Logik und Logikprogrammierung
12. Vorlesung

Dietrich Kuske

FG Automaten und Logik, TU Ilmenau

Wintersemester 2023/24

Ziel

Wir streben einen Resolutionskalkül an, mit dessen Hilfe wir Folgerungen $\Gamma \models \varphi$ bzw. Unerfüllbarkeiten von $\Gamma \cup \{\neg\varphi\}$ feststellen können.

In der Aussagenlogik benötigte dies, daß $\Gamma \cup \{\neg\varphi\}$ Menge von Klauseln ist, aber wir haben auch gesehen, daß sich jede Formelmenge der Aussagenlogik (mittels Tseitins Konstruktion) in eine erfüllbarkeitsäquivalente Klauselmenge umwandeln läßt.

Analog hier: wir werden die Resolution zunächst für restriktive Formelmengen Γ betrachten und dann untersuchen, wie wir sie für allgemeinere Formeln nutzen können.

„Grundresolution“

Definition (vgl. Folie 6.3)

Eine Formel λ ist ein Literal, wenn sie $\bot$, atomar, oder Negation einer atomaren Formel ist (z.B. $\bot$, $s = t$, $\neg P(s, s, t)$, aber nicht $\neg\bot$).

Eine Klausel ist eine Aussage der Gestalt

$$\varphi = \forall x_1 \forall x_2 \ldots \forall x_n \bigvee_{1 \leq i \leq m} \lambda_i$$

wobei jede Formel λ_i ein Literal ist mit $\{x_1, \ldots, x_n\} = FV\left(\bigvee_{1 \leq i \leq m} \lambda_i\right)$.

Die Klausel φ heißt Hornklausel, wenn höchstens ein Literal der Form $P(t_1, \ldots, t_n)$ oder $s = t$ vorkommt.

Bemerkung

Eine variablen- und gleichungslose Klausel ist also eine Disjunktion von Literalen der Form

$$\bot, \; P(s_1, \ldots, s_n) \text{ und } \neg P(s_1, \ldots, s_n)$$

für variablenlose Terme $s_1, \ldots, s_n$.

Sei Γ eine Menge von variablen- und gleichungslosen Klauseln über der Signatur Σ. Jede atomare variablenlose Σ-Formel $P(s_1, \ldots, s_n)$ betrachten wir als atomare Aussage der Aussagenlogik, wodurch Γ eine Menge von Klauseln der Aussagenlogik wird.

Behauptung

Die Menge Γ ist im prädikatenlogischen Sinne genau dann erfüllbar, wenn sie im aussagenlogischen Sinne erfüllbar ist.

Beweis: Sei zunächst $\mathcal{A}$ Struktur und ρ Variableninterpretation mit $\mathcal{A} \models_\rho \Gamma$. Wir definieren eine Belegung $\mathcal{B}$ wie folgt:

$$\mathcal{B}\big(P(s_1, \ldots, s_n)\big) = \begin{cases} 1 & \text{falls } \mathcal{A} \models_\rho P(s_1, \ldots, s_n) \\ 0 & \text{sonst} \end{cases}$$

Für jede variablen- und gleichungslose Klausel γ gilt dann

$$\mathcal{B}(\gamma) = 1 \iff \mathcal{A} \models_\rho \gamma\,.$$

Also ist Γ im aussagenlogischen Sinne erfüllbar.

Sei umgekehrt Γ im aussagenlogischen Sinne erfüllbar, d.h. sei $\mathcal{B}$ eine Belegung mit $\mathcal{B}(\gamma) = 1$ f.a. $\gamma \in \Gamma$.
Wir konstruieren ein (prädikatenlogisches) Modell $\mathcal{A}$ von Γ:

(1) Das Universum $U_\mathcal{A}$ ist die Menge der variablenlosen Terme t.

(2) Die Funktion $f^\mathcal{A}\colon U_\mathcal{A}^n \to U_\mathcal{A}$ für $f \in \mathrm{Fun}$ ist gegeben durch

$$f^\mathcal{A}(t_1, \dots, t_n) = f(t_1, \dots, t_n) \in U_\mathcal{A}$$

für alle $t_1, \dots, t_n \in U_\mathcal{A}$.

(3) Für $P \in \mathrm{Rel}$ setze

$$P^\mathcal{A} = \Big\{ (t_1, \dots, t_n) \;\Big|\; t_1, \dots, t_n \in U_\mathcal{A} \text{ und } \mathcal{B}\big(P(t_1, \dots, t_n)\big) = 1 \Big\}$$

Dann gilt für alle variablen- und gleichungslosen Klauseln γ:

$$\mathcal{A} \models \gamma \iff \mathcal{B}(\gamma) = 1$$

Also haben wir insbesondere $\mathcal{A} \models \Gamma$, d.h. Γ ist erfüllbar im prädikatenlogischen Sinn. $\square$

Aus dem Satz auf Folie 6.13 und der obigen Beobachtung erhalten wir:

Satz

Sei Γ Menge von variablen- und gleichungslosen Klauseln. Dann gilt

$$\Gamma \text{ unerfüllbar} \iff \Gamma \vdash_{\mathsf{Res}} \Box\,.$$

Sind alle Klauseln in Γ sogar Hornklauseln, so haben wir

$$\Gamma \text{ unerfüllbar} \iff \Gamma \vdash_{\mathsf{Horn}} \Box\,.$$

Wir wollen jetzt beliebige gleichungslose Klauseln betrachten.

Definition

Sei $\varphi = \forall x_1 \ldots \forall x_m \bigvee_{1 \leq i \leq m} \lambda_i$ eine Klausel und σ eine Substitution. Ist $\lambda_i \sigma$ variablenlos für alle $1 \leq i \leq m$, so heißt

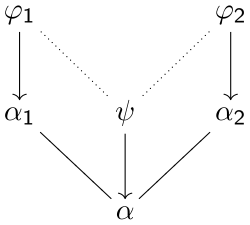
$$\bigvee_{1 \leq i \leq m} \lambda_i \sigma = \left(\bigvee_{1 \leq i \leq m} \lambda_i \right) \sigma$$

eine Grundinstanz von φ.

Idee

Betrachte gleichungslose Klauseln φ_1 und φ_2 als symbolische Darstellungen der Mengen $G(\varphi_1)$ bzw. $G(\varphi_2)$ ihrer Grundinstanzen und berechne aus zwei gleichungslosen Klauseln φ_1 und φ_2 eine gleichungslose Klausel ψ, so daß $G(\psi)$ die Menge der Resolventen von Grundinstanzen $\alpha_1 \in G(\varphi_1)$ und $\alpha_2 \in G(\varphi_2)$ ist.

Veranschaulichung:



$\cdots$: prädikatenlogische Resolution

—: aussagenlogische Resolution

$\downarrow$: Substitution/Grundinstanz

Disclaimer Ganz wird dies nicht funktionieren, aber doch hinreichend gut.

Beispiel: Betrachte die gleichungslosen Klauseln

$$\varphi_1 = \forall x \left(P\big(f(x)\big) \vee \neg R(x) \right) \text{ und } \varphi_2 = \forall y, z \left(R\big(g(y)\big) \vee R(z) \right),$$

die für die Mengen ihrer Grundinstanzen

$$P\big(f(t)\big) \vee \neg R(t) \text{ bzw. } R\big(g(t_1)\big) \vee R(t_2)$$

stehen (hierbei sind t, t_1 und t_2 beliebige variablenlose Terme).

Seien t, t_1 und t_2 variablenlose Terme, $\alpha_1 = P\big(f(t)\big) \vee \neg R(t)$ und $\alpha_2 = R\big(g(t_1)\big) \vee R(t_2)$.

- Mit $t = g(t_1) = t_2$ erhält man die Resolvente $\alpha = P\Big(f\big(g(t_1)\big)\Big)$.
- Mit $t = g(t_1) \neq t_2$ erhält man die Resolvente $\alpha = P\Big(f\big(g(t_1)\big)\Big) \vee R(t_2)$.
- $t = t_2 \neq g(t_1)$ führt zur Resolvente $\alpha = P\big(f(t_2)\big) \vee R\big(g(t_1)\big)$.

Zur Realisierung der Idee von Folie 12.9 benötigen wir die Begriffe „verallgemeinerte Substitution“, „Unifikator“ und „allgemeinster Unifikator“, diese werden wir im Rest dieser Vorlesung einführen und untersuchen; die „prädikatenlogische Resolvente“ wird in der folgenden Vorlesung definiert werden.

Substitutionen

Eine verallgemeinerte Substitution σ ist eine Abbildung der Menge der Variablen in die Menge aller Terme, so daß nur endlich viele Variable x existieren mit $\sigma(x) \neq x$.

Sei $\mathrm{Def}(\sigma) = \{x \text{ Variable} \mid x \neq \sigma(x)\}$ der Definitionsbereich der verallgemeinerten Substitution σ.

Für einen Term t definieren wir den Term $t\,\sigma$ (Anwendung der verallgemeinerten Substitution σ auf den Term t) wie folgt induktiv:

- $x\,\sigma = \sigma(x)$
- $\big[f(t_1, \ldots, t_k)\big]\,\sigma = f(t_1\,\sigma, \ldots, t_k\,\sigma)$ für Terme $t_1, \ldots, t_k$, $f \in \mathrm{Fun}$ und $k = \mathrm{ar}(f)$

Für eine atomare Formel $\alpha = P(t_1, \ldots, t_k)$ (d.h. $P \in \mathrm{Rel}$, $\mathrm{ar}(P) = k$, $t_1, \ldots, t_k$ Terme) sei

$$\alpha\,\sigma \quad = \quad P(t_1\,\sigma, \ldots, t_k\,\sigma)$$

Verknüpfung von verallgemeinerten Substitutionen: Sind σ_1 und σ_2 verallgemeinerte Substitutionen, so definieren wir eine neue verallgemeinerte Substitution $\sigma_1\sigma_2$ durch $(\sigma_1\sigma_2)(x) = (x\,\sigma_1)\,\sigma_2$.

Beispiel

Sei x Variable und t Term. Dann ist σ mit

$$\sigma(y) = \begin{cases} t & \text{falls } x = y \\ y & \text{sonst} \end{cases}$$

eine verallgemeinerte Substitution. Für alle Terme s und alle atomaren Formeln α gilt

$$s\,\sigma = s[x := t] \text{ und } \alpha\,\sigma = \alpha[x := t]\,.$$

Substitutionen sind also ein Spezialfall der verallgemeinerten Substitutionen.

Beispiel: Die verallgemeinerte Substitution σ mit $\mathrm{Def}(\sigma) = \{x, y, z\}$ und

$$\sigma(x) = f\big(h(x')\big), \quad \sigma(y) = g\big(a, h(x')\big), \quad \sigma(z) = h(x')$$

ist gleich der verallgemeinerten Substitution

$$\begin{aligned} & \Big[x := f\big(h(x')\big)\Big] \Big[y := g\big(a, h(x')\big)\Big] \big[z := h(x')\big] \\ = \quad & \big[x := f(z)\big] \big[y := g(a, z)\big] \big[z := h(x')\big] . \end{aligned}$$

Es kann sogar jede verallgemeinerte Substitution σ als Verknüpfung von Substitutionen der Form $[x := t]$ geschrieben werden.

Vereinbarung: Wir sprechen ab jetzt nur von „Substitutionen“, auch wenn wir „verallgemeinerte Substitutionen“ meinen.

Unifikator/Allgemeinster Unifikator

Definition

1. Ein Unifikator eines Paars von Termen (s, t) ist eine Substitution σ mit $s\,\sigma = t\,\sigma$.
2. Ein Unifikator einer Menge $E = \{(s_i, t_i) \mid 1 \leq i \leq n\}$ von Termpaaren ist eine Substitution σ mit $s_i\,\sigma = t_i\,\sigma$ für alle $1 \leq i \leq n$.
3. Ein Unifikator eines Paars (α, β) von Atomformeln ist eine Substitution σ mit $\alpha\,\sigma = \beta\,\sigma$.
4. Ein allgemeinster Unifikator von X ist ein Unifikator σ von X, so daß für jeden Unifikator τ von X eine Substitution σ' existiert mit $\tau = \sigma\,\sigma'$.

Existiert ein Unifikator?

	Ja	Nein
$\Big(P\big(f(x)\big), P\big(g(y)\big)\Big)$		
$\Big(P(x), P\big(f(y)\big)\Big)$		
$\Big\{\big(x, f(u)\big), \big(f(y), z\big)\Big\}$		
$\Big\{\big(x, f(u)\big), \big(f(y), f(z)\big)\Big\}$		
$\Big\{\big(x, f(y)\big), \big(f(x), y\big)\Big\}$		
$\Big\{\big(x, f(y)\big), \big(g(x), z\big), \big(g^2(x), g(z)\big)\Big\}$		

Zum allgemeinsten Unifikator

Eine Variablenumbenennung ist eine Substitution ρ, die $\mathrm{Def}(\rho)$ injektiv in die Menge der Variablen abbildet.

Lemma

Sind σ_1 und σ_2 allgemeinste Unifikatoren von X, so existiert eine Variablenumbenennung ρ mit $\sigma_2 = \sigma_1\,\rho$.

Beweis:

σ_1 und σ_2 allgemeinste Unifikatoren
$\Longrightarrow$ es gibt Substitutionen τ_1 und τ_2 mit $\sigma_1\,\tau_1 = \sigma_2$ und $\sigma_2\,\tau_2 = \sigma_1$.

Definiere eine Substitution ρ durch:

$$\rho(y) = \begin{cases} y\tau_1 & \text{falls es } x \text{ gibt, so daß } y \text{ in } x\sigma_1 \text{ vorkommt} \\ y & \text{sonst} \end{cases}$$

Wegen $\mathrm{Def}(\rho) \subseteq \mathrm{Def}(\tau_1)$ ist $\mathrm{Def}(\rho)$ endlich, also ρ eine Substitution.

- Für alle Variablen x gilt dann

$$x\sigma_1\rho = x\sigma_1\tau_1 = x\sigma_2$$

  und daher $\sigma_2 = \sigma_1\rho$.

- Wir zeigen, daß $\rho(y)$ Variable und ρ auf $\mathrm{Def}(\rho)$ injektiv ist:
  Sei $y \in \mathrm{Def}(\rho)$. Dann existiert Variable x, so daß y in $x\,\sigma_1$ vorkommt.
  Es gilt

$$x\sigma_1 = x\sigma_2\tau_2 = x\sigma_1\tau_1\tau_2\,,$$

  und damit

$$y = y\tau_1\,\tau_2 = y\rho\,\tau_2 = \rho(y)\,\tau_2\,,$$

  d.h. $\rho(y)$ ist Variable, die Abbildung $\rho\colon \mathrm{Def}(\rho) \to \{z \mid z \text{ Variable}\}$ ist invertierbar (durch τ_2) und damit injektiv. $\square$

Alle allgemeinsten Unifikatoren sind also sehr ähnlich, aber wann gibt es überhaupt einen und kann man ggf. einen solchen berechnen?

Beobachtungen

(B1) σ ist genau dann Unifikator von $\big(P(s_1,\ldots,s_k), P(t_1,\ldots,t_k)\big)$ bzw. $\big(f(s_1,\ldots,s_k), f(t_1,\ldots,t_k)\big)$, wenn σ Unifikator von $\big\{(s_1,t_1),(s_2,t_2),\ldots,(s_k,t_k)\big\}$ ist.

(B2) Sei x eine Variable und t ein Term.
Kommt x in t nicht vor, so ist $[x := t]$ ein allgemeinster Unifikator von (x,t).
Kommt x in t vor und gilt $x \neq t$, so existiert kein Unifikator von (x,t).

(B3) Seien $X \subseteq E$ Mengen von Termpaaren und sei σ ein allgemeinster Unifikator von X.
Eine Subsitution τ ist Unifikator von E genau dann, wenn die Menge

$$(E \setminus X)\,\sigma = \big\{(s_1\,\sigma, s_2\,\sigma) \,\big|\, (s_1,s_2) \in E \setminus X\big\}$$

einen Unifikator σ' mit $\tau = \sigma\,\sigma'$ hat.

Unifikationsalgorithmus

Eingabe: endliche Menge von Termpaaren E_0

Sei id die Substitution mit $\mathrm{id}(x) = x$ für alle Variable x.

Setze $E = E_0$ und $\sigma = \mathrm{id}$.
solange möglich, mache eine der folgenden Transformationen:

(1) wähle $(t, t) \in E$ und setze $E := E \setminus \{(t, t)\}$.

(2) wähle $(s, t) = \big(f(s_1, \ldots, s_k), f(t_1, \ldots, t_k)\big) \in E$ und setze $E := E \setminus \{(s, t)\} \cup \{(s_i, t_i) \mid 1 \leq i \leq n\}$.

(3) wähle $(x, t) \in E$, wobei x nicht in t vorkommt, und setze $E := \Big(E \setminus \{(x, t)\}\Big)[x := t]$ und $\sigma := \sigma\,[x := t]$.

(4) wähle $(s, x) \in E$, wobei x nicht in s vorkommt, und setze $E := \Big(E \setminus \{(s, x)\}\Big)[x := s]$ und $\sigma := \sigma\,[x := s]$.

if $E = \emptyset$
then Ausgabe „σ ist allgemeinster Unifikator von E_0“
else Ausgabe „E_0 hat keinen Unifikator“

Beispiel

$$E_0 = \{(x, f(y)), (g(x), z), (g^2(x), g(z))\}$$

Modifikation (3) mit $(x, t) = (x, f(y))$:
$E = \{(gf(y), z), (g^2f(y), g(z))\}, \quad \sigma = [x := f(y)]$

Modifikation (2) mit $(s, t) = (g^2f(y), g(z))$:
$E = \{(gf(y), z)\}, \quad \sigma = [x := f(y)]$

Modifikation (4) mit $(s, x) = (gf(y), z)$:
$E = \emptyset \quad \sigma = [x := f(y)]\,[z := gf(y)]$

Es gilt

$$E_0\,\sigma = \Big\{\big(f(y), f(y)\big), \big(gf(y), gf(y)\big), \big(g^2f(y), g^2f(y)\big)\Big\},$$

d.h. σ ist tatsächlich ein Unifikator von E_0.

Beispiel

$E_0 = \{(x, f(y)), (f(x), y)\}$

Modifikation (3) mit $(x, t) = (x, f(y))$:
$E = \{(f^2(y), y)\}$, $\sigma = [x := f(y)]$

Hier sind keine weiteren Modifikationen möglich. Wegen $E \neq \emptyset$ behauptet der Unifikationsalgorithmus, daß E_0 keinen Unifikator hat (und tatsächlich gibt es auch keinen).

Satz

Bei Eingabe einer Menge E_0 entscheidet der Unifikationsalgorithmus, ob E_0 einen Unifikator hat oder nicht. In positiven Fall gibt er einen allgemeinsten Unifikator aus.

Beweis: siehe Zusatzmaterial auf Folien 12.25ff.

Bemerkung

Insbesondere hat jede unifizierbare Menge E_0 von Termpaaren einen allgemeinsten Unifikator (und alle allgemeinsten Unifikatoren von E_0 unterscheiden sich nur durch Variablenumbenennungen).

Zusammenfassung 12. Vorlesung

in dieser Vorlesung neu

- Grundresolution, d.h. Unerfüllbarkeitstest für Mengen variablen- und gleichungsloser Klauseln
- Unifikation (Vorbereitung allgemeine prädikatenlogische Resolution)

kommende Vorlesung

- allgemeine prädikatenlogische Resolution, d.h. Unerfüllbarkeitstest für Mengen gleichungsloser Klauseln

Zusatzmaterial

Behauptung

Beim Eintritt in die Schleife und beim Austritt aus der Schleife gilt folgende Invariante:

$$\tau \text{ unifiziert } E_0 \iff \text{es gibt } \sigma' \text{ mit } \tau = \sigma\,\sigma' \text{ und } \sigma' \text{ unifiziert } E.$$

Beweis: Beim ersten Eintritt in die Schleife gilt Invariante wegen $(E, \sigma) = (E_0, \mathrm{id})$.

Gelte nun Invariante für (E_1, σ_1) und sei (E_2, σ_2) Ergebnis eines Schleifendurchlaufs, d.h. einer der Modifikationen (1)-(4).

- Anwendung der Modifikation (1): (E_2, σ_2) erfüllt Invariante, da $\sigma_2 = \sigma_1$ und da $E_2 = E_1 \setminus \{(t, t)\}$ und E_1 dieselben Unifikatoren haben.
- Anwendung der Modifikation (2): (E_2, σ_2) erfüllt Invariante, da $\sigma_2 = \sigma_1$ und da E_2 und E_1 nach Beobachtung (B1) von Folie 12.19 dieselben Unifikatoren haben.

- Anwendung der Modifikation (3): Sei τ beliebige Substitution.

  Nach IV unifiziert τ die Menge E_0 genau dann, wenn es eine Substitution σ' gibt mit $\tau = \sigma\,\sigma'$, die E_1 unifiziert.

  Nach Beobachtungen (B2) und (B3) von Folie 12.19 unifiziert σ' die Menge E_1 genau dann, wenn es Subsitution σ'' gibt mit $\sigma' = [x := t]\,\sigma''$, die $\big(E_1 \setminus \{(x,t)\}\big)[x := t] = E_2$ unifiziert.

  also: τ unifiziert E_0 gdw. es Substitution σ'' gibt mit $\tau = \underbrace{\sigma\,[x := t]}_{=\sigma_2}\,\sigma''$, die E_2 unifiziert.

(4) symmetrisch

□

Behauptung

Wenn, bei Eingabe von E_0, der Unifikationsalgorithmus die Substitution σ ausgibt, so ist σ ein allgemeinster Unifikator von E_0.

Beweis:

Da der Algorithmus σ ausgibt, erfüllt $(\emptyset, \sigma)$ die Invariante. Also gilt für alle Substitutionen τ:

$$\begin{aligned} \tau \text{ unifiziert } E_0 \quad &\iff \quad \exists \sigma' \colon \tau = \sigma\,\sigma' \text{ und } \sigma' \text{ unifiziert } \emptyset \\ &\iff \quad \exists \sigma' \colon \tau = \sigma\,\sigma' \end{aligned}$$

σ ist also tatsächlich ein allgemeinster Unifikator. $\square$

Behauptung

Wenn, bei Eingabe von E_0, der Unifikationsalgorithmus ausgibt, es gäbe keinen Unifikator, so ist E_0 tatsächlich nicht unifizierbar.

Beweis:

Da der Algorithmus behauptet, es gäbe keinen Unifikator, existieren (E, σ) mit $E \neq \emptyset$, die die Invariante erfüllen und keine der Modifikationen (1)-(4) erlauben. Wegen $E \neq \emptyset$ existiert also ein Paar $(s, t) \in E$. Da keine Modifikation anwendbar ist, gelten die folgenden Aussagen:

- Falls $s = f(s_1, \dots, s_k)$ und $t = g(t_1, \dots, t_\ell)$, so gilt $f \neq g$.
- Falls s Variable ist, so kommt s in t vor und $s \neq t$.
- Falls t Variable ist, so kommt t in s vor und $s \neq t$.

In all diesen Fällen hat (s, t) keinen Unifikator. Also hat E keinen Unifikator. Da (E, σ) die Invariante erfüllt, hat also auch E_0 keinen Unifikator. □

Behauptung

Der Unifikationsalgorithmus terminiert bei Eingabe von E_0.

Beweis:

Für eine Menge E von Termpaaren sei die Norm $||E||$ die Summe der Größe aller Terme:

$$||E|| = \sum_{(s,t)\in E} |s| + |t| \,.$$

In jedem Schleifendurchlauf sinkt

- die Anzahl der vorkommenden Variablen (Modifikationen (3) und (4)) oder
- die Norm der Formelmenge, wobei die Anzahl der vorkommenden Variablen nicht steigt (Modifikationen (1) und (2)).

Da die Anzahl der vorkommenden Variablen nur endlich oft sinken kann, und da, von (E, σ) ausgehend, nur $||E||$ oft die Modifikationen (1) und (2) angewandt werden können, terminiert der Algorithmus. $\square$