Kohäsivität in Promise Problemen

Ulrike Brandt

Fachbereich Informatik

Technische Universität Darmstadt

Brandt@dekanat.informatik.tu-darmstadt.de

Hermann K.-G.Walter

Fachbereich Informatik

Technische Universität Darmstadt

hwalter@informatik.tu-darmsradt.de

Format 2013

Promise-Probleme

(1985 : S.Even, A.L.Selman and Y.Yacobi)

Verallgemeinerung von Entscheidungsproblemen.

Einschränkung der Instanzen auf zwei Sorten A, B

A - akzeptierend **B - verwerfend**

Keine Erwartungen für Instanzen $a \notin A \cup B$.

Entscheidungsproblem: B Komplement von A

Approximationsalgorithmen - Special Case-algorithmen

Differenziertes Bild der Komplexität von Problemen.

Vielfältige Anwendung z.B. bei Graphproblemen, Kryptografie

Ziel : Lösbarkeit bezüglich einer Mengen-/Sprachfamilie oder Komplexitätsklasse

Bedingungen für die Lösbarkeit bzw. Unlösbarkeit

Existenz und Eigenschaften von Unlösbarkeitskernen.

Vollständige Charakterisierung von Kernen durch Kohäsivität.

Kohäsivität in der Chomsky-hierarchie

Zusammenhänge zu immunen Mengen und Komplexitätskernen

Allgemeiner Ansatz

Gegeben (nichtendliche) Basismenge S, $\mathscr{S} \subseteq \mathbf{2}^{S}$. $A, B \subseteq S$, $A \cap B = \emptyset$.

(A, B) *Promise-Problem* für $\mathscr{S}$.

(A, B) *lösbar* für $\mathscr{S} \Leftrightarrow \exists\ Q, Q^c \in \mathscr{S}: A \subseteq Q\ \&\ B \subseteq Q^c \Leftrightarrow (A, B) \in$ ***promise***$(\mathscr{S})$

($Q^c = S \setminus Q$ Komplement in S!)

Anwendung : Chomsky-Hierarchie, Komplexitätsklassen (deterministische)

Methoden und Voraussetzungen : Mengen, boole'sche Operationen, Variation.

Sprachen, freies Monoid, Linkstranslation, Entscheidbarkeit.

Rekursionstheorie, effektive Aufzählungen.

Separations-Prinzip in der klassischen Rekursionstheorie, Immunität, Kohäsivität

- elementare Mengentheorie.

Beispiele

$S = X^*$, X endliches Alphabet, $\mathscr{L} \subseteq \mathbf{2}^{X^*}$. Chomsky-Hierarchie : $\mathscr{L}_{\mathbf{r.e.}}(X)$, $\mathscr{L}_{\mathbf{cs}}(X)$, $\mathscr{L}_{\mathbf{cf}}X)$, $\mathscr{L}_{\mathbf{reg}}(X)$.

Beipiel : $\mathscr{L}_{\mathbf{reg}}(X)$ mit $X = \{a, b\}$.

$A = \{a^n b^n \mid n > 0\}$, $B = \{a^n b^m \mid n, m > 0 \text{ and } n \neq m\}$, $A, B \in \mathscr{L}_{\mathbf{cf}}(X)$

$(A, B) \notin$ ***promise***$(\mathscr{L}_{\mathbf{reg}}(X))$ (Pumping Lemma),

$(A, B) \in$ ***promise***$(\mathscr{L}_{\mathbf{cf}}(X))$ ($A^c \in \mathscr{L}_{\mathbf{cf}}(X)$, A det.kontextfrei)

Einfache aber wichtige Fakten

(1) $\mathscr{S} = \mathscr{S}^{\mathbf{c}} \Rightarrow \{(A, B) \mid A \in \mathscr{S}, B \subseteq S, A \cap B = \emptyset\} \subseteq \boldsymbol{promise}(\mathscr{S})$.

$(\mathscr{S}^{\mathbf{co}} = \{A^{c} \mid A \in \mathscr{S}\}, \mathscr{S}^{\mathbf{c}} = \mathscr{S} \cup \mathscr{S}^{\mathbf{co}})$

(2) $\mathscr{S} \subseteq \mathscr{S}' \Rightarrow \boldsymbol{promise}(\mathscr{S}) \subseteq \boldsymbol{promise}(\mathscr{S}')$.

(3) $\boldsymbol{promise}(\mathscr{S}) = \boldsymbol{promise}(\mathscr{S}^{\mathbf{co}})$.

(4) $(A, B) \in \boldsymbol{promise}(\mathscr{S}) \Leftrightarrow (B, A) \in \boldsymbol{promise}(\mathscr{S})$.

(5) $A, B' \subseteq B : (A, B) \in \boldsymbol{promise}(\mathscr{S}) \Rightarrow (A, B') \in \boldsymbol{promise}(\mathscr{S})$.

(6) $\mathscr{S} = (\mathscr{S}^{\mathbf{u}})^{\mathbf{s}} \Rightarrow \forall A, B, B'$:

$(A, B) \in \boldsymbol{promise}(\mathscr{S})$ & $(A, B') \in \boldsymbol{promise}(\mathscr{S}) \Rightarrow (A, B \cup B') \in \boldsymbol{promise}(\mathscr{S})$.

$(\mathscr{S}^{\mathbf{u}} = \{A_1 \cup \ldots \cup A_n \mid n > 0, A_i \in \mathscr{S}\ (1 \leq i \leq n)\}, \mathscr{S}^{\mathbf{s}} = ((\mathscr{S}^{\mathbf{co}})^{\mathbf{u}})^{\mathbf{co}}.)$

(7) $(A, A^{c}) \in \boldsymbol{promise}(\mathscr{S}) \Leftrightarrow A \in \mathscr{S} \cap \mathscr{S}^{\mathbf{co}}$.

Variation

$\mathscr{S}_1 \oplus \mathscr{S}_2 = \{A \cup B \mid A \in \mathscr{S}_1 \;\&\; B \in \mathscr{S}_2\}$, $\mathscr{S}_1 \odot \mathscr{S}_2 = (\mathscr{S}_1^{\mathbf{co}} \oplus \mathscr{S}_2^{\mathbf{co}})^{\mathbf{co}}$, $\mathscr{S}_1 \ominus \mathscr{S}_2 = \mathscr{S}_1 \odot \mathscr{S}_2^{\mathbf{co}}$.

$\mathscr{S} \pm \mathscr{V} = \mathscr{S} \oplus \mathscr{V} \cup \mathscr{S} \ominus \mathscr{V}$. (*Variation* von $\mathscr{S}$ durch $\mathscr{V}$)

$\mathscr{S} \pm \mathscr{V} \subseteq \mathscr{S} \Rightarrow \forall\, C \in \mathscr{V}: (A, B) \in \textbf{\textit{promise}}(\mathscr{S}) \Rightarrow (A \cup C, B \cap C^c) \in \textbf{\textit{promise}}(\mathscr{S})$.

endliche Variation : $\mathscr{V} = \textbf{\textit{fin}}(S) = \{S' \subseteq S \mid S \text{ endlich}\}$.

Zwei Ergebnisse aus der Rekursivitätstheorie

Theorem : (*Separation Prinzip*) ($X \neq \emptyset$)

(1) $\exists\, A, B \in \mathscr{L}_{\mathbf{r.e.}}(X) : A \cap B = \emptyset$ und $(A, B) \notin \boldsymbol{promise}(\mathscr{L}_{\mathbf{r.e.}}(X))$.

(2) $\forall A, B \in \mathscr{L}_{\mathbf{r.e.}}(X)^{\mathbf{co}}, A \cap B = \emptyset : (A, B) \in \boldsymbol{promise}(\mathscr{L}_{\mathbf{r.e.}}(X)^{\mathbf{co}})$.

Kohäsivität

Definition : $A \subseteq S$, $A \notin \boldsymbol{fin}(S)$.

$$A\ \mathscr{S}\text{-}\mathit{kohäsiv} \Leftrightarrow \forall\, Q, Q^c \in \mathscr{S} : A \cap Q \in \boldsymbol{fin}(S) \textbf{ oder } A \cap Q^c \in \boldsymbol{fin}(S)$$

$$\Leftrightarrow \forall\, Q, Q^c \in \mathscr{S} : (A \cap Q \in \boldsymbol{fin}(S) \Leftrightarrow A \cap Q^c \notin \boldsymbol{fin}(S)).$$

$$\Leftrightarrow A \in \boldsymbol{cohesive}(\mathscr{S}).$$

Bemerkung : Definition aus der Rekursionstheorie ist equivalent zur $\mathscr{S}^{\mathbf{c}}$-Kohäsivität.

Beispiele : $X = \{a\}$.

(1) $L_{exp} = \{a^{2^n} \mid n > 0\} \notin \boldsymbol{cohesive}(\mathscr{L}_{\mathbf{reg}}(X))$. $((2^{2k} - 1)\ \boldsymbol{mod}\ 3 = 0$ und $(2^{2k+1} - 1)\ \boldsymbol{mod}\ 3 = 1)$

(2) $L_{fac} = \{a^{n!} \mid n > 0\} \in \boldsymbol{cohesive}(\mathscr{L}_{\mathbf{reg}}(X))$.

(Pumping-lemma für $\mathscr{L}_{\mathbf{reg}}(X)$, $\alpha x = y!$ ist lösbar für $y > \alpha \Rightarrow \forall\, R \in \mathscr{L}_{\mathbf{reg}}(X) \setminus \boldsymbol{fin}(a^*)$: $L_{fac} \setminus R \in \boldsymbol{fin}(a^*)$)

(Einfache) Fakten über Kohäsivität

(1) $\mathscr{S} \subseteq \mathscr{S}' \Rightarrow \textbf{\textit{cohesive}}(\mathscr{S}') \subseteq \textbf{\textit{cohesive}}(\mathscr{S})$.

(2) $A' \subseteq A$, $A \in \textbf{\textit{cohesive}}(\mathscr{S})$, $A' \notin \textbf{\textit{fin}}(S) \Rightarrow A' \in \textbf{\textit{cohesive}}(\mathscr{S})$.

(3) $\mathscr{S} \pm \textbf{\textit{fin}}(S) \subseteq \mathscr{S} \Rightarrow \textbf{\textit{cohesive}}(\mathscr{S}) \pm \textbf{\textit{fin}}(S) \subseteq \textbf{\textit{cohesive}}(\mathscr{S})$.

(4) $\textbf{\textit{cohesive}}(\mathscr{S}) = \textbf{\textit{cohesive}}(\mathscr{S}^{\mathbf{co}})$.

(5) $\mathscr{S} = \mathscr{S}^{\mathbf{c}} \Rightarrow \textbf{\textit{cohesive}}(\mathscr{S}) = \textbf{\textit{cohesive}}(\mathscr{S}^{\mathbf{b}})$.

($\mathscr{S}^{\mathbf{b}} = ((\mathscr{S}^{\mathbf{c}})^{\mathbf{s}})^{\mathbf{u}}$ (= boole'scher Abschluß))

(6) $\forall\ A, B \in \textbf{\textit{cohesive}}(\mathscr{S})$, $A \cap B \notin \textbf{\textit{fin}}(S) \Rightarrow A \cup B \in \textbf{\textit{cohesive}}(\mathscr{S})$.

Immunität

Definition : $A \notin \textit{fin}(S)$.

$A \in \textbf{\textit{immune}}(\mathscr{S}) \Leftrightarrow (\forall B \in \mathscr{S} : A \cap B^c \neq \emptyset)$.

Theorem : $\textit{fin}(S) \subseteq \mathscr{S}$, $\mathscr{S} \pm \textit{fin}(S) \subseteq \mathscr{S}$:

$A \notin \textit{fin}(S)$ & $A \in \textbf{\textit{cohesive}}(\mathscr{S}) \setminus \mathscr{S} \Rightarrow A \in \textbf{\textit{immune}}(\mathscr{S})$.

Bemerkung : $X^* \in \textit{cohesive}(\textit{fin}(S)^{\mathbf{c}})$

Beispiel : $X = \{a, b\}$.

- $\{a^n b^n | n > 0\} \notin \textbf{\textit{cohesive}}(\mathscr{L}_{\mathbf{reg}}(X))$ ($n = 2m$ und $n = 2m + 1$)
- $\{a^n b^n | n > 0\} \in \textbf{\textit{immune}}(\mathscr{L}_{\mathbf{reg}}(X))$ (pumping lemma für $\mathscr{L}_{\mathbf{reg}}(X)$)

Myhill-Dekker „Konstruktion“

Theorem von Myhill-Dekker : $\mathscr{S}$ abzählbar.

$$\forall\ A \subseteq S,\ A \notin \boldsymbol{fin}(S)\ \exists\ A' \subseteq A:\ A' \in \boldsymbol{cohesive}(\mathscr{S}).$$

Konstruktion : $\mathbf{e}_{\mathscr{S}}: \mathbb{N}_0 \to \mathbf{2}^S$, $\mathbf{e}_{\mathscr{S}}(\mathbb{N}_0) = \mathscr{S}$, $A \notin \boldsymbol{fin}(S)$.

$$A_0 := A,\ A_{n+1} := \ \underline{\mathbf{if}}\ A_n \cap \mathbf{e}_{\mathscr{S}}(n) \notin \boldsymbol{fin}(S)\ \underline{\mathbf{then}}\ A_n \cap \mathbf{e}_{\mathscr{S}}(n)\ \underline{\mathbf{else}}\ \ A_n \cap \mathbf{e}_{\mathscr{S}}(n)^c\ \ \underline{\mathbf{fi}}$$

- $A_{n+1} \subseteq A_n$ für alle $n \geq 0$.
- $A \notin \boldsymbol{cohesive}(\mathscr{S}) \ \Rightarrow\ A_n \notin \boldsymbol{cohesive}(\mathscr{S})$ (endliche Variation !)

$$\Rightarrow\ \exists\ g : \mathbb{N}_0 \to \mathbb{N}_0 :\ \forall\ n \geq 0 : A_{g(n+1)} \subset A_{g(n)} \text{ and } A_{g(n)} \subseteq A_n.$$

Wähle $a_n \in A_{g(n+1)} \setminus A_{g(n)}$ $(n \geq 0)$.

$$A' = \{a_n \mid n \geq 0\}$$

Markierungstechnik (Linkstranslation) - $\mathscr{L}_{\mathbf{ltr}}(X)$

S = X*, L, L' $\subseteq$ X*, L•L' (= LL') Komplexprodukt, Singletons {w} = w, |w| Wortlänge.

Definition : $\mathscr{L}^{\mathbf{ltr}} = \{wL \mid w \in X^*, L \in \mathscr{L}\}$.

$\mathscr{L} = \mathscr{L}^{\mathbf{ltr}}$ abgeschlossen gegen Linkstranslation

$\mathscr{L}_{\mathrm{ltr}}(X) = ((\boldsymbol{fin}(X^*)^{\mathbf{c}})^{\mathbf{ltr}})^{\mathbf{u}} = \{w_1L_1 \cup \ldots \cup w_kL_k \mid k < 0,\ w_i \in X^*,\ L_i \in \boldsymbol{fin}(X^*)^{\mathbf{c}},\ 1 \leq i \leq k\}$.

Definition : $\mathscr{L}$ <u>ltr-kürzbar</u> $\Leftrightarrow$ $(wL \in \mathscr{L} \Rightarrow L \in \mathscr{L})$.

Theorem : $\mathscr{L}_{\mathrm{ltr}}(X) = \mathscr{L}_{\mathrm{ltr}}(X)^{\mathbf{ltr}} = \mathscr{L}_{\mathrm{ltr}}(X)^{\mathbf{b}}$ ist ltr-kürzbar.

Anwendung : $\mathscr{L} = \mathscr{L}^{\mathbf{ltr}}$, $\mathscr{L} \pm \mathscr{L}_{\mathrm{ltr}}(X) \subseteq \mathscr{L}$, $\mathscr{L}$ ltr-kürzbar.

(1) $\forall\, L \in \mathscr{L}$, $w \in X^*$: $L \in$ ***cohesive***$(\mathscr{L}) \Leftrightarrow wL \in$ ***cohesive***$(\mathscr{L})$.

(2) $\forall\, L, L' \subseteq X^*$, $w \in X^*$: $(L, L') \in$ ***promise***$(\mathscr{L}) \Leftrightarrow (wL, wL') \in$ ***promise***$(\mathscr{L})$.

(3) $X = \{a, b\}$. $L \in$ ***cohesive***$(\mathscr{L})$, $\Rightarrow$ $aL, bL \in$ ***cohesive***$(\mathscr{L})$,

aber $aL \cup bL \notin$ ***cohesive***$(\mathscr{L})$.

Struktur kohäsiver Mengen

Definition : $f : \mathbb{N}_0 \to X^*$ *sequentiell* $\Leftrightarrow \forall\, n \geq 0 : |f(n)| = n$ and $f(n) \leq f(n + 1)(\mathbf{pref})$.

$(u \leq v(\mathbf{pref}) \Leftrightarrow v \in uX^*)$

Theorem : $\#(X) > 1$.

$L \in$ ***cohesive***$((\mathscr{L}_{\mathbf{ltr}}(X)) \Leftrightarrow$

$\exists\, f_L : \mathbb{N}_0 \to X^*$: f_L sequentiell & $\forall\, n \geq 0$: $L \setminus f_L(n)X^* \in$ ***fin***(X^*).

Beobachtung : $L \in$ ***cohesive***$((\mathscr{L}_{\mathbf{ltr}}(X))$, $wX^* \cap L \notin$ ***fin***(X^*) & $uX^* \cap L \notin$ ***fin***$(X^*) \Rightarrow w = u$.

Bemerkung : f_L ist eindeutig bestimmt. $L' \subseteq L \Rightarrow f_L = f_{L'}$.

Beispiel: $X = \{a, b\}$. uw^*v, $\{xu^nwv^ny \mid n \geq 0\} \in$ ***cohesive***$((\mathscr{L}_{\mathbf{ltr}}(X))$.

Chomskyhierarchie und Komplexitätsklassen

- $\boldsymbol{fin}(X^*) \subset \boldsymbol{fin}(X^*)^{\mathbf{c}} \subset \mathscr{L}_{\mathbf{ltr}}(X) \subset \mathscr{L}_{\mathbf{reg}}(X) \subset \mathscr{L}_{\mathbf{cf}}(X) \subset \mathscr{L}_{\mathbf{cs}}(X) \subset \mathscr{L}_{\mathbf{rec}}(X) \subset \mathscr{L}_{\mathbf{r.e.}}(X)$

  alle sind ltr-kürzbar, ab $\mathscr{L}_{\mathbf{ltr}}(X)$ abgeschlossen gegen Linkstranslation.

  Boole'sche algebren : $\boldsymbol{fin}(X^*)^{\mathbf{c}} \subset \mathscr{L}_{\mathbf{ltr}}(X) \subset \mathscr{L}_{\mathbf{reg}}(X) \subset \mathscr{L}_{\mathbf{cs}}(X) \subset \mathscr{L}_{\mathbf{rec}}(X)$.

- $X = \{a, b\}$. “Vernünftige” Komplexitätsklassen $\mathscr{C}$:

  $$\mathscr{L}_{\mathbf{ltr}}(X) \subseteq \mathscr{C} = \mathscr{C}^{\mathbf{ltr}},\ \mathscr{C} \pm \mathscr{L}_{\mathbf{ltr}}(X) \subseteq \mathscr{C},\ \mathscr{C} \text{ ltr-kürzbar}$$

  (zeit/platz-konstruierbare Ressourcen-schranken).

- $X = \{a\}$. $\boldsymbol{fin}(X^*)^{\mathbf{c}} = \mathscr{L}_{\mathbf{ltr}}(X) \subset \mathscr{L}_{\mathbf{reg}}(X) = \mathscr{L}_{\mathbf{cf}}(X)$.

- X bel.: $\boldsymbol{cohesive}(\boldsymbol{fin}(X^*)^{\mathbf{c}}) = \{L \subseteq X^* \mid L \notin \boldsymbol{fin}(X^*)\}$.

Kohäsive Mengen - Chomsky-hierarchie

Theorem von Friedberg : $\exists\, L \in \mathscr{L}_{\mathbf{r.e.}}(X) : A^{\mathbf{c}} \in \textbf{\textit{cohesive}}(\mathscr{L}_{\mathbf{r.e.}}(X)^{\mathbf{c}})$.

Fact : $L \in \textbf{\textit{cohesive}}(\mathscr{L}_{\mathbf{r.e.}}(X)) \Rightarrow L \notin \mathscr{L}_{\mathbf{r.e.}}(X)$.

$|L| = \{a^{|w|} \mid w \in L\}$, $\mathscr{L}_{\mathbf{lreg}}(X) = \{L \subseteq X^* \mid |L| \in \mathscr{L}_{\mathbf{reg}}(a)\}$. $\{a^n b^n a^n \mid n \geq 0\} \in \mathscr{L}_{\mathbf{lreg}}(\{a, b\})$.

Lemma : $L \in \mathscr{L}_{\mathbf{lreg}}(X) \setminus \textbf{\textit{fin}}(X^*) \Rightarrow L \notin \textbf{\textit{cohesive}}(\mathscr{L}_{\mathbf{reg}}(X))$.

Corollary : $L \in \mathscr{L}_{\mathbf{cf}}(X) \Rightarrow L \notin \textbf{\textit{cohesive}}(\mathscr{L}_{\mathbf{cf}}(X))$. $(\mathscr{L}_{\mathbf{reg}}(X) \subseteq \mathscr{L}_{\mathbf{cf}}(X) \subseteq \mathscr{L}_{\mathbf{lreg}}(X))$

Theorem : $L \in \mathscr{L}_{\mathbf{cf}}(X) \setminus \textbf{\textit{fin}}(X^*) \Rightarrow \exists\, L' \subseteq L\colon L' \in \textbf{\textit{cohesive}}(\mathscr{L}_{\mathbf{reg}}(X))$ &

$L' \in \mathscr{L}_{\mathbf{rec}}(X)$.

(Inspektion der Myhill-Dekker „Konstruktion“)

Lösbarkeit und Unlösbarkeit von Promise-Problemen

Lemma : $\mathscr{V} \subseteq \mathscr{S}$, $\mathscr{S} \pm \mathscr{V} \subseteq \mathscr{S}$, $\mathscr{V} = \mathscr{V}^{\mathbf{b}}$:

$$\forall\ A, B \in \mathscr{S} \setminus \textit{\textbf{fin}}(S),\ A, B \notin \textit{\textbf{cohesive}}(\mathscr{V})\ \exists\ Q \in \mathscr{V}:$$

$$(A \cap Q, B \cap Q^{\mathbf{c}}) \in \textit{\textbf{promise}}(\mathscr{S})\ \&\ A \cap Q, B \cap Q^{\mathbf{c}} \in \mathscr{S} \setminus \textit{\textbf{fin}}(S).$$

Definition : $\mathscr{S}(A) = \{B \subseteq S \mid B \subseteq A\ \&\ B \in \mathscr{S}\}$.

Lemma : $\mathscr{S} = \mathscr{S}^{\mathbf{c}}$, $\mathscr{S} \pm \textit{\textbf{fin}}(S) \subseteq \mathscr{S}$,

$$(A, B) \notin \textit{\textbf{promise}}(\mathscr{S}) \Leftrightarrow B^{\mathbf{c}} \in \textit{\textbf{immune}}(\mathscr{S}(A^{\mathbf{c}})^{\mathbf{c}}).$$

Kohäsive Promise-Probleme

Theorem : $\mathscr{S} \subseteq \mathbf{2}^{\mathrm{S}}$, $\mathscr{S} \pm \boldsymbol{\mathit{fin}}(\mathrm{S}) \subseteq \mathscr{S}$: $\mathrm{A} \cap \mathrm{B} = \emptyset$:

$\mathrm{A} \cup \mathrm{B} \in$ ***cohesive***$(\mathscr{S})$, A, B $\notin$ ***fin***(S) $\Leftrightarrow$ A, B $\in$ ***cohesive***$(\mathscr{S})$ & (A, B) $\notin$ ***promise***$(\mathscr{S})$.

Theorem : $\mathscr{S} \subseteq \mathbf{2}^{\mathrm{S}}$, $\mathscr{S} \pm \boldsymbol{\mathit{fin}}(\mathrm{S}) \subseteq \mathscr{S}$: A, B $\in$ ***cohesive***$(\mathscr{S})$

$\mathrm{A} \cup \mathrm{B} \in$ ***cohesive***$(\mathscr{S}) \Leftrightarrow$ (A \ B, B) $\notin$ ***promise***$(\mathscr{S})$ **oder** $\mathrm{A} \cap \mathrm{B} \notin$ ***fin***(S).

Kerne und kohäsive Mengen

Definition : $A \cap B = \emptyset$, $A, B \notin \boldsymbol{fin}(S)$.

(A, B) *Kern von* $\mathscr{S}$ $((A, B) \in \boldsymbol{core}(\mathscr{S})) \Leftrightarrow$

$\forall\ A' \subseteq A,\ B' \subseteq B,\ A', B' \notin \boldsymbol{fin}(S)\text{:}\ (A', B') \notin \boldsymbol{promise}(\mathscr{S}) \Leftrightarrow$

$\forall\ Q \in \mathscr{S} \cap \mathscr{S}^{\mathbf{c}}\text{: } ((A \cap Q) \notin \boldsymbol{fin}(S) \Leftrightarrow (B \cap Q^{\mathbf{c}}) \in \boldsymbol{fin}(S))\ \&$

$((B \cap Q) \notin \boldsymbol{fin}(S) \Leftrightarrow (A \cap Q^{\mathbf{c}}) \in \boldsymbol{fin}(S))$.

Charakterisierungssatz : $\mathscr{S} \pm \boldsymbol{fin}(S) \subseteq \mathscr{S}$, $A \cap B = \emptyset$, $A, B \notin \boldsymbol{fin}(S)$.

$(A, B) \in \boldsymbol{core}(\mathscr{S}) \Leftrightarrow A \cup B \in \boldsymbol{cohesive}(\mathscr{S})$.

Folgerungen aus dem Charakterisierungssatz

Folgerung 1 : $\mathscr{S} \pm \boldsymbol{fin}(\mathrm{S}) \subseteq \mathscr{S}$:

(1) $\mathscr{S} = \mathscr{S}^{\mathbf{c}} \Rightarrow \boldsymbol{core}(\mathscr{S}) = \boldsymbol{core}(\mathscr{S}^{\mathbf{b}})$.

(2) $\mathscr{S} \subseteq \mathscr{S}' \Rightarrow \boldsymbol{core}(\mathscr{S}') \subseteq \boldsymbol{core}(\mathscr{S})$.

Folgerung 2 : $\mathscr{L} = \mathscr{L}^{\mathbf{ltr}}$, $\mathscr{L}$ **ltr**-kürzbar, $\mathscr{L} \pm \mathscr{L}_{\mathbf{ltr}}(\mathrm{X}) \subseteq \mathscr{L}$:

$\boldsymbol{core}(\mathscr{L})$ ist **ltr**-kürzbar.

Transitivität

Lemma : $\mathscr{S} \pm \boldsymbol{fin}(S) \subseteq \mathscr{S}$, $A \cap B = A \cap C = B \cap C = \emptyset$:

(1) $B \in$ ***cohesive***$(\mathscr{S}) \Rightarrow$

$(A, B) \notin$ ***promise***$(\mathscr{S})$ und $(B, C) \notin$ ***promise***$(\mathscr{S}) \Rightarrow (A, C) \notin$ ***promise***$(\mathscr{S})$.

(2) $(A, B) \in$ ***core***$(\mathscr{S})$ & $(B, C) \in$ ***core***$(\mathscr{S}) \Rightarrow (A, C) \in$ ***core***$(\mathscr{S})$.

$(A \cup C \subseteq (A \cup B) \cup (B \cup C)$ und $(A \cup B) \cap (B \cup C) = B)$

Beispiel : $X = \{a, b\}$, $\mathscr{L} = \mathscr{L}^{\mathbf{ltr}}$, $\mathscr{L}$ **ltr**-kürzbar, $\mathscr{L} \pm \mathscr{L}_{\mathbf{ltr}}(X) \subseteq \mathscr{L}$: $A, A^{\mathbf{c}} \notin \mathscr{L}$.

$(aA, aA^{\mathbf{c}} \cup bA^{\mathbf{c}}), (aA^{\mathbf{c}} \cup bA^{\mathbf{c}}, bA) \notin$ ***promise***$(\mathscr{L})$, aber $(aA, bA) \in$ ***promise***$(\mathscr{L})$

Existenz von Kernen in Promise-Problemen

Hauptsatz : $\mathscr{S}$ abzählbar, $\mathscr{S}^{\mathbf{u}} = \mathscr{S} = \mathscr{S}^{\mathbf{s}}$, $\mathscr{S} \pm \mathit{fin}(S) \subseteq \mathscr{S}$:

$(A, B) \notin \boldsymbol{promise}(\mathscr{S}) \Rightarrow \exists\, A' \subseteq A,\ B' \subseteq B : (A', B') \in \boldsymbol{core}(\mathscr{S})$.

Example : $X = \{a, b, c\}$. $|w|_x$ = Anzahl der x in w.

$x \neq y \in X$: $L_{x,y} = \{w \in X^* \mid |w|_x \neq |w|_y\}$. $L_{x,y}$. $L_{x,y}{}^{\mathbf{c}} \in \mathscr{L}_{\mathbf{cf}}(X)$.

$L = L_{a,b} \cup L_{b,c} \cup L_{c,a}$, $L^{\mathbf{c}} = \{w \in X^* \mid |w|_a = |w|_b = |w|_c\} = L_{a,b}{}^{\mathbf{c}} \cap L_{b,c}{}^{\mathbf{c}} \cap L_{c,a}{}^{\mathbf{c}}$.

$L \in \mathscr{L}_{\mathbf{cf}}(X)$, $L^{\mathbf{c}} \notin \mathscr{L}_{\mathbf{cf}}(X)$, $L^{\mathbf{c}} \in \mathscr{L}_{\mathbf{cf}}(X)^{\mathbf{co}}$, $L^{\mathbf{c}} \in \mathscr{L}_{\mathbf{cf}}(X)^{\mathbf{s}}$.

$(L, L^{\mathbf{c}}) \notin \boldsymbol{promise}(\mathscr{L}_{\mathbf{cf}}(X))$, $(L, L^{\mathbf{c}}) \in \boldsymbol{promise}(\mathscr{L}_{\mathbf{cf}}(X)^{\mathbf{c}})$ and $(L, L^{\mathbf{c}}) \in \boldsymbol{promise}(\mathscr{L}_{\mathbf{cf}}(X)^{\mathbf{s}})$.

$(L, L^{\mathbf{c}})$ besitzt keinen Kern

Beweis mit einer Nachbildung der Myhill-Dekker Konstruktion

$$\mathbf{e}_{\mathscr{S}} : \mathbb{N}_0 \to \mathbf{2}^S,\ \mathbf{e}_{\mathscr{S}}(\mathbb{N}_0) = \mathscr{S}.$$

$$(A_0, B_0) := (A, B)\ (\notin \textit{promise}(\mathscr{S}))$$

$$(A_{n+1}, B_{n+1}) := \underline{\mathbf{if}}\ (A_n \cap \mathbf{e}_{\mathscr{S}}(n), B_n \cap \mathbf{e}_{\mathscr{S}}(n)) \notin \textit{promise}(\mathscr{S})\ \underline{\mathbf{then}}\ (A_n \cap \mathbf{e}_{\mathscr{S}}(n), B_n \cap \mathbf{e}_{\mathscr{S}}(n))$$

$$\underline{\mathbf{else}}\ (A_n \cap \mathbf{e}_{\mathscr{S}}(n)^{\mathbf{c}}, B_n \cap \mathbf{e}_{\mathscr{S}}(n)^{\mathbf{c}})\ \underline{\mathbf{fi}}$$

Dann gilt : $\exists\, g : \mathbb{N}_0 \to \mathbb{N}_0 :\ \forall\, n \geq 0 : A_{g(n+1)} \subset A_{g(n)},\ A_{g(n)} \subseteq A_n$ und $B_{g(n+1)} \subset B_{g(n)}$ and $B_{g(n)} \subseteq B_n$.

Wähle $a_n \in A_{g(n+1)} \setminus A_{g(n)}$ und $b_n \in B_{g(n+1)} \setminus B_{g(n)}$ $(n \geq 0)$.

$$\mathbf{A' = \{a_n \mid n \geq 0\},\ B' = \{b_n \mid n \geq 0\}}$$

Lemma : $A \cap B = \emptyset$, $(A, B) \notin \textit{promise}(\mathscr{S})$.

$\forall\ Q, Q^{\mathbf{c}} \in \mathscr{S} : (A \cap Q, B \cap Q) \notin \textit{promise}(\mathscr{S})$ **or** $(A \cap Q^{\mathbf{c}}, B \cap Q^{\mathbf{c}}) \notin \textit{promise}(\mathscr{S})$.

Folgerung 1 : $\mathscr{S}$ abzählbar, $\mathscr{S}^{\mathbf{u}} = \mathscr{S} = \mathscr{S}^{\mathbf{s}}$, $\mathscr{S} \pm \boldsymbol{fin}(S) \subseteq \mathscr{S}$:

$A \cap B = \emptyset$, $(A, B) \notin \boldsymbol{promise}(\mathscr{S})$

$\exists\, B' \subseteq B, B' \notin \boldsymbol{fin}(S)\ \forall\, B'' \subseteq B', B'' \notin \boldsymbol{fin}(S)$: $(A, B'') \notin \boldsymbol{promise}(\mathscr{S})$.

($\Leftrightarrow B' \in \boldsymbol{core}(A, \mathscr{S})$!)

Folgerung 2 : $\mathscr{S}$ abzählbar, $\mathscr{S}^{\mathbf{u}} = \mathscr{S} = \mathscr{S}^{\mathbf{s}}$, $\mathscr{S} \pm \boldsymbol{fin}(S) \subseteq \mathscr{S}$,

$\forall\, A \cap B = A \cap C = B \cap C = \emptyset$, $B \in \boldsymbol{cohesive}(\mathscr{S}) \Rightarrow$

$(A, B) \notin \boldsymbol{promise}(\mathscr{S})$ und $(B, C) \notin \boldsymbol{promise}(\mathscr{S}) \Rightarrow (A, C) \notin \boldsymbol{promise}(\mathscr{S})$.

Beispiel : $X = \{a, b\}$, $\mathscr{L}_{\mathbf{ltr}}(X) \subseteq \mathscr{L}$ ltr-regulär, $\mathscr{L} \pm \mathscr{L}_{\mathbf{ltr}}(X) \subseteq \mathscr{L}$: $A, A^{\mathbf{c}} \notin \mathscr{L}$.

$(aA, aA^{\mathbf{c}} \cup bA^{\mathbf{c}})$, $(aA^{\mathbf{c}} \cup bA^{\mathbf{c}}, bA) \notin \boldsymbol{promise}(\mathscr{L})$, aber $(aA, bA) \in \boldsymbol{promise}(\mathscr{L})$

Komplexitätskerne („Hard Cores“) (Book-Du 1987)

Definition :

- B $\mathscr{S}$-*hardcore* von A $\Leftrightarrow$ (B $\notin$ ***fin***(S) & $\forall$ C $\in \mathscr{S}$(A) : B $\cap$ C $\in$ ***fin***(S)).
- B $\subseteq$ A : B *echter* $\mathscr{S}$-hardcore von A.

Theorem: $\mathscr{C}$ abzählbar, A $\notin$ ***fin***(S).

$\exists$ B $\subseteq$ A, B $\mathscr{C}$-hardcore von A $\Leftrightarrow$ A $\notin \mathscr{S}^{\mathbf{u}} \oplus$ ***fin***(S).

Theorem : ***fin***(S) $\subseteq \mathscr{C} = \mathscr{C}^{\mathbf{u}}$, $\mathscr{C} \pm$ ***fin***(S) $\subseteq \mathscr{C}$, $\mathscr{C}$ *recursiv aufzählbar* (Wortproblem):

$\forall$ L $\in \mathscr{L}_{\mathbf{rec}}$(X) \ $\mathscr{C}$ $\exists$ L' $\subseteq$ L, L' $\mathscr{S}$-hardcore von L: L' $\in \mathscr{L}_{\mathbf{rec}}$(X).

.

Komplexitätskerne und Unlösbarkeitskerne

Lemma : $\mathscr{S} = \mathscr{S}^{\mathbf{c}}$: B $\in$ ***core***(A, $\mathscr{S}$) $\Leftrightarrow$ B echter $\mathscr{L}$-hardcore von $A^{\mathbf{c}}$.

Theorem : $\mathscr{C}$ recursiv aufzählbar, Ø, X* $\in \mathscr{C} = \mathscr{C}^{\mathbf{b}}$:

$\forall\, L^{\mathbf{c}} \in \mathscr{L}_{\mathbf{rec}}(X) \setminus \mathscr{L} \Rightarrow$ ***core***(L, $\mathscr{C}$) $\cap\ \mathscr{L}_{\mathbf{rec}}(X) \neq$ Ø.

Ausblick und weitere Resultate

1. Verallgemeinerung auf Vektoren $(A_1, \dots , A_n)$ mit $A_i \cap A_j = \emptyset$ $(1 \leq i \neq j \leq n)$.

Lösung : $(Q_1, \dots , Q_n)$, $A_i \subseteq Q_i$, $Q_i \in \mathscr{S}$, $Q_i \cap Q_j = \emptyset$ $(1 \leq i \neq j \leq n)$, $Q_1 \cup \dots \cup Q_n = S$.

2. Unlösbarkeitskerne sind gegeben durch (nichttriviale) Partitionen $(B_1, \dots , B_n)$ $\mathscr{S}$-kohäsiver Mengen $A \subseteq S$ (Brandt !).

3. Für $n \geq 3$ gibt es nichtlösbare Promise-Probleme, die keinen Unlösbarkeitskern besitzen. (M.Ziegler !)

4. Problemfeld : Für $n \geq 3$ charakterisiere die nach 3. existierenden nichtlösbaren Promise-Probleme, die keinen Unlösbarkeitskern besitzen.

5. Verbesserung der Konstruktion kohäsiver Mengen, um weitere Eigenschaften sicher zu stellen. (“bi-kohäsive“ Mengen, Dovetailing mit „billigem“ Friedberg-clerk)

6. Reduktionstheorie - Reduktionsprinzip - Dekompositionen ?