunkt liegt hierbei auf der Kategorisierung der Levin-Reduktion und weiteren Definitionen von Reduktionen, sowie die Verknüpfung zu Beweissystemen und der Hypothese Q.

Der zweite Beitrag vertieft den Zusammenhang der Hypothese Q, der Vollständigkeit von Suchproblemen, und Optimalität von Beweissystemen. Konkret ergänzt und erweitert die Arbeit damit die von Pudlák entwickelte Systematisierung, welche verschiedene Hypothesen um Komplexitätsklassen bzw. Beweissysteme in Beziehung setzt.

Aus dieser Erweiterung von Pudláks Systematisierung ergeben sich neue potentielle Implikationen zwischen den Hypothesen. Daher will die Masterarbeit, als dritter Beitrag, einige Orakelkonstruktionen erarbeiten, welche einige dieser (relativierbaren) Implikationen ausschließt. Damit schließt sich die Arbeit auch „Pudláks Programm“ an.

Inhalt Masterarbeit

1. **Einführung**

   - Einführung in das Thema: Suchprobleme als Berechnungsbrobleme; Gegenstand der algorithmischen Komplexitätstheorie
   - Formale Definition von Suchproblemen schon hier aufgreifen
   - Hier ggf. den didaktischen Ansatz von Goldreich nachzeichnen
   - Einordnung in die Geschichte des Themas: Suchprobleme werden nicht so oft diskutiert wie *Entscheidungsprobleme*. Gib die historische Gründe dafür an! Einfachere Konzeptualisierung; Suche reduziert sich zumindest bei NP-vollständigen Problemen auf Entscheidungen; für Probleme in „Bisektions-Form“ gilt das auch für NP-Intermediates; *Erkennung* von Mengen aus der Berechenbarkeitstheorie; Die P-NP-Frage kann sowohl in ihrer Entscheidungsvariante als auch in ihrer Funktionsvariante äquivalent formuliert werden
   - Problematisieren, warum das search-reduces-to-decision-Argument nicht ausreicht: z.B. weil linear (oder logarithmisch) viele Orakelfragen an das Entscheidungsproblem notwendig sind, anstelle *einer* Orakelfrage an ein vollständiges Suchproblem. Wenn man das Argument etwas schwammiger auslegt, sollte das sogar für NP-Intermediates gelten: mehrfaches Auswerten des speziellen Entscheidungsproblems *Hat n eine Faktor* $\leq k$ (ist in $\mathrm{NP} \cap \mathrm{coNP}$ und) erlaubt die effiziente Primfaktorzerlegung (im funktionalen Sinn). Das gilt aber nicht unbedingt wenn man *strikt* die Projektion einer NP-Relation meint, z.B. ist für *Gebe die Primfaktorzerlegung von n aus* die Projektion trivial (vgl. Santilli). Faktorisieren ist mutmaßlich nicht einmal nach unten selbstreduzierbar (vgl. Harsha et al.)!
   - Leitfragen: Was ist die Beziehung zwischen NP-Suchproblemen? Wie hängen Suchprobleme mit weiteren Objekten der Komplexitätstheorie zusammen?
   - Beobachtung: Vermutungen bezüglich Suchproblemen stehen in Beziehung zu Vermutungen bezüglich Beweissystemen bzw. Promise-Klassen. Diese werden im Pudlákschen Programm untersucht.
   - Kontextualisiere das Pudlák'sche Programm: gestartet als Untersuchung über fintistische Logik („Incompleteness in the finite domain“), was dann als Systematisierung zu Vollständigkeit von Promise-Klassen bzw. Optimalität von Beweissystemen bzw. Invertierbarkeit von Funktionen wurde. Ein Ziel von Pudlák: zeigen welche Implikationen gelten, welche Hypothesen unabhängig bzgl. relativierbaren Beweisen sind.
   - Beitrag: (a) Eine Übersicht über Reduzierbarkeitsbegriffe und Forschung zu Suchproblemen; (b) Verknüpfung von Suchproblemen mit Pudláks Hypothesen und der Hypothese Q, Erweiterung von Pudláks Systematisierung; (c) Orakelkonstruktionen, die mehrere Vermutungen voneinander trennen.

2. **Grundlagen**

   - Zweistellige Relationen und Funktionen
   - Notation von Wörtern und Mengen von Wörtern; implizite Ordnungs-Isomorphie zu den natürlichen Zahlen; implizite Listenkodierung; Indizierung von Zeichen in Wörtern
   - Maschinenmodell, insbesondere Orakel-Turing-Maschine; (nichtdeterministischer) Polynomialzeit-Transducer, …
   - Relativierung: Alle Aussagen relativieren sich, es sei denn, es ist anders angegeben.
   - Notation in Bezug auf Orakelkonstruktionen; partielle Orakel als Wörter, definite Berechnungen
   - Definition von Komplexitätsklassen, Reduzierbarkeiten zwischen Mengen, p-Isomorphie, Standardenummerierung von Maschinen, Reduzierbarkeit von Funktionen
   - Beweissysteme und Simulation

3. Zur Ordnung von Suchproblemen

3.1. Suchprobleme und Levin-Reduzierbarkeit

- Formale Definition angeben
- Bezug zur Funktions-Komplexitätstheorie: Relationen können als „partial multivalued functions“ verstanden werden, aus dieser Linse ist FNP identisch zu NPMV_g. An dieser Stelle auch TFNP definieren.
- Einige NP-Relationen angeben: rMATCHING ist z.B. effizient lösbar, rSAT, rVC ist genau dann effizient lösbar wenn P = NP, rFACTORING genau dann effizient lösbar wenn P = UP (und Projektion ist sogar Σ^* und damit trivial entscheidbar).
- Viele Beispiele durchgehen: z.B. ist eine NP-Relation R effizient lösbar genau dann wenn $R \in_c \text{FP}$; search reduces to decision für NP-Relationen R mit vollständigen Projektionen; allgemeiner: $R \in_c \text{FP}^L$ wenn L NP-vollständig ist.
- Noch einmal aufgreifen dass „search reduces to decision“ mutmaßlich nicht für rFACTORING gilt. Falls EE $\neq$ NEE oder EXP $\neq$ NEXP dann existiert eine Sprache $L \in \text{NP} - \text{P}$ sodass keine NP-Relation R mit $\text{Proj}(R) = R$ existiert für die $R \in \text{FP}^L$. (I.e., egal wie einfach die R-Beweise y für $x \in L$ sind, kann y nicht aus Queries an L beantwortet werden. Beachte dass eine NP-Relation für L immer existiert, ist ja $L \in \text{NP}$. Bellare, Goldwasser)
- Levin-Reduktionsbegriff einführen und motivieren
- Levin-Reduktion ordnet intuitiv nach „Schwierigkeit“ wie Karp-Reduktion: habe ich einen effizienten Algorithmus für A und $B \leq_{\text{L}}^{\text{p}} A$ dann habe ich auch für B einen effizienten Algorithmus; die effizient lösbaren Suchprobleme sind also nach unten abgeschlossen
- Damit lässt sich die P-NP-Frage auch als $\text{FNP} \subseteq_c \text{FP}$ formulieren.
- Levin-vollständige Relationen vorstellen: rSAT, rKAN, rVC
- Levin-vollständige Relationen verhalten sich wie Karp-vollständige Mengen: ist R Levin-vollständig, dann gilt $R \in_c \text{FP} \iff \text{FNP} \subseteq_c FP$; ist $R \leq_{\text{L}}^{\text{p}} Q$ dann ist auch Q Levin-vollständig
- Mit diesen Eigenschaften können die oben genannten Claims zu rSAT, rVC geklärt werden
- Fakt: die bekannten natürlichen Relationen, die zu den natürlichen NP-vollständigen Mengen korrespondieren, sind alle Levin-vollständig.
- Es gelten sogar weitere Eigenschaften: z.B. sind gewisse Suchprobleme $\leq_{\text{L},1,\text{inv}}^{\text{p}}$-vollständig. (Ob das für *alle* bekannten natürlichen Suchprobleme gilt, ist nicht erforscht.)
- Erste Fragen: Welche natürlichen NP-Relationen sind auch Levin-vollständig? Sind alle NP-Relationen mit vollständiger Projektion auch Levin-vollständig? Definiere die Hypothese KvL.

3.2. Reduzierbarkeiten von Suchproblemen und die gemeinsame Struktur von vollständigen Suchproblemen

- Motivation: Was ist der Forschungsstand zu NP-Relationen bzw. Suchproblemen allgemein?
- Die Frage Karp-vs-Levin-Vollständigkeit wurde dagegen mutmaßlich nicht so sehr untersucht. Keine Ahnung warum, bzw. auf die Einleitung hinweisen.
- Gibt dagegen einige interessante Forschungen zur search-vs-decision-Frage (unter NP-intermediate-Prolemen)
- Früh aufgegriffen: intuitives Gefühl dass in der Interreduzierbarkeit der NP-vollständigen Mengen mehr erhalten wird als eine alleinige „Equi-Lösbarkeit“
- Beispiel: p-Isomorphie der bekannten vollständigen Mengen; beob. wie für jede vollständigen zu SAT p-isomorphen Menge L eine Relation R existiert mit $\text{Proj}(R) = L$. Die Zertifikate von L haben dann aber einfach keine natürliche Form mehr.
- Simons beobachtet dass die natürlichen Suchprobleme „parsimonious“ sind
- Erste Versuche zur Verstärkung von Lynch und Liption: Menge der jeweiligen Zertifikate von x und $f(x)$ sind nicht nur gleichmächtig sondern auch in einer p-

berechenbaren 1-zu-1-Korrespondenz; Weise darauf hin dass diese Reduktion nicht effektiv ist, und z.B. unvergleichbar mit Levin-Reduktionen ist.
- Verfeinerung durch Fischer, Hemaspaandra, Torevliet: verlangen zusätzlich die p-Isomorphie zwischen den jeweiligen Mengen der Zertifikate; damit Zertifikats-Isomorphie stärker als „parsimonious"- und Levin-Reduktionen.
- Einen anderen Weg gingen Agrawal und Biswas: sind interessiert, wie die natürlichen vollständigen Probleme *strukturiert* sind. Die Intuition ist am verständlichsten wenn man sich in Erinnerung ruft wie übliche Beweise der NP-Vollständigkeit funktionieren. Eine übliche Strategie ist es, „Gadgets" der des betreffenden Problems zu definieren, und diese dann so zusammenzusetzen, dass SAT-Formeln simuliert werden können. Agrawal und Biswas formalisieren das als universelle Relatinen; genau jene Relationen die *joinable*, *coupable* und einen *building block* haben. Interessant: universelle Relationen sind nicht nur Levin-vollständig, sondern auch *projektiv* Levin-vollständig.
- Fasse zusammen wie die einzelnen Vollständigkeitsbegriffe zueinander stehen.
- „Gegenbeispiel" von Edward-Welsh einordnen: Chromatic Index universell aber nicht sparsam vollständig; vielleicht bisschen Lore
- Universelle Relationen als die wohl stärkste Eigenschaft, aber selbst hier gibt es keine Gegenbeispiele (NP-vollständiges Entscheidungsproblem aber Relation nicht universell.) Damit ist die Beobachtung *Graphisomprphismus keine universelle Relation* ein Indiz dass Graphisomorphismus nicht NP-vollständig ist.

4. Suchprobleme und die Hypothese Q im Kontext des Pudlákschen Programms

4.1. Hypothese Q vs. die Vollständigkeit von Suchproblemen

- Anstelle der Frage FNP $\subseteq_c$ FP können wir die Frage abschwächen und nur totale Suchprobleme betrachten: gilt TFNP $\subseteq_c$ FP? Definere TFNP.
- Fenner et al. verstehen diese Hypothese als die Hypothese Q und schaffen es, diese in ganz verschiedenen Darstellungsweisen zu charakterisieren (z.B. Invertierbarkeit von totalen Funktionen, Ausrechnen von akzeptierenden Rechenwegen, Ausrechnen von erfüllenden Belgungen gegeben akz. Rechenweg, usw.) Vielleicht hier schon die Aussagen zeigen.
- Messner kann das erweitern und Q als Frage zur p-Optimalität vom Standardbeweissystem für SAT charakterisieren. Definere das Standardbeweissystem.
- Hier schon mal den bisherigen Stand der Hypothese Q anschreiben

4.2. Karp-Vollständigkeit vs. Levin-Vollständigkeit

- Nachdem die Hypothese Q geklärt wurde, können wir die KvL-Hypothese vom vorigen Kapitel wieder aufgreifen.
- Es scheint schwierig, natürliche notwendige Bedingungen für KvL zu finden.
- Gehe den Widerspruchsbeweis-Versuch $\neg\mathsf{Q} \wedge \neg\mathsf{KvL} \Rightarrow \bot$ durch, und zeige, dass wir zumindest auf einen intuitiven Widerspruch kommen.
- Nimm das als Motivation, KvL über Beweissysteme zu definieren, und $\mathsf{SAT}^{\mathsf{eff}}$ als als eine stärkere Variante von SAT zu motivieren.
- Weise darauf hin, dass trotz der Ähnlichkeit zwischen $\neg\mathsf{KvL}$ und Q es nicht gelungen ist, KvL in anderen Formen (wie z.B. Inverterbarkeit von Funktionen) zu charakterisieren.

4.3. Generalisierung von Q auf allgemeine NP-Relationen

- Werde im Folgenden zeigen, dass das auch auf andere Suchprobleme (als nur SAT) generalisiert. Das ist gar nicht so klar, denn es werden Eigenschaften an das Suchproblem gestellt, die über Levin-Vollständigkeit hinausgehen: Levin-Paddability
- Zeige die zwei jeweiligen Generalisierungen separat mit ihren jeweiligen Voraussetzungen, um herauszuarbeiten welche zusätzlichen Annahmen genau gebraucht werden.
- Zeige dass Levin-Vollständigkeit mit -Paddability hinreichend für beide Generalisierungen ist.
- Müssen uns weiter fragen, für welche NP-Relationen diese obigen stärkereren Vor-

assetzungen gelten. Konkret: welche Levin-vollständigen Suchprobleme sind (nicht) paddalbe? Zeige die jeweiligen Ergebnisse
- Weise darauf hin, dass ein Gegenbeispiel (Levin-vollständig aber nicht paddable) nicht leicht zu finden ist, denn das wäre auch ein Gegenbeispiel einer Levin-vollständigen Relation, die nicht universell ist.

4.4. **Zusammenfassung der Ergebnisse zu Q, Bekannte Implikationen, Offene Orakel**

- Motiviere noch einmal diese Generalisierung mit dem Fakt, auf sichererem Weg mit Relativierungen umzugehen. Zeige z.B., dass die Relativierung von Dose bzgl. SAT genau richtig war, und ich hierzu Evidenz geliefert habe.
- Setze am Ende alle äquivalenten Charakterisierungen zusammen
- Weise auf die ∀-Charakterisierung hin. Damit sind bspw. entweder die Standardbeweissysteme *aller* vollständigen NP-Relationen p-optimal, oder *keine* der Standardbewissysteme vollständiger NP-Relationen p-optimal. Vielleicht aber auch nur skizzieren
- Ordne Q und KvL in den Pudlák-Baum ein.
- Zähle die offenen Orakel auf