Automatisches Beweisen in Modaler Prädikatenlogik

19. Juni 2007

Motivation

- Automatisches Beweisen in modaler Prädikatenlogik unterentwickelt

Motivation

- Automatisches Beweisen in modaler Prädikatenlogik unterentwickelt
- Anwendungen von modaler Prädikatenlogik:
  kompakte, natürliche Modellierung unendlicher Systeme, Spezifikation und Verifikation von verteilten Systemen und Programmen, Datenbanksysteme, Linguistik

Motivation

- Automatisches Beweisen in modaler Prädikatenlogik unterentwickelt
- Anwendungen von modaler Prädikatenlogik:
  kompakte, natürliche Modellierung unendlicher Systeme, Spezifikation und Verifikation von verteilten Systemen und Programmen, Datenbanksysteme, Linguistik
- eigene Vorarbeiten bieten ideale Vorraussetzungen:

  in intuitionistischer Prädikantelogik:

  - konnektionsbasiertes Beweisverfahren (Otten & Kreitz, 1996)
  - schnellster Beweiser: ileanCoP (Otten, 2005)
  - Problemsammlung: ILTP-Library (Raths, Otten & Kreitz, 2005)

Motivation

- Automatisches Beweisen in modaler Prädikatenlogik unterentwickelt
- Anwendungen von modaler Prädikatenlogik:
  kompakte, natürliche Modellierung unendlicher Systeme, Spezifikation und Verifikation von verteilten Systemen und Programmen, Datenbanksysteme, Linguistik
- eigene Vorarbeiten bieten ideale Vorraussetzungen:

  in intuitionistischer Prädikantelogik:

  - konnektionsbasiertes Beweisverfahren (Otten & Kreitz, 1996)
  - schnellster Beweiser: ileanCoP (Otten, 2005)
  - Problemsammlung: ILTP-Library (Raths, Otten & Kreitz, 2005)

  lässt sich auf modale Prädikatenlogik übertragen

Inhalt

1. Motivation ✓
2. Modale Aussagenlogik
3. Modale Prädikatenlogik
4. Forschungsprojekt (DFG-Antrag): Ziele, Arbeitsprogramm

Modallogik

Erweiterung der klassischen Logik um Modi von wahr/falsch

$\Box A$ es ist notwendig, dass A wahr ist
$\Diamond A$ es ist möglich, dass A wahr ist

Modallogik

Erweiterung der klassischen Logik um Modi von wahr/falsch

$\Box A$ es ist notwendig, dass A wahr ist

$\Diamond A$ es ist möglich, dass A wahr ist

$\Diamond A\neg \equiv \Diamond\neg A$

Modallogik

Erweiterung der klassischen Logik um Modi von wahr/falsch

$\Box A$ es ist notwendig, dass A wahr ist
$\Diamond A$ es ist möglich, dass A wahr ist

$\Diamond A\neg \equiv \Diamond\neg A$

multimodale Logik: $\Box_i A$

Modallogik

Erweiterung der klassischen Logik um Modi von wahr/falsch

$\Box A$ es ist notwendig, dass A wahr ist
$\Diamond A$ es ist möglich, dass A wahr ist

$\Diamond A\neg \equiv \Diamond\neg A$

multimodale Logik: $\Box_i A$

Bezug zu anderen Logiken:

Logik	Bedeutung von $\Box_i A$
epistemisch	Agent i glaubt A
temporal	es wird immer A gelten (bei Zeit-Relation R_i)
deskriptive	Rolle (z.B. Attribut) i, Konzept (z.B. Ausprägung) A
dynamisch	nach Durchführung von i gilt A

Kripke-Semantik

modale Interpretation:

Kripke-Semantik

modale Interpretation:

- Menge möglicher Welten:
  Menge von Interpretationen in klassischer Logik

Kripke-Semantik

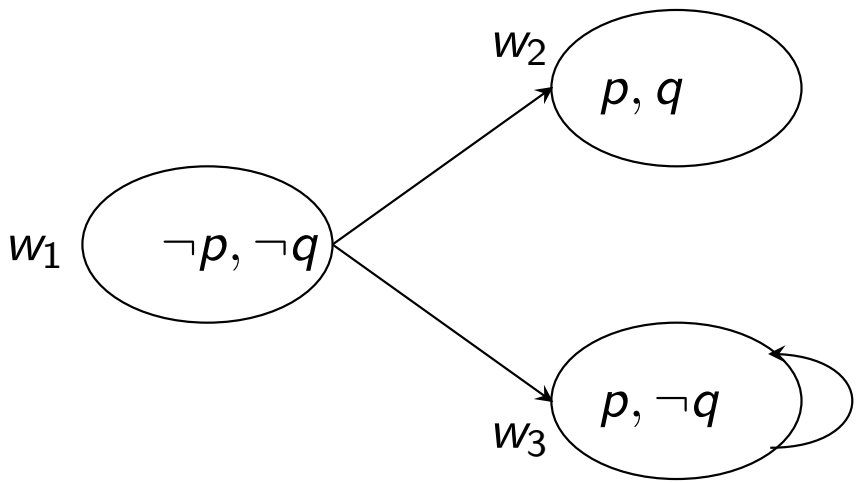
modale Interpretation:

- Menge möglicher Welten:
  Menge von Interpretationen in klassischer Logik
- Erreichbarkeitsrelation zwischen den Welten

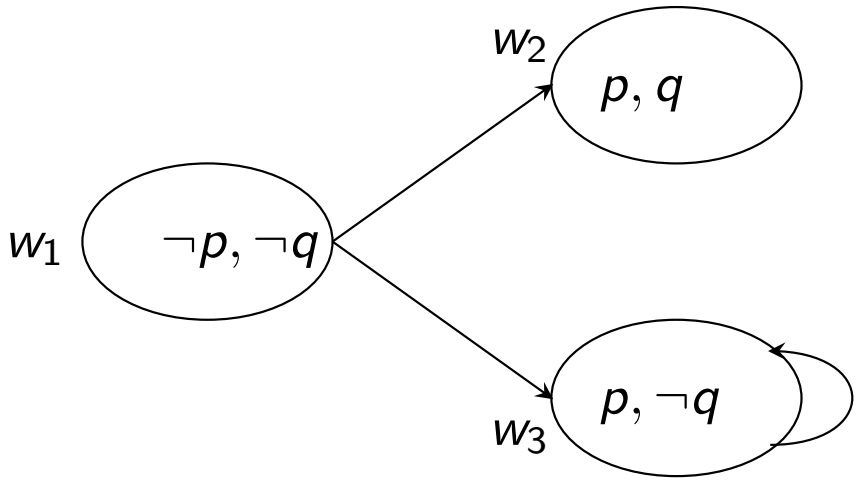
Kripke-Semantik

modale Interpretation:

- Menge möglicher Welten:
  Menge von Interpretationen in klassischer Logik
- Erreichbarkeitsrelation zwischen den Welten

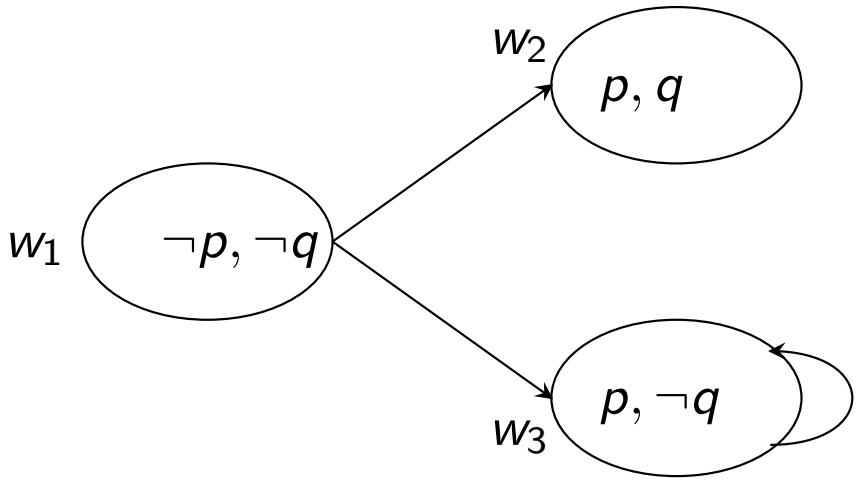


Modale Aussagenlogik



modale Interpretation: $< W, R, V >$:

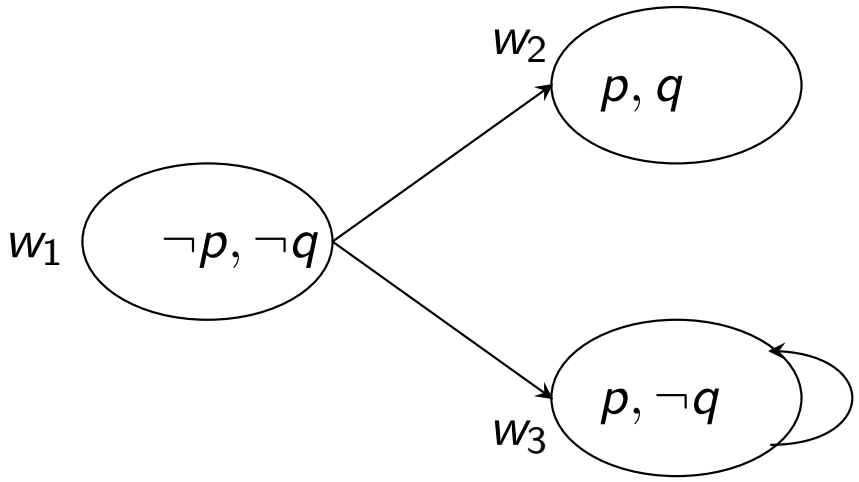
Modale Aussagenlogik



modale Interpretation: $< W, R, V >$:

$W \neq \emptyset$ mögliche Welten

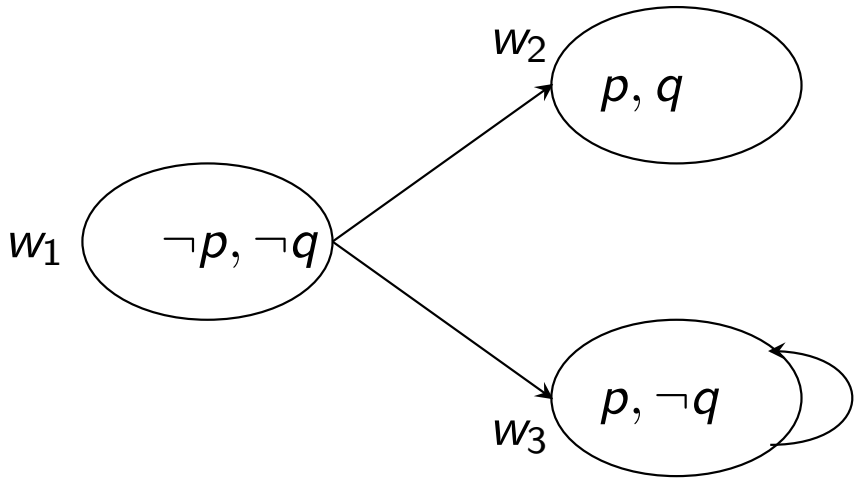
Modale Aussagenlogik



modale Interpretation: $< W, R, V >$:

$W \neq \emptyset$	mögliche Welten
$R \subseteq W \times W$	Erreichbarkeitsrelation

Modale Aussagenlogik



modale Interpretation: $< W, R, V >$:

$W \neq \emptyset$	mögliche Welten
$R \subseteq W \times W$	Erreichbarkeitsrelation
$V : W \rightarrow \mathcal{P}(L)$	Bewertungsfunktion
	L - aussagenlogische Literale p,q,r,...

Erfüllbarkeit, Gültigkeit

Erfüllbarkeit: $w \Vdash F$

Erfüllbarkeit, Gültigkeit

Erfüllbarkeit: $w \Vdash F$

für ein $< W, R, V >$ und ein $w \in W$:

- $w \Vdash p$ gdw. $p \in V(w)$
- $w \Vdash \neg A$ gdw. $w \nVdash A$
- $w \Vdash A \wedge B$ gdw. $w \Vdash A$ und $w \Vdash B$
- $w \Vdash A \vee B$ gdw. $w \Vdash A$ oder $w \Vdash B$
- $w \Vdash \Box A$ gdw. für alle $v \in W$ mit wRv gilt $v \Vdash A$
- $w \Vdash \Diamond A$ gdw. es gibt ein $v \in W$ mit wRv und $v \Vdash A$

Erfüllbarkeit, Gültigkeit

Erfüllbarkeit: $w \Vdash F$

für ein $< W, R, V >$ und ein $w \in W$:

- $w \Vdash p$ gdw. $p \in V(w)$
- $w \Vdash \neg A$ gdw. $w \nVdash A$
- $w \Vdash A \wedge B$ gdw. $w \Vdash A$ und $w \Vdash B$
- $w \Vdash A \vee B$ gdw. $w \Vdash A$ oder $w \Vdash B$
- $w \Vdash \Box A$ gdw. für alle $v \in W$ mit wRv gilt $v \Vdash A$
- $w \Vdash \Diamond A$ gdw. es gibt ein $v \in W$ mit wRv und $v \Vdash A$

Gültigkeit:

F gültig gdw. für alle $< W, R, V >$: für alle $w \in W$: $w \vDash A$

Normale Modallogiken

Notwendigkeitsregel: $\dfrac{A}{\Box A}$

Normale Modallogiken

Notwendigkeitsregel: $\dfrac{A}{\Box A}$

Distributionsaxiom K: $\Box(A \to B) \to (\Box A \to \Box B)$

Normale Modallogiken

Notwendigkeitsregel: $\dfrac{A}{\Box A}$

Distributionsaxiom K: $\Box(A \to B) \to (\Box A \to \Box B)$

einige zusätzliche Axiome:

Name	Axiom	Merkmal von R
T	$\Box A \to A$	reflexiv
D	$\Box A \to \Diamond A$	seriell (erweiterbar)
4	$\Box A \to \Box\Box A$	transitiv
5	$\Diamond A \to \Box\Diamond A$	euklidisch

Normale Modallogiken

Notwendigkeitsregel: $\dfrac{A}{\Box A}$

Distributionsaxiom K: $\Box(A \to B) \to (\Box A \to \Box B)$

einige zusätzliche Axiome:

Name	Axiom	Merkmal von R
T	$\Box A \to A$	reflexiv
D	$\Box A \to \Diamond A$	seriell (erweiterbar)
4	$\Box A \to \Box\Box A$	transitiv
5	$\Diamond A \to \Box\Diamond A$	euklidisch

seriell: $\forall u.\exists v.uRv$

euklidisch: $\forall uvw.uRv \wedge uRw \to vRw$

Normale Modallogiken

Notwendigkeitsregel: $\dfrac{A}{\Box A}$

Distributionsaxiom K: $\Box(A \to B) \to (\Box A \to \Box B)$

einige zusätzliche Axiome:

Name	Axiom	Merkmal von R
T	$\Box A \to A$	reflexiv
D	$\Box A \to \Diamond A$	seriell (erweiterbar)
4	$\Box A \to \Box\Box A$	transitiv
5	$\Diamond A \to \Box\Diamond A$	euklidisch

seriell: $\forall u.\exists v.uRv$

euklidisch: $\forall uvw.uRv \wedge uRw \to vRw$

betrachten: K, K4, D (KD), D4 (KD4), S4 (KT4), S5 (KT5)

Anwendungen von modaler Aussagenlogik

- Spezifikation und Verifikation verteilter Systeme, Multi-Agenten-Systeme, Programme, Protokolle, Betriebssysteme

Anwendungen von modaler Aussagenlogik

- Spezifikation und Verifikation verteilter Systeme, Multi-Agenten-Systeme, Programme, Protokolle, Betriebssysteme
- Schließen über deskriptive, temporale Logik, epistemische, dynamische Logik

Anwendungen von modaler Aussagenlogik

- Spezifikation und Verifikation verteilter Systeme, Multi-Agenten-Systeme, Programme, Protokolle, Betriebssysteme
- Schließen über deskriptive, temporale Logik, epistemische, dynamische Logik
- Linguistik, Datenbanksysteme, Banktransakationssysteme

Automatische Beweiser in modaler Aussagenlogik

hoch-optimierte Beweiser:

Automatische Beweiser in modaler Aussagenlogik

hoch-optimierte Beweiser:

DLP	Paul-Schneider, 1998	tableaubasiert
FaCT++	Horrocks, 1998	tableaubasiert
Racer	Haarslev & Möller, 2001	tableaubasiert
MSPASS	Hustadt & Schmidt, 2000	Translation+Resolution
*SAT	Tacchella, 1999	SAT-Solver-basiert

Automatische Beweiser in modaler Aussagenlogik

hoch-optimierte Beweiser:

DLP	Paul-Schneider, 1998	tableaubasiert
FaCT++	Horrocks, 1998	tableaubasiert
Racer	Haarslev & Möller, 2001	tableaubasiert
MSPASS	Hustadt & Schmidt, 2000	Translation+Resolution
*SAT	Tacchella, 1999	SAT-Solver-basiert

weitere Beweiser:

Modlean*TAP*	Beckert & Goré, 1997	tableaubasiert
LWB	Balsiger *et al.*, 1998	tableaubasiert
JProver($S4_n^J$)	Schmitt *et al.*, 2001 Bryukov, 2005	konnektionsbasiert

Benchmarks in modaler Aussagenlogik

- hand-generiert:

Benchmarks in modaler Aussagenlogik

- hand-generiert:
  - skalierbare Problemklassen in jeweils gültige und ungültige Version
  - Heuerding & Schwendimann (1996), Balsiger *et al.* (2000)
  - zu trivial für heutige state-of-the-art Beweiser
  - Erzeugung schwerer Probleme aufwändig

Benchmarks in modaler Aussagenlogik

- hand-generiert:
  - skalierbare Problemklassen in jeweils gültige und ungültige Version
  - Heuerding & Schwendimann (1996), Balsiger *et al.* (2000)
  - zu trivial für heutige state-of-the-art Beweiser
  - Erzeugung schwerer Probleme aufwändig
- zufällig generierte Probleme in bestimmter Normalform ($3CNF_{\Box}$)

Benchmarks in modaler Aussagenlogik

- hand-generiert:
  - skalierbare Problemklassen in jeweils gültige und ungültige Version
  - Heuerding & Schwendimann (1996), Balsiger *et al.* (2000)
  - zu trivial für heutige state-of-the-art Beweiser
  - Erzeugung schwerer Probleme aufwändig
- zufällig generierte Probleme in bestimmter Normalform ($3CNF_{\Box}$)
  - Giunchiglia *et al.* (1997, 1998), Hustadt & Schmidt (1997,1999)
  - Variation über Parameter z.B. Anzahl der Variablen, Klausen, Verschachtelungstiefe
  - künstlich, kein Bezug zu realen Anwendungen

Benchmarks in modaler Aussagenlogik

- hand-generiert:
  - skalierbare Problemklassen in jeweils gültige und ungültige Version
  - Heuerding & Schwendimann (1996), Balsiger *et al.* (2000)
  - zu trivial für heutige state-of-the-art Beweiser
  - Erzeugung schwerer Probleme aufwändig
- zufällig generierte Probleme in bestimmter Normalform ($3CNF_{\Box}$)
  - Giunchiglia *et al.* (1997, 1998), Hustadt & Schmidt (1997,1999)
  - Variation über Parameter z.B. Anzahl der Variablen, Klausen, Verschachtelungstiefe
  - künstlich, kein Bezug zu realen Anwendungen
- aus realen Anwendungen, z.B. Hardwareverifikation?

Modale Prädikatenlogik

Synonyme: Quantified Modal Logic (QML), First-order Modal Logic

Modale Prädikatenlogik

Synonyme: Quantified Modal Logic (QML), First-order Modal Logic

Kripke-Semantik: modale Interpretation:

Modale Prädikatenlogik

Synonyme: Quantified Modal Logic (QML), First-order Modal Logic

Kripke-Semantik: modale Interpretation:

- Menge möglicher Welten:
  Menge von Interpretationen in klassischer Prädikatenlogik

Modale Prädikatenlogik

Synonyme: Quantified Modal Logic (QML), First-order Modal Logic

Kripke-Semantik: modale Interpretation:

- Menge möglicher Welten:
  Menge von Interpretationen in klassischer Prädikatenlogik
- Erreichbarkeitsrelation zwischen den Welten

Modale Prädikatenlogik

Synonyme: Quantified Modal Logic (QML), First-order Modal Logic

Kripke-Semantik: modale Interpretation:

- Menge möglicher Welten:
  Menge von Interpretationen in klassischer Prädikatenlogik
- Erreichbarkeitsrelation zwischen den Welten

Erweiterung gegenüber modaler Aussagenlogik:
auf jeder Welt: Domäne von Objekten

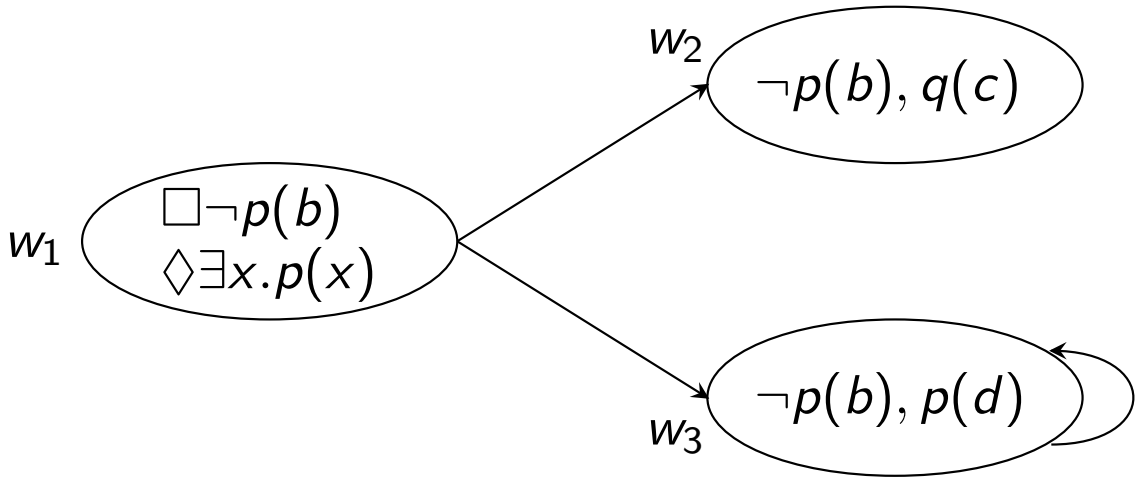
Modale Prädikatenlogik

Synonyme: Quantified Modal Logic (QML), First-order Modal Logic

Kripke-Semantik: modale Interpretation:

- Menge möglicher Welten:
  Menge von Interpretationen in klassischer Prädikatenlogik
- Erreichbarkeitsrelation zwischen den Welten

Erweiterung gegenüber modaler Aussagenlogik:
auf jeder Welt: Domäne von Objekten



Semantik in modaler Prädikatenlogik

modale Interpretation $< W, R, D, \delta, \pi, \phi >$:

Semantik in modaler Prädikatenlogik

modale Interpretation $< W, R, D, \delta, \pi, \phi >$:

$W \neq \emptyset$	mögliche Welten
$R \subseteq W \times W$	Erreichbarkeitsrelation

Semantik in modaler Prädikatenlogik

modale Interpretation $< W, R, D, \delta, \pi, \phi >$:

$W \neq \emptyset$	mögliche Welten
$R \subseteq W \times W$	Erreichbarkeitsrelation
$D \neq \emptyset$	"globale" Objektdomäne

Semantik in modaler Prädikatenlogik

modale Interpretation $< W, R, D, \delta, \pi, \phi >$:

$W \neq \emptyset$	mögliche Welten
$R \subseteq W \times W$	Erreichbarkeitsrelation
$D \neq \emptyset$	"globale" Objektdomäne
δ:	für jedes $w \in W$: Domäne von w: $\delta(w) \subseteq D$

Semantik in modaler Prädikatenlogik

modale Interpretation $< W, R, D, \delta, \pi, \phi >$:

$W \neq \emptyset$	mögliche Welten
$R \subseteq W \times W$	Erreichbarkeitsrelation
$D \neq \emptyset$	"globale" Objektdomäne
δ:	für jedes $w \in W$: Domäne von w: $\delta(w) \subseteq D$
	konstante Domänen: $\delta(w) = D \quad \forall w \in W$

Semantik in modaler Prädikatenlogik

modale Interpretation $< W, R, D, \delta, \pi, \phi >$:

$W \neq \emptyset$	mögliche Welten
$R \subseteq W \times W$	Erreichbarkeitsrelation
$D \neq \emptyset$	"globale" Objektdomäne
δ:	für jedes $w \in W$: Domäne von w: $\delta(w) \subseteq D$
	konstante Domänen: $\delta(w) = D \quad \forall w \in W$
	kumulative Domänen: $\delta(w) \subseteq \delta(w')$, wenn wRw'

Semantik in modaler Prädikatenlogik

modale Interpretation $< W, R, D, \delta, \pi, \phi >$:

$W \neq \emptyset$	mögliche Welten
$R \subseteq W \times W$	Erreichbarkeitsrelation
$D \neq \emptyset$	"globale" Objektdomäne
δ:	für jedes $w \in W$: Domäne von w: $\delta(w) \subseteq D$
	konstante Domänen: $\delta(w) = D \quad \forall w \in W$
	kumulative Domänen: $\delta(w) \subseteq \delta(w')$, wenn wRw'
	variierende Domänen: keine Einschränkung

Semantik in modaler Prädikatenlogik

modale Interpretation $< W, R, D, \delta, \pi, \phi >$:

$W \neq \emptyset$	mögliche Welten
$R \subseteq W \times W$	Erreichbarkeitsrelation
$D \neq \emptyset$	"globale" Objektdomäne
δ:	für jedes $w \in W$: Domäne von w: $\delta(w) \subseteq D$
	konstante Domänen: $\delta(w) = D \quad \forall w \in W$
	kumulative Domänen: $\delta(w) \subseteq \delta(w')$, wenn wRw'
	variierende Domänen: keine Einschränkung
π:	Interpretation der Prädikatensymbole:

Semantik in modaler Prädikatenlogik

modale Interpretation $< W, R, D, \delta, \pi, \phi >$:

$W \neq \emptyset$	mögliche Welten
$R \subseteq W \times W$	Erreichbarkeitsrelation
$D \neq \emptyset$	"globale" Objektdomäne
δ:	für jedes $w \in W$: Domäne von w: $\delta(w) \subseteq D$
	konstante Domänen: $\delta(w) = D \quad \forall w \in W$
	kumulative Domänen: $\delta(w) \subseteq \delta(w')$, wenn wRw'
	variierende Domänen: keine Einschränkung
π:	Interpretation der Prädikatensymbole:
	für ein k-stelliges Prädikatensymbol p und $w \in W$:
	$\pi(w, p) \subseteq D^k$

Semantik in modaler Prädikatenlogik

modale Interpretation $< W, R, D, \delta, \pi, \phi >$:

$W \neq \emptyset$	mögliche Welten
$R \subseteq W \times W$	Erreichbarkeitsrelation
$D \neq \emptyset$	"globale" Objektdomäne

δ: für jedes $w \in W$: Domäne von w: $\delta(w) \subseteq D$

konstante Domänen: $\delta(w) = D \quad \forall w \in W$

kumulative Domänen: $\delta(w) \subseteq \delta(w')$, wenn wRw'

variierende Domänen: keine Einschränkung

π: Interpretation der Prädikatensymbole:
für ein k-stelliges Prädikatensymbol p und $w \in W$:
$\pi(w, p) \subseteq D^k$

ϕ: Interpretation der Funktionssymbole:
für ein k-stelliges Funktionssymbol f und $w \in W$:
$\phi(w, f) \in D^k \rightarrow D$

2 Optionen in der Interpretation der Funktionssymbole

- starre Funktionssymbole: $\phi(w, F)$ gleich für alle $w \in W$
  nicht-starre Funktionssymbole: $\phi(w, F)$ abhängig von $w \in W$

2 Optionen in der Interpretation der Funktionssymbole

- starre Funktionssymbole: $\phi(w, F)$ gleich für alle $w \in W$
  nicht-starre Funktionssymbole: $\phi(w, F)$ abhängig von $w \in W$

- lokale Terme: wenn $d_1, \ldots, d_k \in \delta(w)$,
  dann $\phi(w, f)(d_1, \ldots d_k) \in \delta(w)$
  nicht-lokale Terme: keine Einschränkung

Varianten modaler Prädikatenlogik

- Erreichbarkeitsrelation: K, K4, D, D4, S4, S5, T, ...

Varianten modaler Prädikatenlogik

- Erreichbarkeitsrelation: K, K4, D, D4, S4, S5, T, ...
- Domänen: konstant, kumulativ, variierend

Varianten modaler Prädikatenlogik

- Erreichbarkeitsrelation: K, K4, D, D4, S4, S5, T, ...
- Domänen: konstant, kumulativ, variierend
- Terme: starr, flexibel

Varianten modaler Prädikatenlogik

- Erreichbarkeitsrelation: K, K4, D, D4, S4, S5, T, ...
- Domänen: konstant, kumulativ, variierend
- Terme: starr, flexibel
- Terme: lokal, nicht-lokal

Erfüllbarkeit, Gültigkeit

Erfüllbarkeit: $w \Vdash F$

Erfüllbarkeit, Gültigkeit

Erfüllbarkeit: $w \Vdash F$

für ein $< W, R, D, \delta, \pi, \phi >$ und ein $w \in W$:

Erfüllbarkeit, Gültigkeit

Erfüllbarkeit: $w \Vdash F$

für ein $< W, R, D, \delta, \pi, \phi >$ und ein $w \in W$:

- $w \Vdash p(t_1, \ldots, t_n)$ gdw. $< \phi(w, t_1), \ldots, \phi(w, t_n) > \in \pi(w, p)$

Erfüllbarkeit, Gültigkeit

Erfüllbarkeit: $w \Vdash F$

für ein $< W, R, D, \delta, \pi, \phi >$ und ein $w \in W$:

- $w \Vdash p(t_1, \ldots, t_n)$ gdw. $< \phi(w, t_1), \ldots, \phi(w, t_n) > \in \pi(w, p)$

  $\vdots$
- $w \Vdash \forall x.A$ gdw. für alle $d \in \delta(w)$ gilt $w \Vdash A[\overline{d}/x]$
- $w \Vdash \exists x.A$ gdw. es gibt ein $d \in \delta(w)$ mit $w \Vdash A[\overline{d}/x]$

($\overline{d}$ - Name (Konstante) für d)

Erfüllbarkeit, Gültigkeit

Erfüllbarkeit: $w \Vdash F$

für ein $< W, R, D, \delta, \pi, \phi >$ und ein $w \in W$:

- $w \Vdash p(t_1, \ldots, t_n)$ gdw. $< \phi(w, t_1), \ldots, \phi(w, t_n) > \in \pi(w, p)$

  $\vdots$
- $w \Vdash \forall x.A$ gdw. für alle $d \in \delta(w)$ gilt $w \Vdash A[\overline{d}/x]$
- $w \Vdash \exists x.A$ gdw. es gibt ein $d \in \delta(w)$ mit $w \Vdash A[\overline{d}/x]$

  ($\overline{d}$ - Name (Konstante) für d)

Gültigkeit:

F gültig gdw. für alle $< W, R, D, \delta, \pi, \phi >$: für alle $w \in W$: $w \vDash A$

Beweisverfahren modaler Prädikatenlogik

Translation in klassische Prädikatenlogik +
Beweiser für klassische Prädikatenlogik (meist Resolution)

Beweisverfahren modaler Prädikatenlogik

Translation in klassische Prädikatenlogik +
Beweiser für klassische Prädikatenlogik (meist Resolution)

relationale Translation (van Benthem, 1976):

- binäres Prädikatensymbol R, um die Erreichbarkeitsrelation zu repräsentieren

Beweisverfahren modaler Prädikatenlogik

Translation in klassische Prädikatenlogik +
Beweiser für klassische Prädikatenlogik (meist Resolution)

relationale Translation (van Benthem, 1976):

- binäres Prädikatensymbol R, um die Erreichbarkeitsrelation zu repräsentieren

funktionale Translation (Ohlbach, 1988):

- betrachtet Pfade durch die Welten (*world paths*)
- Literale werden jeweils mit Weltenpfad indiziert

Beweisverfahren modaler Prädikatenlogik

Translation in klassische Prädikatenlogik +
Beweiser für klassische Prädikatenlogik (meist Resolution)

relationale Translation (van Benthem, 1976):

- binäres Prädikatensymbol R, um die Erreichbarkeitsrelation zu repräsentieren

funktionale Translation (Ohlbach, 1988):

- betrachtet Pfade durch die Welten (*world paths*)
- Literale werden jeweils mit Weltenpfad indiziert
- bei optimiert-funktionale Translation: Theorieunifikation über Weltenpfade
- ähnlich zu Präfixen (Wallen, 1987)

Beweisverfahren modaler Prädikatenlogik

Translation in klassische Prädikatenlogik +
Beweiser für klassische Prädikatenlogik (meist Resolution)

relationale Translation (van Benthem, 1976):

- binäres Prädikatensymbol R, um die Erreichbarkeitsrelation zu repräsentieren

funktionale Translation (Ohlbach, 1988):

- betrachtet Pfade durch die Welten (*world paths*)
- Literale werden jeweils mit Weltenpfad indiziert
- bei optimiert-funktionale Translation: Theorieunifikation über Weltenpfade
- ähnlich zu Präfixen (Wallen, 1987)
- nur für Aussagenlogiken K und D in MSPASS implementiert

Beweisverfahren modaler Prädikatenlogik (2)

- Sequenzen-, Tableaukalküle erweitert um Regeln für $\Box$, $\Diamond$

Beweisverfahren modaler Prädikatenlogik (2)

- Sequenzen-, Tableaukalküle erweitert um Regeln für $\Box$, $\Diamond$
  - zunächst nur für kumulative Domänen (z.B. Fitting, 1988)

Beweisverfahren modaler Prädikatenlogik (2)

- Sequenzen-, Tableaukalküle erweitert um Regeln für $\Box$, $\Diamond$
  - zunächst nur für kumulative Domänen (z.B. Fitting, 1988)
  - für andere Varianten:
    Formeln assozieren mit Labels oder Präfixen

Beweisverfahren modaler Prädikatenlogik (2)

- Sequenzen-, Tableaukalküle erweitert um Regeln für $\Box$, $\Diamond$
  - zunächst nur für kumulative Domänen (z.B. Fitting, 1988)
  - für andere Varianten:
    Formeln assozieren mit Labels oder Präfixen
  - Präfixe enthalten keine oder nur eingeschränkte Variablen

Beweisverfahren modaler Prädikatenlogik (2)

- Sequenzen-, Tableaukalküle erweitert um Regeln für $\Box$, $\Diamond$
  - zunächst nur für kumulative Domänen (z.B. Fitting, 1988)
  - für andere Varianten:
    Formeln assozieren mit Labels oder Präfixen
  - Präfixe enthalten keine oder nur eingeschränkte Variablen
  - Thion, Cerrito & Cialdea Mayer (2002):
    Formeln, Funktionssymbole, freie Variablen, Skolemterme sind assoziiert mit einer natürliche Zahl, die die Welt kodiert, in der sie interpretiert werden

  Regeln: α, β, γ, δ^+ $\quad \nu_T : \dfrac{n{:}\Box A, S}{n{:}A^n, \Box A, S}$ $\quad \pi_4 : \dfrac{n{:}\Diamond A, \Box S, S'}{m{:}A^m, S^m, \Box S}$

Beweisverfahren modaler Prädikatenlogik (2)

- Sequenzen-, Tableaukalküle erweitert um Regeln für $\Box$, $\Diamond$
  - zunächst nur für kumulative Domänen (z.B. Fitting, 1988)
  - für andere Varianten:
    Formeln assozieren mit Labels oder Präfixen
  - Präfixe enthalten keine oder nur eingeschränkte Variablen
  - Thion, Cerrito & Cialdea Mayer (2002):
    Formeln, Funktionssymbole, freie Variablen, Skolemterme sind assoziiert mit einer natürliche Zahl, die die Welt kodiert, in der sie interpretiert werden

    Regeln: α, β, γ, δ^+ $\quad \nu_T : \dfrac{n{:}\Box A, S}{n{:}A^n, \Box A, S}$ $\quad \pi_4 : \dfrac{n{:}\Diamond A, \Box S, S'}{m{:}A^m, S^m, \Box S}$

- konnektionsbasiertes Beweisverfahren (Otten & Kreitz, 1996):
  - Beweissuche: Konnektionsmethode, Konnektionstableau
  - Präfixe mit freien Variablen und Skolemterme
  - Präfixunifikation

Anwendungen von modaler Prädikatenlogik

- natürliche Modellierung unendlicher Systeme

Anwendungen von modaler Prädikatenlogik

- natürliche Modellierung unendlicher Systeme
- kompaktere Modellierung der Anwendungen von modaler Aussagenlogik (?):

Anwendungen von modaler Prädikatenlogik

- natürliche Modellierung unendlicher Systeme
- kompaktere Modellierung der Anwendungen von modaler Aussagenlogik (?):
  - Spezifikation und Verifikation verteilter Systeme, Multi-Agenten-Systeme, Programme, Protokolle, Betriebssysteme

Anwendungen von modaler Prädikatenlogik

- natürliche Modellierung unendlicher Systeme
- kompaktere Modellierung der Anwendungen von modaler Aussagenlogik (?):
  - Spezifikation und Verifikation verteilter Systeme, Multi-Agenten-Systeme, Programme, Protokolle, Betriebssysteme
  - Schließen über deskriptive, temporale Logik, epistemische, dynamische Logik

Anwendungen von modaler Prädikatenlogik

- natürliche Modellierung unendlicher Systeme
- kompaktere Modellierung der Anwendungen von modaler Aussagenlogik (?):
  - Spezifikation und Verifikation verteilter Systeme, Multi-Agenten-Systeme, Programme, Protokolle, Betriebssysteme
  - Schließen über deskriptive, temporale Logik, epistemische, dynamische Logik
  - Linguistik, Datenbanksysteme, Banktransakationssysteme

Anwendungen von modaler Prädikatenlogik

- natürliche Modellierung unendlicher Systeme
- kompaktere Modellierung der Anwendungen von modaler Aussagenlogik (?):
  - Spezifikation und Verifikation verteilter Systeme, Multi-Agenten-Systeme, Programme, Protokolle, Betriebssysteme
  - Schließen über deskriptive, temporale Logik, epistemische, dynamische Logik
  - Linguistik, Datenbanksysteme, Banktransakationssysteme
- flexible Terme: Variablen bei Programmen,
  flexible Attribute in Datenbanken,
  Linguistik: Wörter wie “heute”, “dieser”

Beweiser und Benchmarks in modaler Prädikantelogik

automatische Beweiser:

Beweiser und Benchmarks in modaler Prädikantelogik

automatische Beweiser:

nur einen einzigen automatischen Beweiser gefunden:

GQML-Prover:

Beweiser und Benchmarks in modaler Prädikantelogik

automatische Beweiser:

nur einen einzigen automatischen Beweiser gefunden:

GQML-Prover:

- Thion, Cerrito & Cialdea Mayer (2002)

Beweiser und Benchmarks in modaler Prädikantelogik

automatische Beweiser:

nur einen einzigen automatischen Beweiser gefunden:

GQML-Prover:

- Thion, Cerrito & Cialdea Mayer (2002)
- analytischer Tableaukalkül mit freien Variablen

Beweiser und Benchmarks in modaler Prädikantelogik

automatische Beweiser:

nur einen einzigen automatischen Beweiser gefunden:

GQML-Prover:

- Thion, Cerrito & Cialdea Mayer (2002)
- analytischer Tableaukalkül mit freien Variablen
- Formeln, Funktionssymbole, freie Variablen, Skolemterme sind assoziiert mit Label:
  eine natürliche Zahl, die die Welt kodiert, in der sie interpretiert werden

Beweiser und Benchmarks in modaler Prädikantelogik

automatische Beweiser:

nur einen einzigen automatischen Beweiser gefunden:

GQML-Prover:

- Thion, Cerrito & Cialdea Mayer (2002)
- analytischer Tableaukalkül mit freien Variablen
- Formeln, Funktionssymbole, freie Variablen, Skolemterme sind assoziiert mit Label:
  eine natürliche Zahl, die die Welt kodiert, in der sie interpretiert werden
- betrachtete Varianten:
  - K, K4, D, S4,S5
  - kumulative, konstante, variierende Domänen
  - starre/ nicht-starre Terme
  - lokale/ nicht-lokale Terme

Beweiser und Benchmarks in modaler Prädikantelogik

automatische Beweiser:

nur einen einzigen automatischen Beweiser gefunden:

GQML-Prover:

- Thion, Cerrito & Cialdea Mayer (2002)
- analytischer Tableaukalkül mit freien Variablen
- Formeln, Funktionssymbole, freie Variablen, Skolemterme sind assoziiert mit Label:
  eine natürliche Zahl, die die Welt kodiert, in der sie interpretiert werden
- betrachtete Varianten:
  - K, K4, D, S4,S5
  - kumulative, konstante, variierende Domänen
  - starre/ nicht-starre Terme
  - lokale/ nicht-lokale Terme
- Benchmark: 10 einfache Beispielformeln

Beweiser und Benchmarks in modaler Prädikantelogik

interaktive Beweissysteme:

Natürliches Schließen:

- Basin, Mathews & Vigano (1998)
- implementiert in Isabelle

Sequenzenkalküle für lineare temporale Prädikatenlogik:

- Castellini & Smaill (2001):
- implementiert in λClam

Ziele (DFG-Antrag)

Automatisches Beweisen in modaler Prädikatenlogik signifikant beschleunigen

Ziele (DFG-Antrag)

Automatisches Beweisen in modaler Prädikatenlogik signifikant beschleunigen

- automatische Beweiser (Kalküle, Verfahren, Implementierungen) für modale Prädikatenlogik entwickeln und optimieren

Ziele (DFG-Antrag)

Automatisches Beweisen in modaler Prädikatenlogik
signifikant beschleunigen

- automatische Beweiser (Kalküle, Verfahren, Implementierungen)
  für modale Prädikatenlogik entwickeln und optimieren

  100 mal schneller als der schnellste bisherige Beweiser,
  d.h. etwa 10% mehr Probleme der Problemsammlung lösen

Ziele (DFG-Antrag)

Automatisches Beweisen in modaler Prädikatenlogik
signifikant beschleunigen

- automatische Beweiser (Kalküle, Verfahren, Implementierungen)
  für modale Prädikatenlogik entwickeln und optimieren

  100 mal schneller als der schnellste bisherige Beweiser,
  d.h. etwa 10% mehr Probleme der Problemsammlung lösen
- Problemsammlung und Testplattform
  für modale Prädikatenlogik entwickeln

Ziele (DFG-Antrag)

Automatisches Beweisen in modaler Prädikatenlogik
signifikant beschleunigen

- automatische Beweiser (Kalküle, Verfahren, Implementierungen)
  für modale Prädikatenlogik entwickeln und optimieren

  100 mal schneller als der schnellste bisherige Beweiser,
  d.h. etwa 10% mehr Probleme der Problemsammlung lösen
- Problemsammlung und Testplattform
  für modale Prädikatenlogik entwickeln

  umfangreich, repräsentativ für reale Anwendungen,
  standardisiert, gut strukturiert und dokumentiert

Ziele (DFG-Antrag)

Automatisches Beweisen in modaler Prädikatenlogik
signifikant beschleunigen

- automatische Beweiser (Kalküle, Verfahren, Implementierungen)
  für modale Prädikatenlogik entwickeln und optimieren

  100 mal schneller als der schnellste bisherige Beweiser,
  d.h. etwa 10% mehr Probleme der Problemsammlung lösen
- Problemsammlung und Testplattform
  für modale Prädikatenlogik entwickeln

  umfangreich, repräsentativ für reale Anwendungen,
  standardisiert, gut strukturiert und dokumentiert
- Anwendung der entwickelten Beweissysteme in der Praxis:

Ziele (DFG-Antrag)

Automatisches Beweisen in modaler Prädikatenlogik
signifikant beschleunigen

- automatische Beweiser (Kalküle, Verfahren, Implementierungen)
  für modale Prädikatenlogik entwickeln und optimieren

  100 mal schneller als der schnellste bisherige Beweiser,
  d.h. etwa 10% mehr Probleme der Problemsammlung lösen
- Problemsammlung und Testplattform
  für modale Prädikatenlogik entwickeln

  umfangreich, repräsentativ für reale Anwendungen,
  standardisiert, gut strukturiert und dokumentiert
- Anwendung der entwickelten Beweissysteme in der Praxis:
  Sicherheitsanforderungen in verteilten Systemen
  bei betrieblichen Abläufen einer großen Bank

Konnektions- und Tableaukalkül entwickeln

(Jens Otten)

als Basis: Beweiser für intuitionistische Prädikatenlogik:

Konnektions- und Tableaukalkül entwickeln

(Jens Otten)

als Basis: Beweiser für intuitionistische Prädikatenlogik:

- ileanCoP (Otten, 2005):
  - Konnektionskalkül für Klauselform
  - Klauselform mit Präfixen, Präfixunifikation, Skolemisierung

Konnektions- und Tableaukalkül entwickeln

(Jens Otten)

als Basis: Beweiser für intuitionistische Prädikatenlogik:

- ileanCoP (Otten, 2005):
  - Konnektionskalkül für Klauselform
  - Klauselform mit Präfixen, Präfixunifikation, Skolemisierung
- ileanTAP (Otten, 1997):
  - analytischer Tableaukalkül mit freien Variablen
  - Präfixunifikation

Konnektions- und Tableaukalkül entwickeln

(Jens Otten)

als Basis: Beweiser für intuitionistische Prädikatenlogik:

- ileanCoP (Otten, 2005):
  - Konnektionskalkül für Klauselform
  - Klauselform mit Präfixen, Präfixunifikation, Skolemisierung
- ileanTAP (Otten, 1997):
  - analytischer Tableaukalkül mit freien Variablen
  - Präfixunifikation

auf modale Prädikatenlogik übertragen $\Rightarrow$

Konnektions- und Tableaukalkül entwickeln

(Jens Otten)

als Basis: Beweiser für intuitionistische Prädikatenlogik:

- ileanCoP (Otten, 2005):
  - Konnektionskalkül für Klauselform
  - Klauselform mit Präfixen, Präfixunifikation, Skolemisierung
- ileanTAP (Otten, 1997):
  - analytischer Tableaukalkül mit freien Variablen
  - Präfixunifikation

auf modale Prädikatenlogik übertragen $\Rightarrow$

- mleanCoP: Klauselform, Skolemisierung, Präfixunifikation anpassen

Konnektions- und Tableaukalkül entwickeln

(Jens Otten)

als Basis: Beweiser für intuitionistische Prädikatenlogik:

- ileanCoP (Otten, 2005):
  - Konnektionskalkül für Klauselform
  - Klauselform mit Präfixen, Präfixunifikation, Skolemisierung
- ileanTAP (Otten, 1997):
  - analytischer Tableaukalkül mit freien Variablen
  - Präfixunifikation

auf modale Prädikatenlogik übertragen $\Rightarrow$

- mleanCoP: Klauselform, Skolemisierung, Präfixunifikation anpassen
- mleanTAP: Regeln für modale Operatoren zufügen, Präfixunifikation anpassen

Konnektions- und Tableaukalkül entwickeln (2)

- mleanCoP:
  - Konnektionskalkül für Klauselform
  - Klauselform mit Präfixen, Präfixunifikation, Skolemisierung
- mleanTAP:
  - analytischer Tableaukalkül mit freien Variablen
  - Präfixunifikation

betrachtete Varianten:

- D, D4, S4, S5, T
- kumulative, konstante, variierende Domänen

Sequenzenkalkül entwickeln

als Basis: Beweiser für intuitionistische Prädikatenlogik:

- ileanSeP (Otten, 2005):
  - analytischer Sequenzenkalkül mit freien Variablen
  - Skolemisierung

Sequenzenkalkül entwickeln

als Basis: Beweiser für intuitionistische Prädikatenlogik:

- ileanSeP (Otten, 2005):
  - analytischer Sequenzenkalkül mit freien Variablen
  - Skolemisierung

auf modale Prädikatenlogik übertragen $\Rightarrow$

Sequenzenkalkül entwickeln

als Basis: Beweiser für intuitionistische Prädikatenlogik:

- ileanSeP (Otten, 2005):
  - analytischer Sequenzenkalkül mit freien Variablen
  - Skolemisierung

auf modale Prädikatenlogik übertragen $\Rightarrow$

- mleanSeP

Sequenzenkalkül entwickeln

als Basis: Beweiser für intuitionistische Prädikatenlogik:

- ileanSeP (Otten, 2005):
  - analytischer Sequenzenkalkül mit freien Variablen
  - Skolemisierung

auf modale Prädikatenlogik übertragen $\Rightarrow$

- mleanSeP

betrachtete Varianten:

- K, K4, D, D4, S4, S5, T
- kumulative Domänen

instanzenbasierte Methode entwickeln

als Basis: für intuitionistische Prädikatenlogik:

instanzenbasierte Methode entwickeln

als Basis: für intuitionistische Prädikatenlogik:

Komponenten:

- Nichtklauselform-Instanzen-Generator (Otten, 2006)
- aussagenlogischer intuitionistischer Beweiser

instanzenbasierte Methode entwickeln

als Basis: für intuitionistische Prädikatenlogik:

Komponenten:

- Nichtklauselform-Instanzen-Generator (Otten, 2006)
- aussagenlogischer intuitionistischer Beweiser

1. generiere Nichtklauselform-Instanz:

instanzenbasierte Methode entwickeln

als Basis: für intuitionistische Prädikatenlogik:

Komponenten:

- Nichtklauselform-Instanzen-Generator (Otten, 2006)
- aussagenlogischer intuitionistischer Beweiser

1. generiere Nichtklauselform-Instanz:
   ersetze alle universell quantifizierten Variablen durch eine einzige Konstante und skolemisiere existenziell quantifizierte Variablen

instanzenbasierte Methode entwickeln

als Basis: für intuitionistische Prädikatenlogik:

Komponenten:

- Nichtklauselform-Instanzen-Generator (Otten, 2006)
- aussagenlogischer intuitionistischer Beweiser

1. generiere Nichtklauselform-Instanz:
   ersetze alle universell quantifizierten Variablen durch eine einzige Konstante und skolemisiere existenziell quantifizierte Variablen
2. beweise oder widerlege die Instanz

instanzenbasierte Methode entwickeln

als Basis: für intuitionistische Prädikatenlogik:

Komponenten:

- Nichtklauselform-Instanzen-Generator (Otten, 2006)
- aussagenlogischer intuitionistischer Beweiser

1. generiere Nichtklauselform-Instanz:
   ersetze alle universell quantifizierten Variablen durch eine einzige Konstante und skolemisiere existenziell quantifizierte Variablen
2. beweise oder widerlege die Instanz
3. wenn gültig, dann fertig

instanzenbasierte Methode entwickeln

als Basis: für intuitionistische Prädikatenlogik:

Komponenten:

- Nichtklauselform-Instanzen-Generator (Otten, 2006)
- aussagenlogischer intuitionistischer Beweiser

1. generiere Nichtklauselform-Instanz:
   ersetze alle universell quantifizierten Variablen durch eine einzige Konstante und skolemisiere existenziell quantifizierte Variablen
2. beweise oder widerlege die Instanz
3. wenn gültig, dann fertig
4. wenn ungültig, dann generiere neue Instanz

instanzenbasierte Methode entwickeln

als Basis: für intuitionistische Prädikatenlogik:

Komponenten:

- Nichtklauselform-Instanzen-Generator (Otten, 2006)
- aussagenlogischer intuitionistischer Beweiser

1. generiere Nichtklauselform-Instanz:
   ersetze alle universell quantifizierten Variablen durch eine einzige Konstante und skolemisiere existenziell quantifizierte Variablen
2. beweise oder widerlege die Instanz
3. wenn gültig, dann fertig
4. wenn ungültig, dann generiere neue Instanz
5. wenn keine neuen Instanzen generiert werden, dann stop

instanzenbasierte Methode entwickeln

als Basis: für intuitionistische Prädikatenlogik:

Komponenten:

- Nichtklauselform-Instanzen-Generator (Otten, 2006)
- aussagenlogischer intuitionistischer Beweiser

1. generiere Nichtklauselform-Instanz:
   ersetze alle universell quantifizierten Variablen durch eine einzige Konstante und skolemisiere existenziell quantifizierte Variablen
2. beweise oder widerlege die Instanz
3. wenn gültig, dann fertig
4. wenn ungültig, dann generiere neue Instanz
5. wenn keine neuen Instanzen generiert werden, dann stop

Einschränkung: nicht gleichzeitig $\forall$ und $\exists$ im Problem

instanzenbasierte Methode entwickeln (2)

auf modale Prädikatenlogik übertragen: Komponenten anpassen

instanzenbasierte Methode entwickeln (2)

auf modale Prädikatenlogik übertragen: Komponenten anpassen

aussagenlogische modale Beweiser:

instanzenbasierte Methode entwickeln (2)

auf modale Prädikatenlogik übertragen: Komponenten anpassen

aussagenlogische modale Beweiser:

- DLP, FaCT++, Racer, MSPASS, *SAT oder

instanzenbasierte Methode entwickeln (2)

auf modale Prädikatenlogik übertragen: Komponenten anpassen

aussagenlogische modale Beweiser:

- DLP, FaCT++, Racer, MSPASS, *SAT oder
- Translation von modaler in klassische Aussagenlogik:
  Translation von intuitionistischer in klassischer Aussagenlogik (Korn & Kreitz, 1997) anpassen

instanzenbasierte Methode entwickeln (2)

auf modale Prädikatenlogik übertragen: Komponenten anpassen

aussagenlogische modale Beweiser:

- DLP, FaCT++, Racer, MSPASS, *SAT oder
- Translation von modaler in klassische Aussagenlogik:
  Translation von intuitionistischer in klassischer Aussagenlogik (Korn & Kreitz, 1997) anpassen
  +
  Nichtklausel-DPLL-Verfahren (Otten, 1997)

instanzenbasierte Methode entwickeln (2)

auf modale Prädikatenlogik übertragen: Komponenten anpassen

aussagenlogische modale Beweiser:

- DLP, FaCT++, Racer, MSPASS, *SAT oder
- Translation von modaler in klassische Aussagenlogik:
  Translation von intuitionistischer in klassischer Aussagenlogik (Korn & Kreitz, 1997) anpassen
  +
  Nichtklausel-DPLL-Verfahren (Otten, 1997) oder
  Klauseltransformation + SAT-Solver (zchaff oder MiniSAT)

instanzenbasierte Methode entwickeln (2)

auf modale Prädikatenlogik übertragen: Komponenten anpassen

aussagenlogische modale Beweiser:

- DLP, FaCT++, Racer, MSPASS, *SAT oder
- Translation von modaler in klassische Aussagenlogik:
  Translation von intuitionistischer in klassischer Aussagenlogik
  (Korn & Kreitz, 1997) anpassen
  +
  Nichtklausel-DPLL-Verfahren (Otten, 1997) oder
  Klauseltransformation + SAT-Solver (zchaff oder MiniSAT)

betrachtete Varianten:

- K, K4, D4, S4, S5, T
- kumulative, konstante variierende, Domänen
  (bei kumulativen und varrierenden Domänen: nicht $\forall$ und $\exists$)

Benchmarksammlung entwickeln

Nutzen:

- Korrektheit der Beweiser testen
- Geschwindigkeit messen und vergleichen
- Anreiz für neue Kalküle, Verfahren, Implementierungen

Benchmarksammlung entwickeln

Nutzen:

- Korrektheit der Beweiser testen
- Geschwindigkeit messen und vergleichen
- Anreiz für neue Kalküle, Verfahren, Implementierungen

TPTP-Problemsammlung (klassische Prädikatenlogik) ✓

Benchmarksammlung entwickeln

Nutzen:

- Korrektheit der Beweiser testen
- Geschwindigkeit messen und vergleichen
- Anreiz für neue Kalküle, Verfahren, Implementierungen

TPTP-Problemsammlung (klassische Prädikatenlogik) ✓
ILTP-Problemsammlung (intuitionistische Prädikatenlogik) ✓

Benchmarksammlung entwickeln

Nutzen:

- Korrektheit der Beweiser testen
- Geschwindigkeit messen und vergleichen
- Anreiz für neue Kalküle, Verfahren, Implementierungen

TPTP-Problemsammlung (klassische Prädikatenlogik) ✓
ILTP-Problemsammlung (intuitionistische Prädikatenlogik) ✓

MLTP-Problemsammlung (modale Prädikatenlogik)

Benchmarksammlung entwickeln

Nutzen:

- Korrektheit der Beweiser testen
- Geschwindigkeit messen und vergleichen
- Anreiz für neue Kalküle, Verfahren, Implementierungen

TPTP-Problemsammlung (klassische Prädikatenlogik) ✓
ILTP-Problemsammlung (intuitionistische Prädikatenlogik) ✓

MLTP-Problemsammlung (modale Prädikatenlogik)

Kriterien:

- umfassend und überschaubar
- aus realen Anwendungen in Mathematik und Informatik
- verschiedener Schwierigkeitsgrad, verschiedene Größe
- Status und Schwierigkeitsgrad (Rating) für jedes Problem
- standardisierte Syntax
- gut strukturiert, dokumentiert, leicht zu bedienen

Benchmarksammlung entwickeln (2)

Inhalt:

- Problemsammlung
  modaler Status und Rating, Beschreibung, Referenzen für jedes Problem
- Informationen über verfügbare automatische Beweiser:
  Kurzbeschreibung, Autor, Referenzen, Testergebnisse
- Statistiken über Testergebnisse, Status, Rating
- Tools für Syntaxtransformation, evtl. auch für Durchführen der Tests, Generieren von Probleminstanzen, Statistiken
- Dokumentation

Benchmarksammlung entwickeln (3)

Quellen:

- bereits vorhandene Problemsammlungen

Benchmarksammlung entwickeln (3)

Quellen:

- bereits vorhandene Problemsammlungen
- Gödels Transformation:
  intuitionistische Logik in Modallogik S4

Benchmarksammlung entwickeln (3)

Quellen:

- bereits vorhandene Problemsammlungen
- Gödels Transformation:
  intuitionistische Logik in Modallogik S4
  $p \quad \Rightarrow \quad \Box p$,

Benchmarksammlung entwickeln (3)

Quellen:

- bereits vorhandene Problemsammlungen
- Gödels Transformation:
  intuitionistische Logik in Modallogik S4
  $p \Rightarrow \Box p$,
  $\neg A \Rightarrow \Box\neg A'$ (mit $A \Rightarrow A'$)

Benchmarksammlung entwickeln (3)

Quellen:

- bereits vorhandene Problemsammlungen
- Gödels Transformation:
  intuitionistische Logik in Modallogik S4
  $p \Rightarrow \Box p$,
  $\neg A \Rightarrow \Box \neg A'$ (mit $A \Rightarrow A'$)
  $A \rightarrow B \Rightarrow \Box A' \rightarrow B'$ (mit $A \Rightarrow A'$, $B \Rightarrow B'$)

Benchmarksammlung entwickeln (3)

Quellen:

- bereits vorhandene Problemsammlungen
- Gödels Transformation:
  intuitionistische Logik in Modallogik S4
  $p \Rightarrow \Box p$,
  $\neg A \Rightarrow \Box\neg A'$ (mit $A \Rightarrow A'$)
  $A \rightarrow B \Rightarrow \Box A' \rightarrow B'$ (mit $A \Rightarrow A'$, $B \Rightarrow B'$)
  $\forall x.A \Rightarrow \Box\forall x.A'$ (mit $A \Rightarrow A'$)

Benchmarksammlung entwickeln (3)

Quellen:

- bereits vorhandene Problemsammlungen
- Gödels Transformation:
  intuitionistische Logik in Modallogik S4
  $p \Rightarrow \Box p$,
  $\neg A \Rightarrow \Box\neg A'$ (mit $A \Rightarrow A'$)
  $A \rightarrow B \Rightarrow \Box A' \rightarrow B'$ (mit $A \Rightarrow A'$, $B \Rightarrow B'$)
  $\forall x.A \Rightarrow \Box\forall x.A'$ (mit $A \Rightarrow A'$)
  anwenden auf ILTP-Problemsammlung

Benchmarksammlung entwickeln (3)

Quellen:

- bereits vorhandene Problemsammlungen
- Gödels Transformation:
  intuitionistische Logik in Modallogik S4
  $p \Rightarrow \Box p$,
  $\neg A \Rightarrow \Box\neg A'$ (mit $A \Rightarrow A'$)
  $A \rightarrow B \Rightarrow \Box A' \rightarrow B'$ (mit $A \Rightarrow A'$, $B \Rightarrow B'$)
  $\forall x.A \Rightarrow \Box\forall x.A'$ (mit $A \Rightarrow A'$)
  anwenden auf ILTP-Problemsammlung
- Nichtklauselform-Instanzen-Generator (aussagenlogisch)

Benchmarksammlung entwickeln (3)

Quellen:

- bereits vorhandene Problemsammlungen
- Gödels Transformation:
  intuitionistische Logik in Modallogik S4
  $p \Rightarrow \Box p$,
  $\neg A \Rightarrow \Box\neg A'$ (mit $A \Rightarrow A'$)
  $A \rightarrow B \Rightarrow \Box A' \rightarrow B'$ (mit $A \Rightarrow A'$, $B \Rightarrow B'$)
  $\forall x.A \Rightarrow \Box\forall x.A'$ (mit $A \Rightarrow A'$)
  anwenden auf ILTP-Problemsammlung
- Nichtklauselform-Instanzen-Generator (aussagenlogisch)
- Anwendungen in modaler Prädikatenlogik
  z.B. Modellierung von Sicherheitsanforderungen in verteilten Systemen

Benchmarksammlung entwickeln (3)

Quellen:

- bereits vorhandene Problemsammlungen
- Gödels Transformation:
  intuitionistische Logik in Modallogik S4
  $p \Rightarrow \Box p$,
  $\neg A \Rightarrow \Box\neg A'$ (mit $A \Rightarrow A'$)
  $A \rightarrow B \Rightarrow \Box A' \rightarrow B'$ (mit $A \Rightarrow A'$, $B \Rightarrow B'$)
  $\forall x.A \Rightarrow \Box\forall x.A'$ (mit $A \Rightarrow A'$)
  anwenden auf ILTP-Problemsammlung
- Nichtklauselform-Instanzen-Generator (aussagenlogisch)
- Anwendungen in modaler Prädikatenlogik
  z.B. Modellierung von Sicherheitsanforderungen in verteilten Systemen
- Call-for-Problem

Benchmarksammlung entwickeln (4)

Status und Rating:

- Status: Theorem, Nicht-Theorem, Unsolved
- Rating: 0.0 . . . 1.0
  Anteil der besten Beweiser, die das Problem nicht gelöst haben
- für verschiedene modale Prädikatenlogik-Varianten:
  - K, K4, D, D4, S4, S5, T
  - kumulative, konstante, variierdende Domänen
- Tests aller verfügbaren automatischen Beweiser
- Tools zum automatischen Durchführen der Tests, Erstellen von Statistiken und Vergleichen, Prüfen von Inkonsistenzen aus dem Erstellen der ILTP-Problemsammlung verwenden
- Hardware: 18-Prozessor-Cluster, Xeon 3.4 Ghz

Erste Benchmarks

Gödel-Transformation der ILTP-v1.1.2-Library

- 2550 Probleme aus Mathematik, Programmverifikation, ...
- S4, kumulative Domäne, starre, lokale Terme
- bis jetzt "nur" 1792 Probleme getestet

	GQML-Prover	mleanSeP	mleanTAP
bewiesen	44	177	103
unbekannt	57	0	0
0-1 s	38	132	97
1-10 s	0	24	5
10-100 s	5	17	0
100-600 s	1	4	1
>600s	1691	1466	1677

Anwendung

Schließen über Sicherheitsanforderungen in verteilten Systemen

- Forschungsprojekt von TU Darmstadt, Universität Luxemburg und einer großen Bank
- Christoph Brandt (Universität Luxemburg)
- Zertifizierung von Komponenten der IT-Infrastruktur in der Bank
- für höchste Zertifizierungsstufe sind formale Methoden vorgeschrieben
- Formalisierung der Sicherheitsanforderungen in verteilten Systemen, die in betrieblichen Abläufen einer großen Bank auftreten
- Unvollständikgeiten und Inkonsistenzen in den Sicherheitsanforderungen durch ein Beweissystem erkennen
- modale Prädikatenlogik kann hier verwendet werden

Kooperationen

- Christoph Brandt (Universität Luxemburg):
  Anwendung auf Sicherheitsanforderungen in verteilten Systemen
- Geoff Sutcliffe (Universität Miami):
  Problemsammlungen (TPTP, MPTP Challenge)
- Arild Waaler (Universität Oslo):
  Beweisverfahren in nichtklassischer Logik
- Daniel Korn:
  gültigkeitserhaltende Translation von intuitionistische in klassische Aussagenlogik

Sonstiges

Untersuchungen am Menschen:

— entfällt —

Tierversuche:

— entfällt —

Gentechnologische Experimente:

— entfällt —

Zusammenfassung

Automatisches Beweisen in modaler Prädikatenlogik

- Automatisches Beweisen in modaler Prädikatenlogik unterentwickelt gegenüber modaler Aussagenlogik (Beweiser, Problemsammlungen, Anwendungen)
- modale Prädikatenlogik, Varianten:
  - Merkmale der Erreichbarkeitsrelation: K, K4, D, D4, S4, S5, T
  - konstante, kumulative, variierende Domänen
  - starre, flexible Terme
  - lokale, nicht-lokale Terme
- Automatische Beweiser und Problemsammlung für intuitionistische Prädikatenlogik lassen sich auf modale Prädikatenlogik übertragen
- Anwendungen möglich