2.3 Der Satz von Herbrand

Frage

Wie zeigt man die Unerfüllbarkeit einer Formel φ in CNF?
(Es gibt viele sig-Algebren $\mathcal{A}$, die φ erfüllen könnten!)

Hier

Es reicht, solche $\mathcal{A}$ zu betrachten, bei denen die Grundterme über sig das Universum bilden.

$\Rightarrow$ Herbrand-Interpretationen.

Bezeichnung

Ein Objekt (Term, Gleichung, Atom, ...) heißt ein **Grundobjekt**, falls es keine Variablen enthält.

Sei Term(F) die Menge der **Grundterme** über sig $= (F, P, \alpha)$.

Ab jetzt

sig $= (F, P, \alpha)$ ist eine Signatur. Es gibt eine Konstante $c \in F$.

φ ist eine Formel über sig in CNF.

S ist eine Klauselmenge über sig, die Klauseln sind paarweise Variablen-disjunkt.

Bezeichnungen

Klauseln

Schreibweise einer Klausel $C \equiv \Gamma \Rightarrow \Delta$ mit Γ, Δ Multimengen von Atomen:

- Ist $\Gamma = \{A_1, \ldots, A_n\}$ und $\Delta = \{B_1, \ldots, B_m\}$, so ist $C \equiv \neg A_1 \vee \cdots \vee \neg A_n \vee B_1 \vee \cdots \vee B_m$.
- Γ ist der **Antezedent**, Δ ist der **Sukzedent** von C.
- Die A_i (B_i) sind die negativen (positiven) Literale in C.
- Es ist $\Box$ die **leere Klausel**, d. h. $n = m = 0$.
- C ist eine **Horn-Klausel**, falls $m \leq 1$.
- $A, \Gamma, \Gamma' \Rightarrow \Delta, B$ steht für $\{A\} \cup \Gamma \cup \Gamma' \Rightarrow \Delta \cup \{B\}$.

Substitutionen

Eine Substitution σ ist gegeben durch $\sigma : V \to$ Term(F, V).

Dann
$$\begin{aligned}
&\sigma(f(t_1, \ldots, t_n)) \equiv f(\sigma(t_1), \ldots, \sigma(t_n))\\
&\sigma(p(t_1, \ldots, t_n)) \equiv p(\sigma(t_1), \ldots, \sigma(t_n))\\
&\sigma(\Gamma) \equiv \{\sigma(A) \mid A \in \Gamma\}\\
&\sigma(\Gamma \Rightarrow \Delta) \equiv \sigma(\Gamma) \Rightarrow \sigma(\Delta)
\end{aligned}$$

Herbrand-Strukturen

Definition 2.7.

Eine sig-Algebra $\mathcal{A} = (A;\ F^{\mathcal{A}}, P^{\mathcal{A}})$ über sig $= (F, P, \alpha)$ ist eine **Herbrand-Algebra**, falls

$$\begin{array}{ll} A = \mathsf{Term}(F) & \\ f^{\mathcal{A}}(t_1, \dots, t_n) = f(t_1, \dots, t_n) & \text{für } f \in F,\ t_1, \dots, t_n \in A \\ p^{\mathcal{A}} \subseteq A^n & \text{für } p \in P \end{array}$$

Also

Eine Herbrand-Algebra $\mathcal{A}$
- hat die Grundterme als Elemente des Universums,
- interpretiert die $f \in F$ in kanonischer Weise,
- interpretiert die $p \in P$ als Prädikate auf $A = \mathsf{Term}(F)$.

Sie ist festgelegt durch die **Herbrand-Interpretation**

$$I = \{p(t_1, \dots, t_n) \mid (t_1, \dots, t_n) \in p^{\mathcal{A}}\}$$

Dies steht für

$$I(p(t_1, \dots, t_n)) = \begin{cases} \text{true} & \text{falls } (t_1, \dots, t_n) \in p^{\mathcal{A}} \\ \text{false} & \text{falls } (t_1, \dots, t_n) \notin p^{\mathcal{A}} \end{cases}$$

Beachte

Eine Herbrand-Algebra $\mathcal{A}$ (**ein H-Modell**) ist eindeutig durch die Interpretation I der Grundatome $p(t_1, \dots, t_n)$, d. h., deren Belegung mit Wahrheitswerten, festgelegt.

Herbrand-Erfüllbarkeit

Sei $\varphi \equiv \forall^*(C_1 \wedge \cdots \wedge C_n)$ eine Formel in CNF.
$S_\varphi = \{C_1, \dots, C_n\}$.
$\mathcal{A}$ eine H-Algebra, festgelegt durch I.

Bezeichnung

- I erfüllt Grundatom $p(t_1, \dots, t_n)$ gdw $p(t_1, \dots, t_n) \in I$.
- I erfüllt Grundklausel $\Gamma \Rightarrow \Delta$ gdw I erfüllt ein Atom aus Γ nicht oder I erfüllt ein Atom aus Δ.
- I erfüllt die Klausel C, falls für jede Grundsubstitution σ gilt: I erfüllt $\sigma(C)$.
- I erfüllt eine Klauselmenge S, falls I alle $C \in S$ erfüllt.
- $\mathsf{gnd}(S) = \{\sigma(C) \mid C \in S, \sigma(C) \text{ ist eine Grundklausel } \}$

Lemma 2.7

$\mathcal{A}$ erfüllt φ gdw I erfüllt $\mathsf{gnd}(S_\varphi)$.

Definition 2.8.

φ ist **Herbrand-erfüllbar**, falls es eine H-Algebra $\mathcal{A}$ gibt, die φ erfüllt (also: falls es eine H-Interpretation I gibt, die $\mathsf{gnd}(S_\varphi)$ erfüllt).

Hauptresultat für PL1

Satz 2.4. (Gödel-Herbrand-Skolem)

Eine Formel φ in CNF ist erfüllbar genau dann, wenn sie Herbrand-erfüllbar ist.

Beweis:

- Sei $\varphi \equiv \forall x_1, \ldots, x_m.M$ und $M \equiv C_1 \wedge \cdots \wedge C_n$.
- Ist φ H-erfüllbar, so ist φ auch erfüllbar.
- Sei φ erfüllbar, etwa durch sig-Algebra $\mathcal{A} = (A, F^{\mathcal{A}}, P^{\mathcal{A}})$, d. h., $\mathcal{A} \models \varphi$.
- Wir konstruieren eine H-Interpretation I, die alle $\sigma(C_i)$ mit $i = 1, \ldots, n$, σ Grundsubstitution erfüllt: Setze

  $$I = \{p(t_1, \ldots, t_k) \mid \mathcal{A} \models p(t_1, \ldots, t_k), t_j \in \mathsf{Term}(F)\}$$

- Wegen $\mathcal{A} \models \varphi$ gilt $\mathcal{A} \models \forall x_1, \ldots, x_m.C_i$,
  also auch für alle Grundsubstitutionen σ und alle $i = 1, \ldots, n$:
  $\mathcal{A} \models \sigma(C_i)$
  also $\mathcal{A} \models l$ für ein Literal l in $\sigma(C_i)$
  also I erfüllt $\sigma(C_i)$.
- Also erfüllt I $\mathsf{gnd}(S_\varphi)$.

Bemerkung zu Satz 2.4

Sei $\varphi \equiv \forall^*(C_1 \wedge \cdots \wedge C_n)$ eine Formel in CNF.
$S = \{C_1, \ldots, C_n\}$.

Es gilt

S ist erfüllbar gdw $\mathsf{gnd}(S)$ ist erfüllbar.

Beachte

$\mathsf{gnd}(S)$ ist eine (i. Allg. unendliche) Menge von Grundklauseln. Die Erfüllbarkeit von $\mathsf{gnd}(S)$ bezieht sich also auf die Aussagenlogik.

Also

Sei $\mathcal{A}x = \{\psi_1, \ldots, \psi_n\}$ und S eine Klauselmenge zu $\psi_1 \wedge \cdots \wedge \psi_n \wedge \neg\psi$. Dann gilt

$\mathcal{A}x \models \psi$ gdw $\mathsf{gnd}(S)$ ist aussagenlogisch unerfüllbar.

Beispiel

Sei $\mathcal{A}x = \{\forall x.p(x), \forall y.q(y)\}$ $\quad \psi \equiv \forall x.(p(f(x)) \wedge q(x))$
Dann $S = \{p(x), q(y), \neg p(f(a)) \vee \neg q(a)\}$.
Also $\mathsf{gnd}(S) = \{p(t_1), q(t_2) \mid t_1, t_2 \in \mathsf{Term}(F)\}$
$\cup\{\neg p(f(a)) \vee \neg q(a)\}$,
also $p(f(a)), q(a), \neg p(f(a)) \vee \neg q(a) \in \mathsf{gnd}(S)$.
Also $\mathsf{gnd}(S)$ ist unerfüllbar.

Hauptresultat für PL1 mit Gleichheit

Definition 2.9.

Eine **Herbrand-Algebra** $\mathcal{A}$ in PL1 mit Gleichheit ist eine Herbrand-Algebra in der $=^{\mathcal{A}}$ eine Kongruenzrelation ist (d. h., es gilt $\mathcal{A} \models \varphi$ für alle $\varphi \in \mathcal{A}x_=$). Die durch sie festgelegte Interpretation ist eine **Herbrand-Interpretation** (**H-Interpretation**).

Dann

Es bleiben alle Begriffe sinnvoll und die Überlegungen richtig.

Satz 2.5.

Eine Formel φ in CNF ist genau dann erfüllbar, wenn sie Herbrand-erfüllbar ist.

Also

Sei $\mathcal{A}x = \{\varphi_1, \ldots, \varphi_m\}$ und S eine Klauselmenge zu $\varphi_1 \wedge \cdots \wedge \varphi_m \wedge \neg\varphi$. Es gilt
$\mathcal{A}x \models \varphi$ gdw keine Herbrand-Interpretation I erfüllt S.

Beachte

Eine H-Algebra $\mathcal{A}$ zu sig ist eine sig-Algebra im Sinn von PL1.
Es gilt dann $\mathcal{A} \models \varphi$ in PL1 $\quad \mathrm{gdw} \quad \mathcal{A}/=^{\mathcal{A}} \models \varphi$ in PL1=

Behandlung von Prädikatssymbolen (1)

Ziel

Der Superpositionskalkül, wie er später eingeführt wird, geht davon aus, dass $=$ das einzige Prädikatssymbol ist. Wir zeigen, dass dies keine wesentliche Beschränkung ist.

Transformation

Gegeben: Signatur sig $= (S, F, P \cup \{=\}, \alpha)$ und Klauselmenge S über sig.

Gesucht: Signatur $\text{sig}_0 = (S_0, F_0, \{=\}, \alpha_0)$ und Klauselmenge S_0 über sig_0 mit S ist H-erfüllbar gdw S_0 ist H-erfüllbar.

Setze $S_0 = S \cup \{\mathsf{BOOL}_0\}$, BOOL_0 eine neue Sorte
$F_0 = F \cup P \cup \{\top\}$
$\alpha_0(f) = \alpha(f)$ für $f \in F$
$\alpha_0(p) = s_1 \ldots s_n \to \mathsf{BOOL}_0$, falls $\alpha(p) = s_1 \ldots s_n$
$\alpha_0(\top) = \to \mathsf{BOOL}_0$.
Die Klauselmenge S_0 entsteht aus S dadurch, dass jedes Atom A durch $A = \top$ ersetzt wird.

Beachte

Ein H-Modell zu sig hat als Universum die Menge $\mathrm{Term}(F, \emptyset)$ der Grundterme. Es ist eindeutig festgelegt durch eine Menge I von Grundatomen (den Atomen, die im Modell wahr sind). Das Modell muss die Gleichheitsaxiome erfüllen.

Behandlung von Prädikatssymbolen (2)

Satz 2.6.

Sei (sig, S) und (sig_0, S_0) wie eben. Es gilt S ist H-erfüllbar über sig gdw S_0 ist H-erfüllbar über sig_0.

Beweis:

a) Sei I ein H-Modell zu sig, das S erfüllt. Wir konstruieren ein H-Modell I_0 zu sig_0, das S_0 erfüllt: Setze
   $I_0 = =_E$ mit $E = E' \cup E''$
   $E' = \{t_1 = t_2 \mid I \models t_1 = t_2,\ t_1 = t_2 \text{ Grundatom zu sig}\}$
   $E'' = \{A = \top \mid I \models A,\ A \text{ Grundatom zu sig}\}$
   Es gilt
   (1) $A =_E \top$ gdw $I \models A$ (Übung)
   (2) I_0 ist ein H-Modell zu sig_0
   (3) I_0 erfüllt S_0, wegen (1) und I erfüllt S.

b) Sei I_0 ein H-Modell zu sig_0, das S_0 erfüllt. Wir konstruieren ein H-Modell zu sig, das S erfüllt: Setze
   $I = M \cup =_E$ mit
   $M = \{A \mid I_0 \models A = \top,\ A \text{ Grundatom zu sig}\}$
   $E = \{t_1 = t_2 \mid I_0 \models t_1 = t_2,\ t_1 = t_2 \text{ Grundatom zu sig}\}$
   Es gilt
   (1) I ist ein H-Modell zu sig, da I_0 ein H-Modell zu sig_0 ist.
   (2) I erfüllt S, da I_0 S_0 erfüllt.

Bemerkung zur Herbrand-Erfüllbarkeit

Betrachte PL1:

Sei $S = \{C_1, \ldots, C_n\}$
$\text{gnd}(S) = \{\sigma(C) \mid C \in S, \sigma \text{ Grundsubstitution}\}$

Es gilt

S ist H-erfüllbar gdw $\text{gnd}(S)$ ist aussagenlogisch erfüllbar.

Satz 2.7. (Kompaktheitssatz der Aussagenlogik)

Eine unendliche Menge M von aussagenlogischen Formeln ist genau dann unerfüllbar, wenn eine endliche Teilmenge $M_0 \subseteq M$ unerfüllbar ist.

ohne Beweis.

Folgerung

Das folgende Problem ist rekursiv aufzählbar.

Eingabe: S, eine endliche Klauselmenge über endlicher Signatur.
Frage: Ist S unerfüllbar?

Beweis: Man zähle die endlichen Teilmengen S_0 von $\text{gnd}(S)$ auf und teste jeweils auf Erfüllbarkeit.
Antworte JA, falls eine Menge $S_0 \subseteq \text{gnd}(S)$ unerfüllbar ist.

Das Entscheidungsproblem der Prädikatenlogik

Satz 2.8.

Das folgende Problem ist rekursiv aufzählbar, aber nicht rekursiv.

Eingabe: $\mathcal{A}x, \varphi$ über endlicher Signatur.
Frage: Gilt $\mathcal{A}x \models \varphi$?

Beweis-Idee:

Aus der letzten Folgerung ergibt sich, dass das Problem rekursiv aufzählbar ist.
Man kann das Post'sche Korrespondenzproblem PCP auf dieses Problem reduzieren. Also ist es nicht rekursiv.

Ziel der Vorlesung

Ein effizientes Verfahren, das JA meldet, wenn eine Klauselmenge S unerfüllbar ist.

Beachte

Das eben skizzierte Verfahren ist hochgradig ineffizient, wenn das Herbrand-Universum Term(F) unendlich ist. Sonst ist das Problem entscheidbar, da reduzierbar auf ein endliches Problem der Aussagenlogik.

3 Reine Gleichheitslogik

3.1 Der generelle Ansatz

Problemstellung in Kapitel 3

Gegeben: $\mathcal{A}x = \{\varphi_1, \dots, \varphi_n\}$ und φ mit
$\varphi_i \equiv \forall^* s_i = t_i$ und $\varphi \equiv Q^* u = v$
Frage: Gilt $\mathcal{A}x \models \varphi$?
Dabei ist Q^* eine Folge von $\forall$, $\exists$-Quantoren.

Transformation in Klauselform von $\varphi_1 \wedge \cdots \wedge \varphi_n \wedge \neg\varphi$ liefert
$S = Ax \cup \{\neg\bar{u} = \bar{v}\}$ mit $Ax = \{s_i = t_i \mid i = 1, \dots, n\}$

Es gilt

$\mathcal{A}x \models \varphi$

gdw es gibt keine H-Interpretation für S,

gdw jede H-Interpretation für Ax erfüllt nicht $\forall^*\bar{u} \neq \bar{v}$

gdw jede H-Interpretation für Ax erfüllt $\exists^*\bar{u} = \bar{v}$ (*)

Frage

Wie zeigt man (*)?

Die Beweistechnik

Beachte

Jede H-Interpretation für Ax ist eine Kongruenzrelation $\sim_{Ax}$ auf den Grundtermen, die Ax erfüllt.

Die gröbste dieser H-Interpretationen ist $=_{Ax}$. Dabei gilt $u =_{Ax} v$ genau dann, wenn sich u durch Anwenden von Gleichungen aus Ax in v überführen lässt.

Erfüllt $=_{Ax}$ die Formel $\exists^* \bar{u} = \bar{v}$, so gilt dies auch für alle $\sim_{Ax}$.

Definition 3.1.

Eine Ax-**Lösung** von $\bar{u} = \bar{v}$ ist eine Grundsubstitution σ mit $\sigma(\bar{u}) =_{Ax} \sigma(\bar{v})$.

Folgerung

Es gilt $\mathcal{A}x \models \varphi \text{ gdw } \bar{u} = \bar{v}$ ist Ax-lösbar.

Ziel

a) Aus Ax ein grundkonvergentes Regelsystem R erstellen.
b) Mit R die Ax-Lösbarkeit von $\bar{u} = \bar{v}$ testen.

Ein Beispiel

Beachte

Sei $\varphi \equiv \forall x_1, \ldots, x_k.u = v$ ein all-quantifiziertes Ziel.

Skolemisierung liefert $\bar{u} = \bar{v}$ mit
$\bar{u} \equiv \sigma(u), \bar{v} \equiv \sigma(v), \sigma = \{x_i \leftarrow a_i \mid i = 1, \ldots, k\}, a_i$ neu.

Also ist $\bar{u} = \bar{v}$ eine Grundgleichung (variablenfrei).

Es gilt: $\bar{u} = \bar{v}$ ist Ax-lösbar $\text{gdw } \bar{u} =_{Ax} \bar{v}$.

Beispiel

$\mathcal{A}x$: $\forall x.\ x + 0 = x$, $\forall x, y.\ x + s(y) = s(x + y)$, $s^3(0) = 0$.
φ: $\forall x.\ s^3(x) = x$.

Dies liefert
Ax: $x + 0 = x \quad x + s(y) = s(x + y) \quad s^3(0) = 0$.
$\bar{u} = \bar{v}$: $s^3(a) = a$.

Vervollständigung von Ax liefert

$R : x + 0 \to x \quad x + s(y) \to s(x + y) \quad s^3(x) \to x$

Also $s^3(a) \downarrow a$ und $\bar{u} =_{Ax} \bar{v}$.

Also gilt $\mathcal{A}x \models \varphi$.

Bemerkungen zu $\mathcal{A}x \models \varphi$

1. Bemerkung

Die Beweistechnik funktioniert immer, falls

1. $=$ das einzige Prädikatensymbol ist, also jedes Atom die Form $t_1 = t_2$ hat.
2. S nur Unit-Klauseln enthält, also jedes C in S nur aus einem Literal besteht.

2. Bemerkung

Sei sig $= (F, P, \alpha)$ und $\mathcal{A}x \cup \{\varphi\}$ enthalte nur sig-Formeln.

Dann sind die Terme in S F^e-Terme mit $F \subseteq F^e$, denn die Skolemisierung von $\neg\varphi$ führt neue Funktionssymbole ein.

Dann ist das Herbrand-Universum Term(F^e), nicht Term(F).

3. Bemerkung

Man benötigt häufig kein grund-konvergentes R zu $\mathcal{A}x$. (Es kann unendlich sein!) Es reicht, R hinreichend genau zu approximieren, so dass die Ax-Lösbarkeit von $\bar{u} = \bar{v}$ nachweisbar ist.

Reduzierte Problemstellung

Problemstellung ursprünglich

Gegeben: $\mathcal{A}x, \varphi$ über sig $= (F, P, \alpha)$ mit $P = \{=\}$ wie oben.
Frage: Gilt $\mathcal{A}x \models \varphi$?

Problemstellung reduziert

Gegeben: $Ax = \{s_i = t_i \mid i = 1, \ldots, n\}$ und $\bar{u} = \bar{v}$ mit $s_i, t_i, \bar{u}, \bar{v} \in$ Term(F^e, V), $F \subseteq F^e$.
Frage: Ist $\bar{u} = \bar{v}$ Ax-lösbar?

Ab jetzt:

Nur noch reduzierte Problemstellung betrachtet.

Wir schreiben F statt F^e und $u = v$ statt $\bar{u} = \bar{v}$.

Beachte

Ist φ all-quantifiziert, d. h. $\varphi \equiv \forall^* u = v$, so ist $\bar{u} = \bar{v}$ eine Grundgleichung. Enthält φ auch den $\exists$-Quantor, so enthält $\bar{u} = \bar{v}$ auch Variablen.