Disjunkte NP-Paare und aussagenlogische Beweissysteme

Olaf Beyersdorff

Institut für Informatik
Humboldt-Universität zu Berlin

Gliederung

NP-Paare
- Separierbare Paare
- Kryptografische Paare
- Reduktionen zwischen Paaren

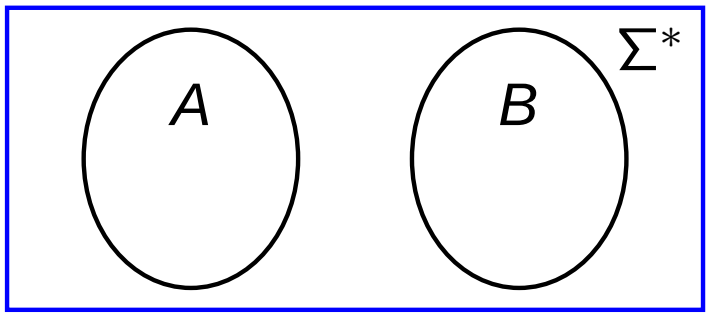
Beweissysteme
- Extended Frege *EF*
- Simulationen

NP-Paare und Beweissysteme
- Kanonische Paare
- Interpolationspaare
- Repräsentationen von Paaren
- Die Komplexitätsklasse DNPP(P)
- Vollständige Paare

Disjunkte NP-Paare

Definition (Grollmann, Selman 88)

(A, B) heißt disjunktes NP-Paar (DNPP), falls $A, B \in \text{NP}$ und $A \cap B = \emptyset$.



Beispiel

Clique-Colouring-Paar (CC_0, CC_1)

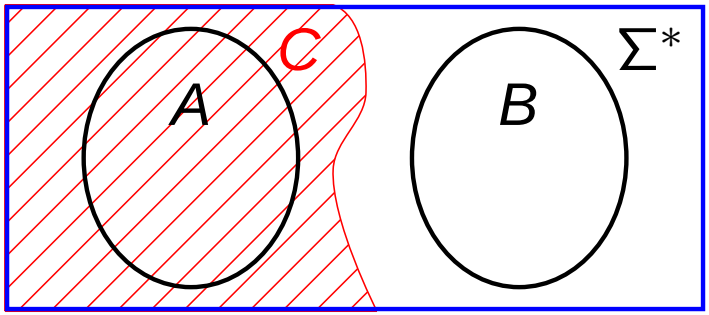
$CC_0 = \{(G, k) \mid G \text{ enthält eine Clique der Größe } k\}$

$CC_1 = \{(G, k) \mid G \text{ ist } k-1 \text{ färbbar }\}$

Separierbare Paare

Definition (Grollmann, Selman 88)

(A,B) heißt p-separierbar, falls eine Menge $C \in P$ mit $A \subseteq C$ und $B \cap C = \emptyset$ existiert.

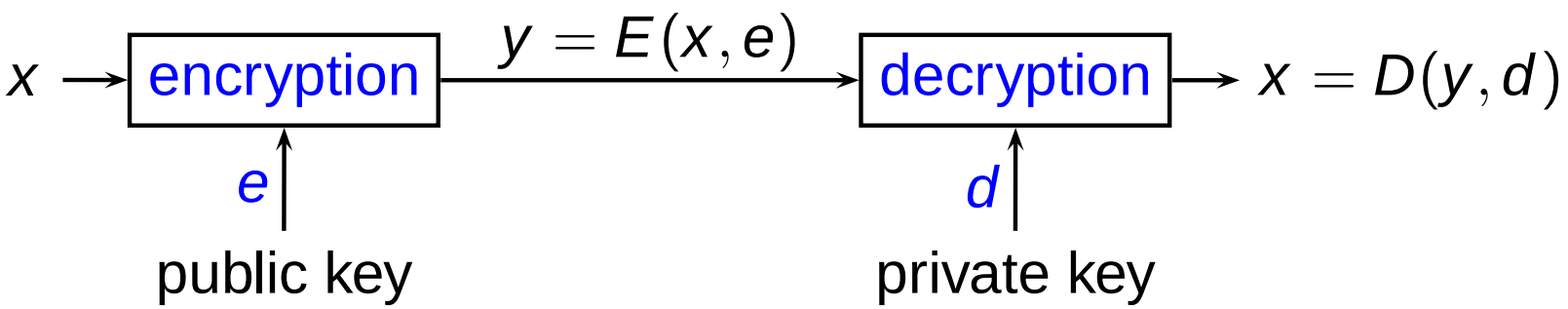


Theorem (Lovász 79)

Das Clique-Colouring-Paar ist p-separierbar.

Kryptografische Paare

Ein Public-Key-System $\mathcal{P} = (E, D)$



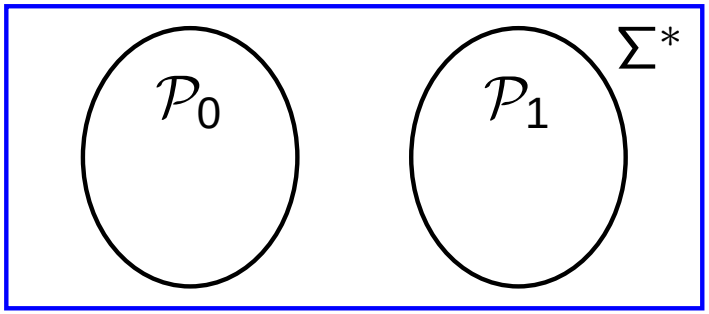
Beispiel (Grollmann, Selman 88)

Einem Public-Key-Kryptosystem $\mathcal{P} = (E, D)$ wird das NP-Paar $(\mathcal{P}_0, \mathcal{P}_1)$ zugeordnet, wobei

$$\mathcal{P}_0 = \{(e, y, i) \mid \quad e \text{ ist öffentlicher Schlüssel}, \; \exists x \, E(x, e) = y, \text{ das } i\text{-te Bit von } x \text{ ist } 0\}$$
$$\mathcal{P}_1 = \{(e, y, i) \mid \quad \ldots \quad \text{ist } 1\}.$$

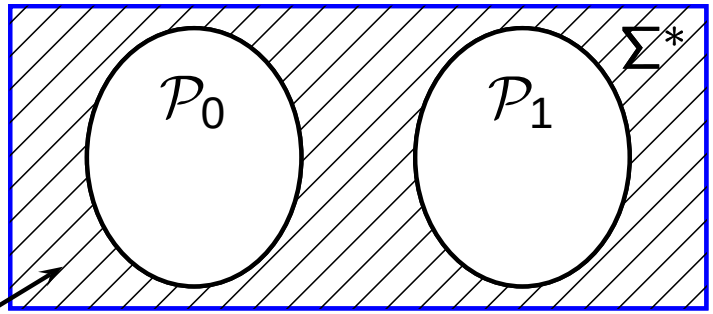
Sicherheit von Kryptosystemen

$$\mathcal{P}_0 = \{(e, y, i) \mid \quad e \text{ ist öffentlicher Schlüssel,}$$
$$\exists x\, E(x, e) = y, \text{ das } i\text{-te Bit von } x \text{ ist } 0\}$$



Sicherheit von Kryptosystemen

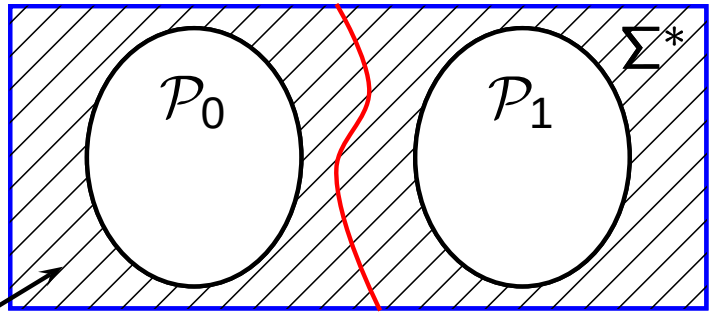
$$\mathcal{P}_0 = \{(e, y, i) \mid \begin{array}{l} e \text{ ist öffentlicher Schlüssel,} \\ \exists x\, E(x, e) = y, \text{ das } i\text{-te Bit von } x \text{ ist } 0\} \end{array}$$



$$\overline{\mathcal{P}_0 \cup \mathcal{P}_1} = \{(y, e, i) \mid e \text{ ist kein gültiger öffentlicher Schlüssel}\}$$

Sicherheit von Kryptosystemen

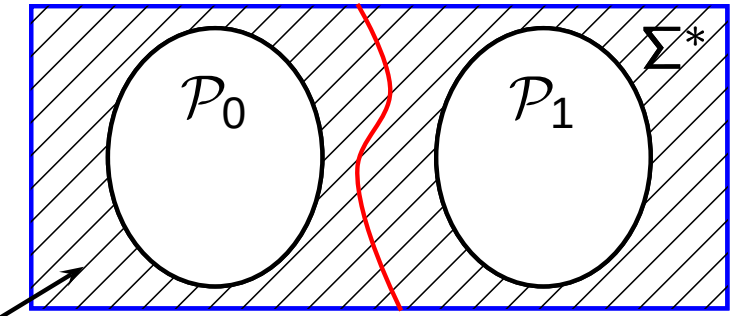
$$\mathcal{P}_0 = \{(e, y, i) \mid \begin{array}{l} e \text{ ist öffentlicher Schlüssel,} \\ \exists x\, E(x, e) = y, \text{ das } i\text{-te Bit von } x \text{ ist } 0\} \end{array}$$



$$\overline{\mathcal{P}_0 \cup \mathcal{P}_1} = \{(y, e, i) \mid e \text{ ist kein gültiger öffentlicher Schlüssel}\}$$

Sicherheit von Kryptosystemen

$$\mathcal{P}_0 = \{(e, y, i) \mid \begin{array}{l} e \text{ ist öffentlicher Schlüssel,} \\ \exists x\, E(x, e) = y, \text{ das } i\text{-te Bit von } x \text{ ist } 0\} \end{array}$$



$$\overline{\mathcal{P}_0 \cup \mathcal{P}_1} = \{(y, e, i) \mid e \text{ ist kein gültiger öffentlicher Schlüssel}\}$$

Theorem (Grollmann, Selman 88)

Falls das Kryptosystem $\mathcal{P}$ sicher ist, so ist $(\mathcal{P}_0, \mathcal{P}_1)$ nicht p-separierbar.

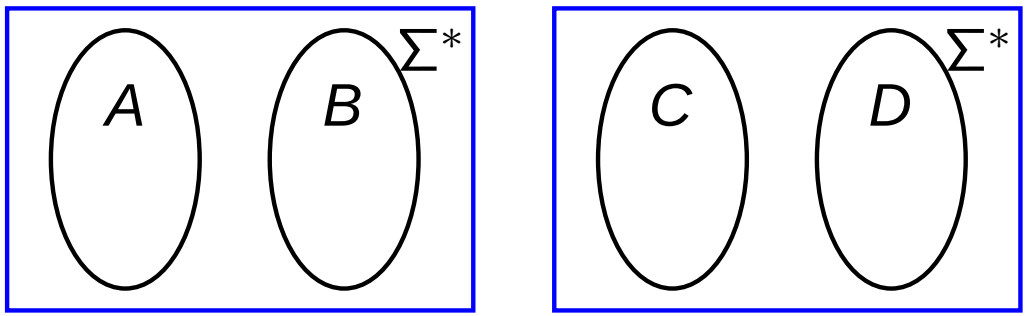
Anwendungen und Querbezüge

- Sicherheit von Public-Key-Kryptosystemen
  [Grollmann, Selman 88], [Homer, Selman 92]
- Charakterisierung von Eigenschaften aussagenlogischer Beweissysteme
  [Bonet, Pitassi, Raz 00], [Pudlák 03]
- untere Schranken für die Beweislänge in aussagenlogischen Beweissystemen
  [Razborov 96], [Pudlák 97], [Krajíček 04]
- beschränkte Arithmetik
  [Razborov 94], [Krajíček, Pudlák 98]
- vollständige Probleme für Promise-Klassen
  [Köbler, Messner, Torán 03],
  [Glaßer, Selman, Sengupta, Zhang 04]

Reduktionen zwischen Paaren

Definition (Grollmann, Selman 88)

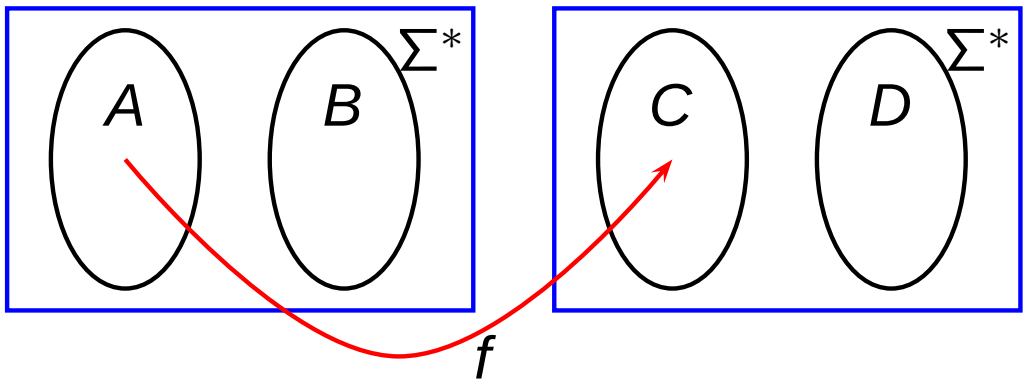
$(A, B) \leq_p (C, D) \overset{df}{\iff}$ es existiert eine in Polynomialzeit berechenbare Funktion f mit $f(A) \subseteq C$ und $f(B) \subseteq D$.



Reduktionen zwischen Paaren

Definition (Grollmann, Selman 88)

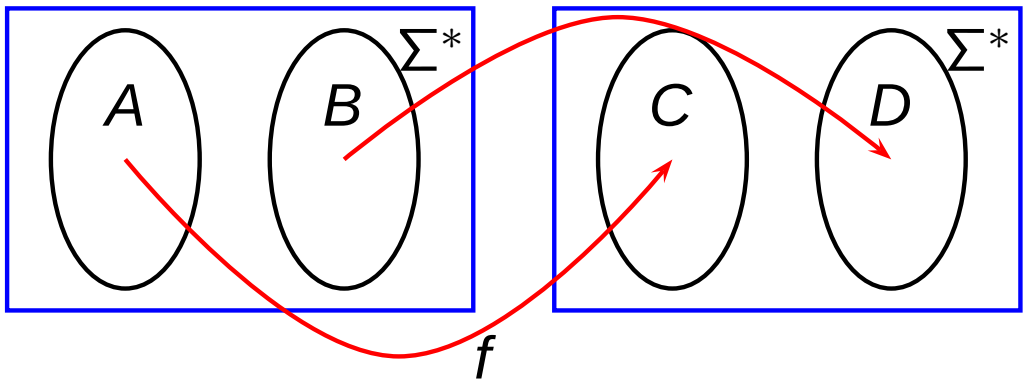
$(A,B) \leq_p (C,D) \overset{df}{\iff}$ es existiert eine in Polynomialzeit berechenbare Funktion f mit $f(A) \subseteq C$ und $f(B) \subseteq D$.



Reduktionen zwischen Paaren

Definition (Grollmann, Selman 88)

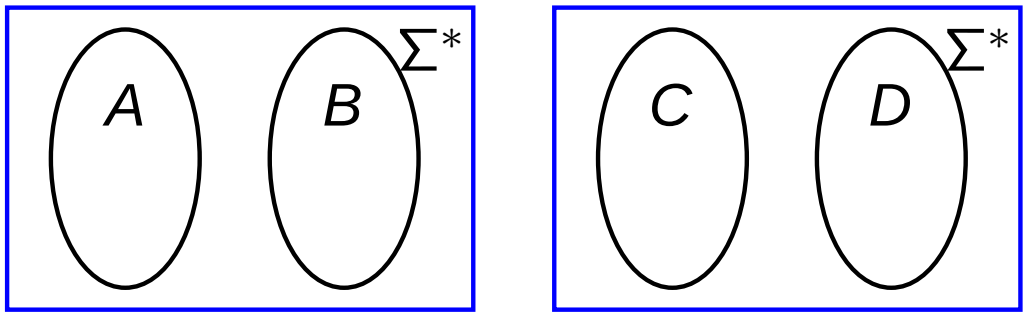
$(A,B) \leq_p (C,D) \overset{df}{\iff}$ es existiert eine in Polynomialzeit berechenbare Funktion f mit $f(A) \subseteq C$ und $f(B) \subseteq D$.



Eine starke Reduktion zwischen Paaren

Definition (Köbler, Messner, Torán 03)

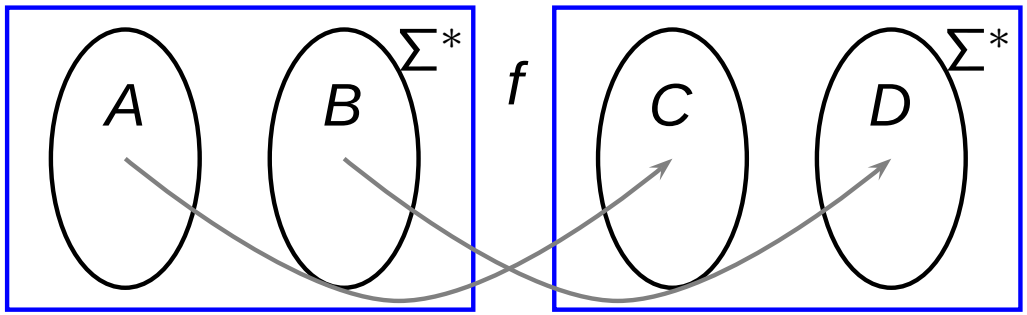
$(A, B) \leq_s (C, D) \overset{df}{\iff}$ es existiert eine in Polynomialzeit berechenbare Funktion f mit $f : A \leq_m^p C$ und $f : B \leq_m^p D$.



Eine starke Reduktion zwischen Paaren

Definition (Köbler, Messner, Torán 03)

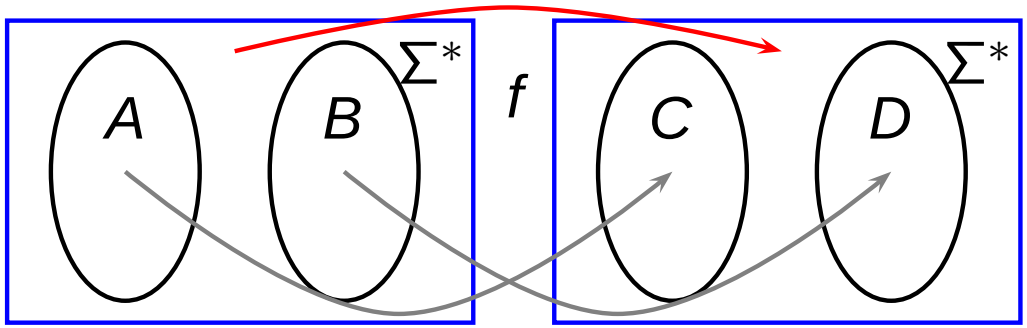
$(A, B) \leq_s (C, D) \overset{df}{\iff}$ es existiert eine in Polynomialzeit berechenbare Funktion f mit $f : A \leq_m^p C$ und $f : B \leq_m^p D$.



Eine starke Reduktion zwischen Paaren

Definition (Köbler, Messner, Torán 03)

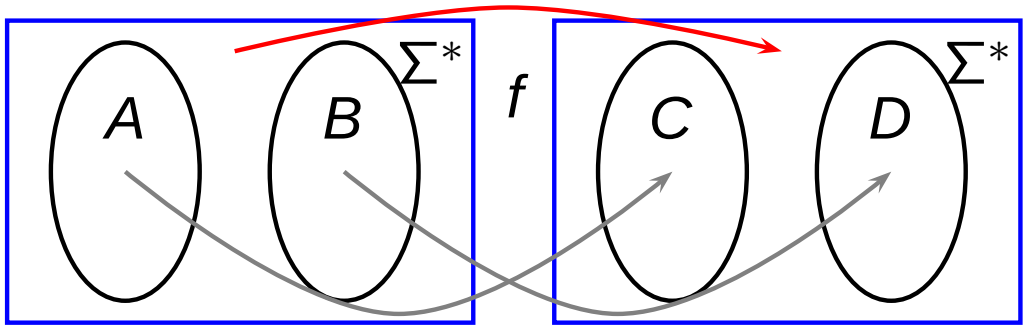
$(A, B) \leq_s (C, D) \overset{df}{\iff}$ es existiert eine in Polynomialzeit berechenbare Funktion f mit $f : A \leq_m^p C$ und $f : B \leq_m^p D$.



Eine starke Reduktion zwischen Paaren

Definition (Köbler, Messner, Torán 03)

$(A, B) \leq_s (C, D) \overset{df}{\iff}$ es existiert eine in Polynomialzeit berechenbare Funktion f mit $f : A \leq_m^p C$ und $f : B \leq_m^p D$.



Theorem (Glaßer, Selman, Sengupta 04)

Die Reduktion $\leq_s$ ist genau dann eine echte Verfeinerung von $\leq_p$, wenn P $\neq$ NP.

Zwei wichtige offene Probleme

Problem (Grollmann, Selman 88)

Gibt es nicht p-separierbare NP-Paare?

Antwort

Ja, falls $\mathrm{P} \neq \mathrm{NP} \cap \mathrm{coNP}$*.*

Kandidaten

- kryptografische Paare [Grollmann, Selman 88]
- Paare zu aussagenlogischen Beweissystemen [Krajíček, Pudlák 98]

Problem (Razborov 94)

Gibt es NP-Paare, die vollständig für die Klasse aller DNPP sind?

Aussagenlogische Beweissysteme

Definition (Cook, Reckhow 79)

- Ein aussagenlogisches Beweissystem ist eine in Polynomialzeit berechenbare Funktion P mit $rng(P) = TAUT$.
- Ist $P(\pi) = \varphi$, so heißt π P-Beweis von φ.
- $P \vdash_{\leq m} \varphi \overset{df}{\iff}$ es gibt einen P-Beweis von φ der Länge $\leq m$.

Motivation

Beweise sind effizient überprüfbar.

Beispiele

Wahrheitstafelmethode, Resolution, Frege-Systeme

Frege-Systeme

Extended Frege *EF*

- Axiomenschemata: $\varphi \to \varphi, \quad \varphi \to \varphi \vee \psi, \quad \ldots$
- Schlussregeln: $\dfrac{\varphi \quad \varphi \to \psi}{\psi}$ (Modus Ponens)
- Abkürzungen für lange Formeln: $p \leftrightarrow \varphi$

Erweiterungen von *EF*

Sei $\Phi \subseteq \mathit{TAUT}$ in Polynomialzeit entscheidbar.

- $\mathit{EF} \cup \Phi$: Φ als neue Axiome
- $\mathit{EF} + \Phi$: Φ als Axiomenschemata

Simulationen zwischen Beweissystemen

Definition (Cook, Reckhow 79)

Ein Beweissystem Q simuliert ein Beweissystem P ($P \leq Q$), falls Q-Beweise höchstens polynomiell länger als P-Beweise sind.

Theorem (Krajíček, Pudlák 89)

Für alle Beweissysteme P gilt: $P \leq EF + RFN(P)$.

Reflektionsprinzip:
$RFN(P) = (\forall \pi)(\forall \varphi) Prf_P(\pi, \varphi) \rightarrow Taut(\varphi)$

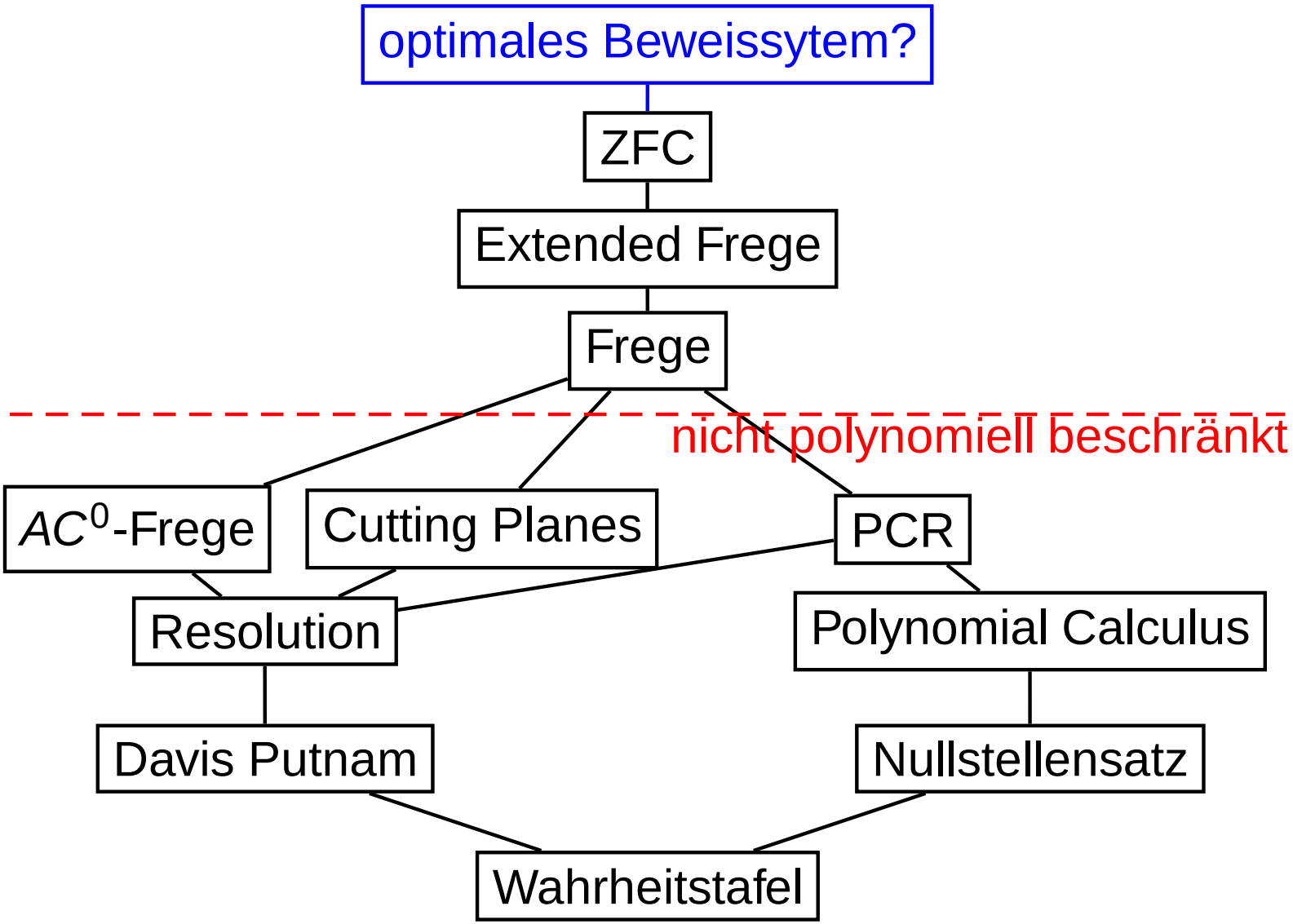
Definition

P heißt optimal, falls P alle Beweissysteme simuliert.

Problem (Krajíček, Pudlák 89)

Gibt es optimale Beweissysteme?

Die Simulationsordnung wichtiger Beweissysteme



Kanonische Paare

Definition (Razborov 94)

Einem Beweissystem P ordnen wir ein kanonisches Paar zu:

$$\begin{aligned} Ref(P) &= \{(\varphi, 1^m) \mid P \vdash_{\leq m} \varphi\} \\ Sat^* &= \{(\varphi, 1^m) \mid \neg\varphi \text{ ist erfüllbar}\} \end{aligned}$$

Anwendungen

Das kanonische Paar charakterisiert die

- Automatisierbarkeit von P [Pudlák 03] (Automatisches Theorembeweisen)
- Reflektionseigenschaft von P

Das Interpolationspaar

Definition (Pudlák 03)

Das Interpolationspaar eines Beweissystems P ist

$$
\begin{aligned}
I_1(P) &= \{(\varphi, \psi, \pi) \mid \varphi, \psi \text{ haben keine gem. Variablen,} \\
&\qquad P(\pi) = \varphi \vee \psi \text{ und } \neg\varphi \in SAT\} \\
I_2(P) &= \{(\varphi, \psi, \pi) \mid \ldots \neg\psi \in SAT\}.
\end{aligned}
$$

Anwendung

Das Interpolationspaar charakterisiert die Interpolationseigenschaft eines Beweissystems (untere Schranken für die Beweislänge in P).

Repräsentationen von NP-Mengen

Definition

Eine Repräsentation einer NP-Menge A ist eine Folge aussagenlogischer Formeln

$$\varphi_n(\bar{x}, \bar{y}) \quad |\bar{x}| = n \ ,$$

so dass

- es einen Polynomialzeitalgorithmus gibt, der bei Eingabe 1^n $\varphi_n(\bar{x}, \bar{y})$ konstruiert und
- für alle $a \in \{0,1\}^n$ gilt

$$a \in A \quad \Longleftrightarrow \quad \varphi_n(\bar{a}, \bar{y}) \text{ ist erfüllbar.}$$

Repräsentierbare disjunkte NP-Paare

Definition

Ein DNPP (A, B) heißt repräsentierbar in P, falls Repräsentationen

$$\begin{array}{ll} \varphi_n(\bar{x}, \bar{y}) & \text{von } A \quad \text{und} \\ \psi_n(\bar{x}, \bar{z}) & \text{von } B \end{array}$$

existieren, so dass $P \vdash_* \neg\varphi_n(\bar{x}, \bar{y}) \vee \neg\psi_n(\bar{x}, \bar{z})$.

$\mathrm{DNPP}(P) = \{(A, B) \mid (A, B) \text{ ist repräsentierbar in } P\}$

Satz

Sind P und Q Beweissysteme mit $P \leq Q$, so gilt $\mathrm{DNPP}(P) \subseteq \mathrm{DNPP}(Q)$.

Die Komplexitätsklasse DNPP(P)

Resultate

- Für $P \geq$ *Resolution* ist DNPP(P) abgeschlossen unter $\leq_p$.
  (P ist abgeschlossen unter Disjunktionen.)
- Uniforme und nichtuniforme Definitionen von DNPP(P) liefern dieselben Klassen.
  (P korrespondiert zu einer arithmetischen Theorie.)
- $(Ref(P), Sat^*)$ ist $\leq_p$-hart für DNPP(P).
  (P ist abgeschlossen unter Modus Ponens und Substitutionen.)
- Falls P die Reflektionseigenschaft besitzt, dann ist $(Ref(P), Sat^*)$ $\leq_p$-vollständig für DNPP(P).
  (P ist abgeschlossen unter Modus Ponens und Substitutionen.)

DNPP(P) unter der starken $\leq_s$-Reduktion

Ein weiteres Paar:

$$U_1(P) = \{(\varphi, \psi, 1^m) \mid \varphi, \psi \text{ haben keine gem. Var., } P \vdash_{\leq m} \varphi \vee \psi \text{ und } \neg\varphi \in SAT\}$$
$$U_2(P) = \{(\varphi, \psi, 1^m) \mid \ldots \neg\psi \in SAT\}.$$

Theorem

Sei das Beweissystem P abgeschlossen unter Substitutionen mit Konstanten. Dann gilt:

- $(U_1(P), U_2(P))$ *ist* $\leq_s$*-hart für* DNPP(P).
- *Besitzt P die Reflektionseigenschaft, so ist* $(U_1(P), U_2(P))$ $\leq_s$*-vollständig für* DNPP(P).
- *Korrespondiert P zu einer arithmetischen Theorie, so sind* $(U_1(P), U_2(P))$ *und* $(I_1(P), I_2(P))$ $\leq_s$*-vollständig für* DNPP(P).

Vollständige Paare

Theorem

Folgende Bedingungen sind äquivalent:

- *Es gibt $\leq_s$-vollständige disjunkte NP-Paare.*
- *Es existiert ein Beweissystem, in dem alle NP-Paare repräsentierbar sind.*

Korollar

Ist P ein optimales Beweissystem, so ist ein $(U_1(P), U_2(P))$ $\leq_s$-vollständiges NP-Paar.

Das kanonische *EF*-Paar

Theorem

Für jede in Polynomialzeit generierbare Tautologienfolge $\Phi = \{\varphi_1, \varphi_2, \dots\}$ *gilt*

$$(Ref(EF), Sat^*) \equiv_p (Ref(EF \cup \Phi), Sat^*) \ .$$

Korollar

Wenigstens eine der folgenden Bedingungen ist erfüllt:

- Das kanonische $EF-$Paar ist vollständig für die Klasse aller disjunkten NP-Paare.
- Es existiert ein Beweissystem P, so dass

$$EF \ \leq \ EF \cup RFN(P) \ \leq \ EF + RFN(P)$$

eine Kette paarweise nicht äquivalenter Beweissysteme bildet.

Verschiedene Szenarien für DNPP(P)

Beweissystem P	Resolution, CP	$EF + \Phi$	$EF \cup \Phi$
$(Ref(P), Sat^*)$	$\leq_p$-hart	$\leq_p$-vollst.	nicht $\leq_p$-hart*
$(U_1(P), U_2(P))$	$\leq_s$-hart	$\leq_s$-vollst.	
$(I_1(P), I_2(P))$	p-separierbar	$\leq_s$-vollst.	
abgeschl. unter	Modus Ponens, Subst.		Mod. Pon.

* falls $(Ref(EF), Sat^*)$ nicht $\leq_p$-vollständig ist

Zusammenfassung

- Zwischen disjunkten NP-Paaren und aussagenlogischen Beweissystemen besteht ein enger Zusammenhang.
- Zu jedem Beweissystem definieren wir eine Komplexitätsklasse DNPP(P) disjunkter NP-Paare.
- Kanonische Paare der Beweissysteme fungieren als harte bzw. vollständige Paare für DNPP(P).

Zusammenfassung

- Zwischen disjunkten NP-Paaren und aussagenlogischen Beweissystemen besteht ein enger Zusammenhang.
- Zu jedem Beweissystem definieren wir eine Komplexitätsklasse DNPP(P) disjunkter NP-Paare.
- Kanonische Paare der Beweissysteme fungieren als harte bzw. vollständige Paare für DNPP(P).

Weitere Resultate

- NP-Paare und beschränkte Arithmetik
- Verallgemeinerungen auf Tupel von NP-Mengen

Offene Probleme

- Gibt es vollständige NP-Paare?
- Welche Eigenschaften haben kanonische NP-Paare konkreter Beweissysteme wie Resolution oder *EF*?
- Gibt es kombinatorisch definierte Kandidaten für nicht p-separierbare NP-Paare?