Logika és informatikai alkalmazásai

Wednesday 17th February, 2016, 09:03

A logika rövid története

A logika rövid története

Ókor

- **Triviális**: A trivium szóból származik
  trivium (tri+via = három út): nyelvtan, retorika, logika
  a trivium az alapja a quadrivium (aritmetika, geometria, zene, asztronómia) megismerésének.
- **Szofisták**: formális érvelés, paradoxonok
  Hazug paradoxon: Én most hazudok.
  Dolgozatírás paradoxona: A jövő hét valamelyik napján dolgozatot írtok. Nem mondom meg, melyik napon, csak azt, hogy meg fogtok lepődni.

Ókor

- **Axiomatikus módszer**: Euklidesz
  Geometriai tételeket tisztán logikai úton axiómákból bizonyított, a geometria axiomatikus felépítése.
  Néhány euklideszi axióma:
  - Bármely két ponton át húzható egyenes.
  - Minden középpontból minden sugárral lehet kört rajzolni.
  - (**Párhuzamossági axióma**) Ha két egyenest úgy metsz egy harmadik egyenes, hogy a metsző egyenes egyik oldalán keletkező szögek összege kisebb 180 foknál, akkor az első két egyenes is metszi egymást.
    Ekvivalens alak: Bármely egyeneshez, bármely rajta kívül fekvő ponton át legfeljebb egy párhuzamos egyenes húzható.

A logika rövid története

17-18. század: Leibniz

Logika tanulmányozására matematikai módszereket javasolt.
Univerzális problémamegoldó gépies eljárás gondolata.

19. század közepe – 19. század vége

A logika algebraizálása: Boole, Schröder, De Morgan, Pierce
Logikai fogalmakat algebrai fogalmakkal modelleztek.
Boole algebra, relációalgebra

A logika rövid története

19. század vége – 20. század első fele

- Ellentmondások az analízisben, naiv halmazelméletben
  - Cauchy ,,tétele" folytonos függvénysor összegéről
  - Russel paradoxona: Az összes halmazok H halmazának számossága megegyezik hatványhalmazának számosságával, hiszen H tartalmazza minden részhalmazát.
  - Az összes, önmagukat nem tartalmazó halmazok halmaza.
- A logika mint a matematika formális nyelve (bizonyítások pontossága).
- Frege formális rendszere (formális nyelv, levezetési szabályok) és alkalmazása az aritmetikára.
- Russell-Whitehead: Principia Mathematica (1910–13). A matematika addigi ismeretei nagy részének axiomatikus tárgyalása a formális logika nyelvén. A halmazelméleti ellentmondások feloldása az osztályfogalmat bevezető formális rendszerben.

A logika rövid története

- Hilbert programja: az egész matematika axiomatikus megalapozása és konzisztenciájának bizonyítása véges eszközökkel. Hilbert kalkulus: 1920.
- Gödel teljességi tétele.
- Gödel nemteljességi tételei.
  1. Ha egy axiómarendszer elegendően erős (kifejező) és ellentmondástalan, akkor mindig lesz olyan állítás, hogy sem ő, sem tagadása nem igazolható az axiómákból.
  2. Egy axiómarendszer ellentmondástalansága általában nem bizonyítható az axiómarendszeren belül.
- Hilbert programja megvalósíthatatlan.
- Church-Turing kiszámíthatóság (1930-as évek).
  Church tétele: Az elsőrendű logika eldönthetetlen.
  Az aritmetika (a természetes számok elsőrendű elmélete) eldönthetetlen.

A logika rövid története

20. század közepétől: Logika a számítástudomány jegyében

- Kombinatorikus és szekvenciális áramkörök tervezése.
- Automaták és formális nyelvek elmélete.
- Adatbázisok és lekérdező nyelvek.
- Logikai programozás.
- Programtervezés.
- Rendszerek verifikációja.
- Mesterséges intelligencia (szakértői rendszerek, gépi tanulás).
- Bonyolultságelmélet.
- Programozási nyelvek szemantikájának elmélete.

Az előadás felépítése

Felépítés

- Predikátumkalkulus és ítéletkalkulus.
- A logikai programozás alapjai.
- Heterogén és másodrendű logikák.
- Rendszerek specifikációja és verifikációja:
  - Temporális logikák.
  - Hoare kalkulus.

Logikai rendszerek

Főbb komponensek és kérdések

- Modellek.
- Szintaxis: formulák.
- Szemantikus fogalmak: mikor elégül ki (érvényes) egy formula egy modellben, . . .
- Bizonyításelmélet (formális rendszerek).
- Helyesség és teljesség.
- Algoritmikus kérdések.

Az elsőrendű nyelv modelljei

Elsőrendű struktúrák komponensei

- Egy nemüres halmaz, az **univerzum**.
- Az univerzumon értelmezett **függvények** és **relációk** (vagy **predikátumok**).

Minden függvény felfogható relációként.

Példa: Irányított gráfok

- **Csúcsok** (nemüres) halmaza: V
- **Él reláció**: $E \subseteq V^2$ (vagy $E : V^2 \to \{0, 1\}$)

Az elsőrendű nyelv modelljei

Példa: Természetes számok struktúrája

- Természetes számok $\{0, 1, \ldots\}$ halmaza: $\mathbb{N}$
- A **rákövetkezés** művelete: $' : \mathbb{N} \to \mathbb{N}$
- Az **összeadás** és **szorzás** műveletei: $+, \cdot : \mathbb{N}^2 \to \mathbb{N}$
- A 0 konstans: $0 : \mathbb{N}^0 \to \mathbb{N}$ (vagy $0 \in \mathbb{N}$)
- A **rendezési reláció**: $<\subseteq \mathbb{N}^2$ (vagy $<: \mathbb{N}^2 \to \{0, 1\}$)

Példa: Valós számok struktúrája

- Valós számok halmaza: $\mathbb{R}$
- Az **összeadás**, **szorzás** és **kivonás** műveletei: $+, \cdot, - : \mathbb{R}^2 \to \mathbb{R}$
- A $0, 1 \in \mathbb{R}$ konstansok
- A rendezési reláció: $<\subseteq \mathbb{R}^2$

Az elsőrendű nyelv szintaxisa

Jelkészlet

1. Elsőrendű változók, vagy individuum változók: $x, y, \ldots, x_1, y_1, \ldots$
2. Függvényjelek, vagy függvényszimbólumok: $f, g, \ldots, f_1, g_1, \ldots$
3. Predikátumjelek, predikátumszimbólumok, vagy relációszimbólumok: $p, q, r, \ldots, p_1, q_1, r_1, \ldots$
4. Logikai jelek: $\wedge, \vee, \rightarrow, \leftrightarrow, \neg, \uparrow, \downarrow, \exists, \forall$
5. Elválasztó jelek: $)$, $($ és ,.

A változók halmaza megszámlálhatóan végtelen, a függvény- és predikátumszimbólumok halmaza véges vagy megszámlálhatóan végtelen.

Minden függvényszimbólumra és predikátumszimbólumra adott a szimbólum **rangja**, vagy **aritása**, amely nemnegatív egész szám. 0 aritású függvényjel: **konstans**, vagy **konstansszimbólum**.

Az elsőrendű nyelv szintaxisa

Az **egyenlőséges** elsőrendű logikában egy bináris relációszimbólum kitüntetett: $=$.

Definíció

A **termek** halmaza a legszűkebb olyan halmaz, melyre teljesül:

- Minden változó term.
- Ha $t_1, \ldots, t_n$ termek, f pedig n-rangú függvényjel, akkor $f(t_1, \ldots, t_n)$ is term. ($n = 0$ esetén ez maga az f konstansjel.)

Példa

$f(g(x, h(y)), c)$, ahol f, g 2-rangú függvényjelek, h 1-rangú függvényjel, c konstansjel, x, y változók.

Egy term **alapterm**, ha nem fordul elő benne változó.

Az elsőrendű nyelv szintaxisa

Állítás

Minden term egyértelműen olvasható, azaz vagy változó, vagy egyértelműen írható $f(t_1, \ldots, t_n)$ alakban, ahol f függvényjel, $t_1, \ldots, t_n$ termek.

Megjegyzés

Az $f(t_1, \ldots, t_n)$ term a **lengyel jelölésben** $ft'_1 \ldots t'_n$, ahol $t'_1, \ldots, t'_n$ rendre a $t_1, \ldots, t_n$ lengyel jelölése.
Fordított lengyel jelölésben $t''_1 \ldots t''_n f$, ahol $t''_1, \ldots, t''_n$ rendre a $t_1, \ldots, t_n$ fordított lengyel jelölése.
Egy további reprezentáció: **fa reprezentáció**.
Példákban gyakran használunk **infix** írásmódot is, pl. $t + t'$.

Definíció

- **Atomi formula** egy $p(t_1, \ldots, t_n)$ alakú kifejezés, ahol p egy n-rangú predikátumszimbólum, $t_1, \ldots, t_n$ pedig termek. (Ez maga a p jel, ha $n = 0$.)
- A **formulák** halmaza a legszűkebb olyan halmaz, melyre teljesül:
  1. Minden atomi formula egyben formula is.
  2. $\uparrow, \downarrow$ formulák. Ha F, G formulák, akkor $(F \wedge G)$, $(F \vee G)$, $(F \to G)$, $(F \leftrightarrow G)$ és $(\neg F)$ is formulák.
  3. Ha F formula, x változó, akkor $(\exists x F)$ és $(\forall x F)$ is formulák.

Megjegyzés

A szokásos precedencia szabályokkal élve gyakran elhagyjuk a külső, és a feleslegessé váló zárójeleket. Egy $F \to (G \to H)$ formulát $F \to G \to H$ alakban is írunk.

Példa

$p(x, f(y)) \vee (\exists z \neg(q(x, z)))$, ahol x, y, z változók, f 1-rangú függvényjel, p, q 2-rangú predikátumjelek.

Az elsőrendű nyelv szintaxisa

Állítás

Minden formula egyértelműen olvasható.

Definíció

Legyenek F és G formulák.

- F a G **közvetlen részformulája**, ha G $(\neg F)$, $(F \bullet H)$, $(H \bullet F)$ vagy (QxF) alakú, ahol $\bullet \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ és $Q \in \{\exists, \forall\}$, H formula, x változó.
- F a G **részformulája**, ha létezik a formulák olyan $H_0, \ldots, H_n, n \geq 0$ sorozata, hogy $H_0 = G$, $H_n = F$ és H_i a H_{i-1} közvetlen részformulája, $i = 1, \ldots, n$ esetén.

Állítás

Egy F formula pontosan akkor a G formula részformulája, ha G felírható $G = uFv$ alakban alkalmas u, v szavakra, azaz ha F részszóként előfordul G-ben.

Az elsőrendű nyelv szintaxisa

Definíció

Legyen F formula, G az F egy QxH alakú részformulája. Ekkor az x H-ban való előfordulásai **kötöttek**. Az x egy F-ben való előfordulása **szabad**, ha nem kötött.

Példa

Az alábbi formulában az aláhúzott változó-előfordulások kötöttek, a többi szabad:

$$\exists x\big(p(\underline{x}, y) \vee \forall z(q(\underline{x}, y) \wedge r(\underline{x}, \underline{z}))\big) \vee q(x, x)$$

Definíció

Zárt formulának vagy **mondatnak** nevezünk egy olyan formulát, melyben egyetlen változó sem fordul elő szabadon.

Példa

$\exists x \forall y p(f(x, y))$ mondat.

Az elsőrendű nyelv szemantikája

Legyen $\mathcal{L}$ elsőrendű nyelv (mely a függvény- és predikátumszimbólumokkal adott).

Definíció

$\mathcal{L}$-típusú struktúra egy olyan $\mathcal{A} = (A, I, \varphi)$ hármas, ahol

1. A nemüres halmaz,
2. I minden f n-rangú függvényszimbólumhoz egy
$$I(f) : A^n \to A$$
függvényt, és minden n-rangú p predikátumszimbólumhoz egy
$$I(p) : A^n \to \{0, 1\}$$
predikátumot (vagy relációt) rendel,
3. φ minden változóhoz az A egy $\varphi(x)$ elemét rendeli.

Megjegyzés

- Az $n = 0$ esetben $I(f)$-et az A, $I(p)$-t a $\{0, 1\}$ halmaz egy elemével azonosíthatjuk.
- Néha a struktúra harmadik komponensét elhagyjuk, ekkor struktúra egy (A, I) pár.
- Amennyiben a nyelv egyenlőséges, kikötjük, hogy $I(=)$ az A halmazon értelmezett egyenlőségi predikátum.

Definíció

Legyen t term, $\mathcal{A} = (A, I, \varphi)$ struktúra. Ekkor a $\boldsymbol{t}$ **által az** $\boldsymbol{\mathcal{A}}$ **struktúrában jelölt** $\boldsymbol{\mathcal{A}(t) \in A}$ **elemet** az alábbi módon definiáljuk:

1. $t = x$. Ekkor $\mathcal{A}(t) = \varphi(x)$.
2. $t = f(t_1, \ldots, t_n)$. Ekkor $\mathcal{A}(t) = I(f)(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_n))$.

$I(f)$ helyett gyakran f-et, $I(p)$ helyett p-t írunk.

Példa

Legyenek $+, \times$ 2-rangú függvényjelek, $'$ 1-rangú függvényjel, $\underline{0}, \underline{1}$ konstansjelek, $<$ 2-rangú predikátumszimbólum.
$\mathcal{N} = (\mathbb{N}, I, \varphi)$, ahol

1. $\mathbb{N} = \{0, 1, 2, \dots\}$,
2. $I(')$ a rákövetkezési függvény, $I(+)$ és $I(\times)$ az összeadás és szorzás függvények, $I(\underline{0}) = 0$, $I(\underline{1}) = 1$, $I(<)$ a szokásos rendezés,
3. $\varphi(x) = 2, \varphi(y) = 3, \dots$

Ekkor:

1. $t = (x + \underline{1}) \times y$, $\mathcal{N}(t) = 9$,
2. $t = (x \times y) + \underline{0}$, $\mathcal{N}(t) = 6$,
3. $t = (\underline{0} + \underline{1}) \times \underline{1}$, $\mathcal{N}(t) = 1$.

Definíció

Legyen $\mathcal{A} = (A, I, \varphi)$ struktúra, x változó, $a \in A$. Ekkor $\mathcal{A}_{[x \mapsto a]}$ az (A, I, φ') struktúra, ahol

$$\varphi'(y) = \begin{cases} \varphi(y) & \text{ha } y \neq x \\ a & \text{különben.} \end{cases}$$

Definíció

Legyen F formula, $\mathcal{A} = (A, I, \varphi)$ struktúra. Az $\boldsymbol{F}$ **értéke az** $\boldsymbol{\mathcal{A}}$ **struktúrában** az alábbi $\mathcal{A}(F) \in \{0, 1\}$ érték:

- Ha F a $p(t_1, \ldots, t_n)$ atomi formula, akkor $\mathcal{A}(F) = I(p)(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_n))$.
- Ha $F = \downarrow$ vagy $F = \uparrow$, akkor sorrendben $\mathcal{A}(F) = 0$ ill. $\mathcal{A}(F) = 1$.
- Ha $F = G \bullet H$, ahol $\bullet \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$, akkor $\mathcal{A}(F) = \mathcal{A}(G) \bullet \mathcal{A}(H)$.
- Ha $F = \neg G$, akkor $\mathcal{A}(F) = \neg(\mathcal{A}(G))$.

Szemantika

- Ha $F = \exists x G$, akkor
$$\mathcal{A}(F) = \begin{cases} 1 & \text{ha van olyan } a \in A, \text{ hogy } \mathcal{A}_{[x \mapsto a]}(G) = 1 \\ 0 & \text{különben.} \end{cases}$$

- Ha $F = \forall x G$, akkor
$$\mathcal{A}(F) = \begin{cases} 1 & \text{ha bármely } a \in A\text{-ra } \mathcal{A}_{[x \mapsto a]}(G) = 1 \\ 0 & \text{különben.} \end{cases}$$

Megjegyzés

Amennyiben $\mathcal{A}(F) = 1$, az $\mathcal{A} \models F$ vagy az $\mathcal{A} \in \mathrm{Mod}(F)$ jelölést is használjuk, és azt mondjuk, hogy $\mathcal{A}$ **kielégíti** az F formulát, vagy **modellje** az F formulának.
Ellenkező esetben az $\mathcal{A} \not\models F$ jelölést használjuk.

Példa

Legyen $\mathcal{N} = (\mathbb{N}, I, \varphi)$ ahol $\mathbb{N}$ és I a korábban megadottak.

- Ha $\varphi(x) = 0$, akkor $\mathcal{N} \not\models \exists y(y < x)$.
- Ha $\varphi(x) = 3$, akkor $\mathcal{N} \models \exists y(y < x)$.
- Tetszőleges φ esetén $\mathcal{N}$ modellje az alábbi formulák mindegyikének:
  - $x < x + \underline{1}$, $\forall x(x < x + \underline{1})$
  - $\forall x\big(x \times x = x \ \rightarrow \ (x = \underline{0} \vee x = \underline{1})\big)$
  - $\forall x \forall y(x < y \ \vee \ y < x \ \vee \ x = y)$

Állítás

Legyen t term, F formula és legyenek $\mathcal{A} = (A, I, \varphi)$ és $\mathcal{A}' = (A, I, \varphi')$ struktúrák.

1. Ha $\varphi(x) = \varphi'(x)$ minden olyan x változóra, mely előfordul t-ben, akkor $\mathcal{A}(t) = \mathcal{A}'(t)$.
2. Ha $\varphi(x) = \varphi'(x)$ minden olyan x változóra, mely **szabadon** előfordul F-ben, akkor $\mathcal{A}(F) = \mathcal{A}'(F)$.

Következmény

A fenti jelölésekkel, $\mathcal{A}(t)$ független minden olyan változó értékétől, mely nem fordul elő t-ben. Továbbá $\mathcal{A}(F)$ független minden olyan változó értékétől, mely nem fordul elő szabadon F-ben.
Ezért ha F mondat, akkor értelmes arról beszélni, hogy $\mathcal{A} \models F$ teljesül-e egy $\mathcal{A} = (A, I)$ változó-hozzárendelés nélküli struktúrában.

Bizonyítás

1. $t = y$. Ekkor $\mathcal{A}(t) = \varphi(y) = \varphi'(y) = \mathcal{A}(t')$.
2. $t = \sigma(t_1, \ldots, t_n)$. Ekkor tetszőleges i esetén $\varphi(x) = \varphi'(x)$ minden olyan x változóra, amely t_i-ben előfordul. Ezért

$$\begin{aligned} \mathcal{A}(t) &= I(f)(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_n)) \\ &= I(f)(\mathcal{A}'(t_1), \ldots, \mathcal{A}'(t_n)) = \mathcal{A}'(t) \end{aligned}$$

Bizonyítás

1. $F = p(t_1, \ldots, t_n)$. Ekkor tetszőleges i esetén $\varphi(x) = \varphi'(x)$ minden olyan x változóra, amely t_i-ben előfordul.
$$\begin{aligned} \mathcal{A}(F) &= I(p)(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_n)) \\ &= I(p)(\mathcal{A}'(t_1), \ldots, \mathcal{A}'(t_n)) = \mathcal{A}'(F) \end{aligned}$$
2. $F = \downarrow$ vagy $F = \uparrow$. Triviális.
3. $F = G \bullet H$. Ekkor $\varphi(x) = \varphi'(x)$ minden olyan x változóra, amely szabadon előfordul G-ben vagy H-ban. Ezért
$$\mathcal{A}(F) = \mathcal{A}(G) \bullet \mathcal{A}(H) = \mathcal{A}'(G) \bullet \mathcal{A}'(H) = \mathcal{A}'(F)$$
4. $F = \neg G$. Hasonló az előző esethez.
5. $F = Qy.G$. Tetszőleges $a \in A$ esetén legyen $\mathcal{A}_{[y \mapsto a]} = (A, I, \psi_a)$ és $\mathcal{A}'_{[y \mapsto a]} = (A, I, \psi'_a)$, ekkor $\psi_a(x) = \psi'_a(x)$ valahányszor x szabadon előfordul G-ben.
$$\begin{aligned} \mathcal{A}(F) = 1 &\Leftrightarrow Qa\ \mathcal{A}_{[y \mapsto a]} = 1 \\ &\Leftrightarrow Qa\ \mathcal{A}'_{[y \mapsto a]} = 1 \Leftrightarrow \mathcal{A}'(F) = 1 \end{aligned}$$

Definíció

1. Egy F formulát **kielégíthetőnek** nevezünk, ha van modellje. Ellenkező esetben F **kielégíthetetlen**, vagy **azonosan hamis**.
2. Egy F formulát **tautológiának** (vagy **érvényesnek** vagy **azonosan igaznak**) nevezünk, ha minden struktúra kielégíti. Jelölés: $\models \boldsymbol{F}$.

Példa

- Tautológiák: $\uparrow$, $F \vee \neg F$, $F \to F$, $F \to G \to F$, ahol F, G tetszőlegesek.
- Kielégíthető formulák, melyek nem tautológiák: $(p \wedge q) \to \neg p$, $\exists x p(x)$.
- Azonosan hamis: $\downarrow$, $F \wedge \neg F$, ahol F tetszőleges.

Állítás

F akkor és csak akkor kielégíthető, ha $\neg F$ nem tautológia. F akkor és csak akkor tautológia, ha $\neg F$ azonosan hamis.

Állítás

Tetszőleges F formulára és x változóra:

1. $\models F$ akkor és csak akkor, ha $\models \forall x F$.
2. F akkor és csak akkor kielégíthető, ha $\exists x F$ az.

Tehát egy formula akkor és csakis akkor azonosan igaz, ha **univerzális lezártja** az, és akkor és csak akkor kielégíthető, ha **egzisztenciális lezártja** az.

Definíció

Azt mondjuk, hogy az F és G formulák **ekvivalensek**, ha $\mathrm{Mod}(F) = \mathrm{Mod}(G)$. Jelölés: $\boldsymbol{F \equiv G}$.

Állítás

$\equiv$ ekvivalencia-reláció.

Állítás

$\models F$ akkor és csak akkor, ha $F \equiv \uparrow$.

Állítás

$F \equiv G$ akkor és csakis akkor, ha $\models (F \leftrightarrow G)$.

Bizonyítás

$$
\begin{aligned}
& \mathrm{Mod}(F) = \mathrm{Mod}(G) \\
\Leftrightarrow \quad & \forall \mathcal{A}\ (\mathcal{A} \models F \text{ és } \mathcal{A} \models G) \text{ vagy } (\mathcal{A} \not\models F \text{ és } \mathcal{A} \not\models G) \\
\Leftrightarrow \quad & \forall \mathcal{A}\ \mathcal{A} \models ((F \wedge G) \vee (\neg F \wedge \neg G)) \\
\Leftrightarrow \quad & \forall \mathcal{A}\ \mathcal{A} \models (F \leftrightarrow G).
\end{aligned}
$$

Szemantika

- $\neg \uparrow \equiv \downarrow$, $\neg \downarrow \equiv \uparrow$, $F \wedge \uparrow \equiv F$, $F \wedge \downarrow \equiv \downarrow$, $F \vee \uparrow \equiv \uparrow$, $F \vee \downarrow \equiv F$
- $F \rightarrow \uparrow \equiv \uparrow$, $\uparrow \rightarrow F \equiv F$, $F \rightarrow \downarrow \equiv \neg F$, $\downarrow \rightarrow F \equiv \uparrow$
- $F \wedge F \equiv F$, $F \vee F \equiv F$, $F \rightarrow F \equiv \uparrow$
- $F \wedge G \equiv G \wedge F$, $F \vee G \equiv G \vee F$
- $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$, $(F \vee G) \vee H \equiv F \vee (G \vee H)$
- $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$,
  $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$
- $F \wedge \neg F \equiv \downarrow$, $F \vee \neg F \equiv \uparrow$
- $\neg\neg F \equiv F$
- $\neg(F \wedge G) \equiv \neg F \vee \neg G$, $\neg(F \vee G) \equiv \neg F \wedge \neg G$
- $F \rightarrow G \equiv \neg F \vee G$, $F \rightarrow G \equiv \neg(F \wedge \neg G)$
- $F \rightarrow G \equiv \neg G \rightarrow \neg F$
- $F \vee G \equiv \neg F \rightarrow G$, $F \wedge G \equiv \neg(F \rightarrow \neg G)$
- $F \leftrightarrow G \equiv (F \rightarrow G) \wedge (G \rightarrow F)$

1. $\neg(\forall x F) \equiv \exists x(\neg F)$ és $\neg(\exists x F) \equiv \forall x(\neg F)$.
2. $\forall x F \wedge \forall x G \equiv \forall x(F \wedge G)$ és $\exists x F \vee \exists x G \equiv \exists x(F \vee G)$.
3. Ha x nem fordul elő szabadon G-ben, akkor $Q = \exists, \forall$ esetén $QxF \wedge G \equiv Qx(F \wedge G)$ és $QxF \vee G \equiv Qx(F \vee G)$.
4. $\forall x \forall y F \equiv \forall y \forall x F$ és $\exists x \exists y F \equiv \exists y \exists x F$.

Megegyezünk abban, hogy a kvantorok erősebben kötnek, mint $\vee$, $\wedge$, $\rightarrow$ vagy $\leftrightarrow$.

Az ekvivalenciák miatt elegendő lenne a $\vee, \neg$, a $\wedge, \neg$, a $\rightarrow, \neg$ vagy a $\rightarrow, \downarrow$ jeleket, valamint valamelyik kvantort megengedni.

$\forall x(F \vee G) \equiv \forall xF \vee \forall xG$ általában **nem** teljesül.
Legyen pl. F a $\underline{0} \leq x$, G az $x \leq \underline{0}$ formula, és vegyük az egész számokat a szokásos rendezéssel.

$\exists x(F \wedge G) \equiv \exists xF \wedge \exists xG$ általában **nem** teljesül.
Legyen F a $\underline{0} < x$, G az $x < \underline{0}$ formula, és vegyük az előző struktúrát.

Lemma (Kongruencia tulajdonság)

- Ha $F \equiv F'$ és $G \equiv G'$, akkor $F \bullet G \equiv F' \bullet G'$, ahol $\bullet \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$.
- Ha $F \equiv F'$, akkor $\neg F \equiv \neg F'$.
- Ha $F \equiv F'$, akkor $QxF \equiv QxF'$, ahol $Q \in \{\exists, \forall\}$ és x változó.

Bizonyítás

- $\mathcal{A}(F \bullet G) = \mathcal{A}(F) \bullet \mathcal{A}(G) = \mathcal{A}(F') \bullet \mathcal{A}(G') = \mathcal{A}(F' \bullet G')$.
- $\mathcal{A}(\neg F) = \neg\mathcal{A}(F) = \neg\mathcal{A}(F') = \mathcal{A}(\neg F')$.
- $\mathcal{A} \models \exists x F \;\Leftrightarrow\; \exists a \in A\ \mathcal{A}_{[x \mapsto a]} \models F \Leftrightarrow$ $\exists a \in A\ \mathcal{A}_{[x \mapsto a]} \models F' \;\Leftrightarrow\; \mathcal{A} \models \exists x F'$.

Állítás

Ha az F' formula úgy áll elő az F formulából, hogy az F egy H részformuláját ekvivalens H' formulára cseréljük, akkor $F \equiv F'$.

Bizonyítás

Az F felépítése szerinti indukcióval.

- Ha H maga az F formula, akkor $F' = H'$, így $F \equiv F'$ teljesül a $H \equiv H'$ feltevés miatt.
  Ez az eset magába foglalja az indukciós alaplépést.
- Indukciós lépés. Feltehető, hogy $F \neq H$. Csak két esetet nézünk meg:

- $F = F_1 \vee F_2$. Ekkor H az F_1 vagy F_2 részformulája.
  Szimmetria miatt elegendő csak azzal az esettel foglalkozni, amikor H az F_1 részformulája. Ekkor $F' = F_1' \vee F_2$, ahol F_1' úgy áll elő F_1-ből, hogy benne egy H részformulát H'-vel kicserélünk.
  Az indukciós feltevésből: $F_1' \equiv F_1$. Az előző lemmából: $F \equiv F'$.
- $F = \exists x G$. Ekkor H a G részformulája és $F' = \exists x G'$ alakú, ahol G' úgy áll elő G-ből, hogy benne a H egy előfordulását H'-vel helyettesítjük.
  Indukciós feltevésből: $G' \equiv G$, így az előző lemmából $F' \equiv F$.

Definíció

Legyen Σ formulák egy halmaza. Azt mondjuk, hogy az $\mathcal{A}$ struktúra **kielégíti** Σ-t, vagy a Σ **modellje**, ha $\mathcal{A} \models F$ teljesül minden $F \in \Sigma$ formulára.
Jelölés: $\boldsymbol{\mathcal{A} \models \Sigma}$ vagy $\boldsymbol{\mathcal{A} \in \mathbf{Mod}(\Sigma)}$.
A Σ halmazt **kielégíthetőnek** nevezzük, ha létezik modellje.

Definíció

Legyen Σ formulák halmaza, F pedig formula. Azt mondjuk, hogy F a Σ **(logikai) következménye**, ha $\mathrm{Mod}(\Sigma) \subseteq \mathrm{Mod}(F)$, azaz valahányszor $\mathcal{A} \models \Sigma$, mindig $\mathcal{A} \models F$.
Jelölés: $\boldsymbol{\Sigma \models F}$. Amennyiben $\Sigma = \{G\}$, akkor $\Sigma \models F$ helyett $G \models F$-et is írunk.

Állítás

Σ akkor és csakis akkor kielégíthetetlen, ha $\Sigma \models \downarrow$.

Állítás

$\Sigma \models F$ akkor és csak akkor, ha $\Sigma \cup \{\neg F\}$ kielégíthetetlen.

Állítás

$F \equiv G$ akkor és csak akkor, ha $F \models G$ és $G \models F$.

Állítás

Tetszőleges F, G, H formulákra érvényesek az alábbiak:

- $\{F, F \to G\} \models G$ (leválasztás).
- $\{F, \neg G \to \neg F\} \models G$ (indirekt következtetés).
- $(F \vee G) \wedge (\neg F \vee H) \models G \vee H$ (rezolúciós következtetés).

Bizonyítás

- Ha $\mathcal{A}(F) = \mathcal{A}(F \to G) = 1$, akkor $\mathcal{A}(G) = 1$.
- Ha $\mathcal{A}(F) = \mathcal{A}(\neg G \to \neg F) = 1$, akkor $\mathcal{A}(\neg F) = 0$, így $\mathcal{A}(G) = 1$.
- Tegyük fel, hogy $\mathcal{A}(F \vee G) = \mathcal{A}(\neg F \vee H) = 1$. Ha $\mathcal{A}(G) = 0$, akkor $\mathcal{A}(F) = 1$, így $\mathcal{A}(\neg F) = 0$ és $\mathcal{A}(H) = 1$.

Formalizálás

Formalizálás

- Adott egy struktúra, vagy strukúrák egy osztálya, melyek az összes olyan mondatok, amelyek érvényesek a tekinett struktúrákban?
- Adott mondatok egy Σ halmaza, az axiómák, melyek ezek összes logikai következményei?
- **Elsőrendű elméletek**

Példa: Természetes számok elmélete, az aritmetika

- $\mathcal{N}$ a természetes számok szokásos struktúrája.
- Az $\mathcal{N}$-ben érvényes mondatok: az $\mathcal{N}$ elmélete.
- $\forall x \exists y_1 \exists y_2 \exists y_3 \exists y_4 (x = y_1^2 + y_2^2 + y_3^2 + y_4^2)$ (Lagrange tétele)
- $\forall x \exists y (y > x \wedge \text{prím}(y) \wedge \text{prím}(y + \underline{2}))$

  $$\text{prím}(x):\ x > \underline{1} \wedge \forall y \forall z (x = y \cdot z \to (y = \underline{1} \vee z = \underline{1}))$$

  (Goldbach sejtés)

Példa: félcsoportok elmélete

- Egyetlen axióma: $\forall x \forall y \forall z (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $\forall x \forall y [\forall z (x \cdot z = z \wedge z \cdot y = z)) \to x = y]$

Definíció

Mondatok egy Σ halmazát **elméletnek** nevezünk, ha valahányszor $\Sigma \models F$ egy F mondatra, akkor $F \in \Sigma$.

Definíció

Egy Σ elméletet **ellentmondástalannak** nevezünk, ha Σ kielégíthető. Különben Σ **ellentmondásos**.

Definíció

Egy ellentmondástalan Σ elmélet **teljes**, ha minden F mondatra $F \in \Sigma$ vagy $\neg F \in \Sigma$.

Állítás

Az alábbiak ekvivalensek egy Σ elméletre:

i) Σ ellentmondásos.

ii) $\Sigma \models \downarrow$.

iii) $\downarrow \in \Sigma$.

iv) Van olyan F mondat, hogy $F, \neg F \in \Sigma$.

Bizonyítás

i)$\rightarrow$ii) Ha Σ ellentmondásos, akkor $\mathrm{Mod}(\Sigma) = \emptyset$, így valahányszor $\mathcal{A} \models \Sigma$, mindig $\mathcal{A} \models \downarrow$.

ii)$\rightarrow$iii) Ha Σ elmélet és $\Sigma \models \downarrow$, akkor $\downarrow \in \Sigma$.

iii)$\rightarrow$iv) Legyen $F = \downarrow$.

iv)$\rightarrow$i) Nincs olyan $\mathcal{A}$ struktúra, melyre $\mathcal{A} \models \{F, \neg F\}$.

Állítás

Legyen $\mathcal{K}$ az $\mathcal{A} = (A, I)$ alakú struktúrák egy osztálya.
Ekkor $\mathbf{Th}(\boldsymbol{\mathcal{K}}) = \{\boldsymbol{F} : \boldsymbol{F}\ \mathbf{mondat},\ \boldsymbol{\mathcal{K}} \models \boldsymbol{F}\}$ elmélet, ahol $\mathcal{K} \models F$ azt jelöli, hogy $\mathcal{A} \models F$ minden $\mathcal{A} \in \mathcal{K}$ esetén.
Ha $\mathcal{K}$ nemüres, akkor $\mathrm{Th}(\mathcal{K})$ ellentmondástalan.
Ha $\mathcal{K} = \{\mathcal{A}\}$ egyetlen $\mathcal{A}$ struktúrából áll, akkor $\mathrm{Th}(\mathcal{K})$ teljes.
(Jelölés: $\mathrm{Th}(\mathcal{A})$.)

Bizonyítás

- Ha $\mathrm{Th}(\mathcal{K}) \models F$ az F mondatra, akkor $\mathcal{K} \models F$. Tehát $F \in \mathrm{Th}(\mathcal{K})$.
- Tegyük fel, hogy $\mathcal{K}$ nemüres, mondjuk $\mathcal{A} \in \mathcal{K}$. Akkor $\mathcal{A} \models \mathrm{Th}(\mathcal{K})$ miatt $\mathrm{Th}(\mathcal{K})$ kielégíthető.
- Minden F mondatra, $\mathcal{A}(F) = 0$ vagy $\mathcal{A}(F) = 1$. Ha $\mathcal{A}(F) = 0$, akkor $\mathcal{A}(\neg F) = 1$. Tehát $F \in \mathrm{Th}(\mathcal{A})$ vagy $\neg F \in \mathrm{Th}(\mathcal{A})$.

Definíció

Mondatok tetszőleges Σ halmazára legyen

$$\mathbf{Cons(\Sigma)} \;=\; \mathbf{\{}\boldsymbol{F}\mathbf{:}\;\boldsymbol{F}\;\mathbf{mondat,}\;\boldsymbol{\Sigma}\models\boldsymbol{F}\mathbf{\}.}$$

Világos, hogy $\mathrm{Cons}(\Sigma)$ elmélet.

Definíció

Egy T elmélet **axiomatizálható**, ha létezik mondatok olyan Σ **rekurzív** halmaza, hogy $T = \mathrm{Cons}(\Sigma)$. Ekkor Σ a T **axiómarendszere**.

Struktúrák egy $\mathcal{K}$ osztályát axiomatizálhatónak nevezzük, ha létezik mondatok olyan Σ rekurzív halmaza, melyre $\mathrm{Mod}(\Sigma) = \mathcal{K}$.

Ha Σ véges halmaz, a **véges axiomatizálhatóság** definícióját kapjuk.

Megjegyzés

Ha egy elmélet végesen axiomatizálható, akkor egyetlen mondattal is axiomatizálható.

Formalizálás

Csoportelmélet

- $\forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$
- $\forall x (x \cdot 1 = x \ \wedge \ 1 \cdot x = x)$
- $\forall x (x \cdot x^{-1} = 1 \ \wedge \ x^{-1} \cdot x = 1)$

Ha a második axiómát két axiómának tekintjük, akkor a fenti axiómarendszer **nem független**:

$$1 \cdot x = (x \cdot x^{-1}) \cdot x = x \cdot (x^{-1} \cdot x) = x \cdot 1$$

Tehát a második sorban szereplő axióma egyszerűsíthető.

Csoportelmélet másképp

- $\forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$
- $\forall x (x \cdot 1 = x \ \wedge \ 1 \cdot x = x)$
- $\forall x \exists y (x \cdot y = 1 \ \wedge \ y \cdot x = 1)$

Formalizálás

Rendezett halmazok

- $\forall x \forall y \forall z((x < y \ \wedge \ y < z) \rightarrow x < z)$
- $\forall x \neg(x < x)$
- $\forall x \forall y(x < y \ \vee \ x = y \ \vee \ y < x)$

Létezik legkisebb elem

$$\exists x \forall y(x < y \ \vee \ x = y)$$

Az $I(p)$ predikátumot kielégítő elemeknek van **legkisebb felső korlátja**

$$\exists z\big(\forall y(p(y) \rightarrow y \leq z) \ \wedge \ \forall u(\forall y(p(y) \rightarrow y \leq u) \rightarrow z \leq u)\big)$$

Itt $t \leq t'$ a $t < t' \ \vee \ t = t'$ formula helyett áll.

Formalizálás

Peano axiómák

- $\forall x(\neg x' = \underline{0})$
- $\forall x \forall y(x' = y' \to x = y)$
- $\forall x(x + \underline{0} = x)$
- $\forall x \forall y(x + y' = (x + y)')$
- $\forall x(x \cdot \underline{0} = \underline{0})$
- $\forall x \forall y(x \cdot y' = x \cdot y + x)$
- $\forall x(x \leq \underline{0} \to x = \underline{0})$
- $\forall x \forall y(x \leq y' \to (x \leq y \vee x = y'))$
- $\forall x \forall y(x < y \ \vee \ x = y \ \vee \ y < x)$
- **Indukciós axióma séma**:
  $(F(\underline{0}) \wedge \forall x(F(x) \to F(x'))) \to \forall x F(x)$, ahol $F(x)$ olyan formula, melyben legfeljebb az x változó fordul elő szabadon, és $F(\underline{0})$, $F(x')$ úgy állnak elő, hogy x helyébe $\underline{0}$-t ill. x'-t helyettesítünk (ld. később).

Állítás (**Galois kapcsolat**)

Legyenek Σ, Σ_1, Σ_2 mondatok halmazai, $\mathcal{K}$, $\mathcal{K}_1$, $\mathcal{K}_2$ struktúrák osztályai.

1. Ha $\Sigma_1 \subseteq \Sigma_2$, akkor $\mathrm{Mod}(\Sigma_1) \supseteq \mathrm{Mod}(\Sigma_2)$.
2. Ha $\mathcal{K}_1 \subseteq K_2$, akkor $\mathrm{Th}(\mathcal{K}_1) \supseteq \mathrm{Th}(\mathcal{K}_2)$.
3. $\Sigma \subseteq \mathrm{Th}(\mathcal{K})$ akkor és csak akkor, ha $\mathrm{Mod}(\Sigma) \supseteq \mathcal{K}$.
4. $\Sigma \subseteq \mathrm{Th}(\mathrm{Mod}(\Sigma))$.
5. $\mathcal{K} \subseteq \mathrm{Mod}(\mathrm{Th}(\mathcal{K}))$.
6. $\mathrm{Th}(\mathrm{Mod}(\Sigma)) = \mathrm{Th}(\mathrm{Mod}(\mathrm{Th}(\mathrm{Mod}(\Sigma))))$.
7. $\mathrm{Mod}(\mathrm{Th}(\mathcal{K})) = \mathrm{Mod}(\mathrm{Th}(\mathrm{Mod}(\mathrm{Th}(\mathcal{K}))))$.
8. Σ akkor és csak akkor elmélet, ha $\Sigma = \mathrm{Th}(\mathrm{Mod}(\Sigma))$.
9. $\mathcal{K}$ akkor és csak akkor gyengén axiomatizálható osztály, ha $\mathcal{K} = \mathrm{Mod}(\mathrm{Th}(\mathcal{K}))$.

Bizonyítás

1. Ha $\Sigma_1 \subseteq \Sigma_2$ és $\mathcal{A} \models \Sigma_2$, akkor $\mathcal{A} \models \Sigma_1$.
2. Ha $\mathcal{K}_1 \subseteq \mathcal{K}_2$ és $\mathcal{K}_2 \models F$, akkor $\mathcal{K}_1 \models F$.
3. Ha $\Sigma \subseteq \mathrm{Th}(\mathcal{K})$ és $\mathcal{A} \in \mathcal{K}$, akkor $\mathcal{A} \models \Sigma$, így $\mathcal{A} \in \mathrm{Mod}(\Sigma)$.
   Ha $\mathrm{Mod}(\Sigma) \supseteq \mathcal{K}$ és $F \in \Sigma$, akkor $\mathcal{K} \models F$, így $F \in \mathrm{Th}(\mathcal{K})$.
4. Legyen $\mathcal{K} = \mathrm{Mod}(\Sigma)$ a 3. pontban.
5. Legyen $\Sigma = \mathrm{Th}(\mathcal{K})$ a 3. pontban.
6. $\mathrm{Th}(\mathrm{Mod}(\Sigma)) \subseteq \mathrm{Th}(\mathrm{Mod}(\mathrm{Th}(\mathrm{Mod}(\Sigma))))$ a 4. pont miatt.
   $\mathrm{Mod}(\Sigma) \subseteq \mathrm{Mod}(\mathrm{Th}(\mathrm{Mod}(\Sigma)))$ az 5. pont miatt.
   Így a 2. pontból $\mathrm{Th}(\mathrm{Mod}(\mathrm{Th}(\mathrm{Mod}(\Sigma)))) \subseteq \mathrm{Th}(\mathrm{Mod}(\Sigma))$.
7. Hasonló.
8. A 6. pontból.
9. A 7. pontból.

Az ítéletkalkulus

Az ítéletkalkulus

Az elsőrendű logika azon speciális esete, amikor csak nulladrangú predikátumszimbólumok vannak, és azokból megszámlálhatóan végtelen sok van: $p, q, p_1, q_1, \ldots$.

Az elsőrendű változók, kvantorok és függvényszimbólumok feleslegessé válnak, elhagyjuk őket.

Ekkor egy struktúra: a predikátumszimbólumokat a $\{0, 1\}$ halmazba képező függvény.

Ezért a predikátumszimbólumokat **ítéletváltozóknak** is nevezzük.

Tehát modell: az ítéletváltozók egy (ki)értékelése.

Állítás

Ha F az ítéletkalkulus egy tautológiája, akkor minden olyan F' formula is tautológia, amely úgy áll elő F-ből, hogy benne a p ítéletváltozókat valamely elsőrendű nyelv tetszőleges G_p elsőrendű formuláival helyettesítjük.

Bizonyítás

Legyen $\mathcal{A}$ tetszőleges (elsőrendű) struktúra. Minden egyes p-re legyen $\mathcal{B}(p) = \mathcal{A}(G_p)$. A logikai jelek kongruencia tulajdonságából:

$$\mathcal{A}(F') = \mathcal{B}(F).$$

Így ha F tautológia, akkor F' is az.

Állítás

Legyenek F, G az ítéletkalkulus formulái. Az F', G' elsőrendű formulák álljanak úgy elő az ítéletkalkulus F és G formuláiból, hogy bennük minden egyes p ítéletváltozót valamely H_p formulával helyettesítünk. Ekkor $F \equiv G$ esetén $F' \equiv G'$.

Bizonyítás

$F \equiv G$ akkor és csak akkor, ha $\models (F \leftrightarrow G)$, és $F' \equiv G'$ akkor és csak akkor, ha $\models (F' \leftrightarrow G')$. Használjuk az előző állítást.

Állítás

Legyen Σ az ítéletkalkulus formuláinak halmaza, F az ítéletkalkulus formulája. Minden egyes p ítéletváltozóra legyen G_p valamely elsőrendű nyelv egy formulája. Σ' és F' álljon elő Σ-ból és F-ből úgy, hogy p helyébe mindenhol G_p-t helyettesítünk. Ekkor $\Sigma \models F$ esetén $\Sigma' \models F'$.

Normálformák az ítéletkalkulusban

Definíció

- **Literálnak** nevezünk minden p vagy $\neg p$ alakú formulát, ahol p változó. Ezen belül p **pozitív**, $\neg p$ pedig **negatív** literál.
- Egy ℓ literál **ellentettje** az alábbi literál:

$$\overline{\ell} = \begin{cases} \neg p & \text{ha } \ell = p \\ p & \text{ha } \ell = \neg p. \end{cases}$$

- **Konjunktív normálformán** egy

$$\wedge_{i=1}^{n} \vee_{j=1}^{m_i} \ell_{i,j}$$

alakú formulát, **diszjunktív normálformán** pedig egy

$$\vee_{i=1}^{n} \wedge_{j=1}^{m_i} \ell_{i,j}$$

alakú formulát értünk, ahol $\ell_{i,j}$ literál, $i = 1, \ldots, n$, $j = 1, \ldots, m_i$.

Megjegyzés

- Az üres diszjunktív normálforma azonosan hamis, az üres konjunktív normálforma azonosan igaz. Diszjunktív normálforma üres tagja azonosan igaz, konjunktív normálforma üres tagja azonosan hamis.
- Kiköthetjük, hogy az egy tagban szereplő literálok páronként különböznek, és hogy a tagok páronként különböznek.
- A $q_1, \ldots, q_n$ változók feletti normálformára kiköthetjük, hogy minden tagban minden q_i változó pontosan egyszer fordul elő (**teljes** normálforma).
- Általában azonosítunk két normálformát, ha csak a tagok sorrendjében és/vagy tagonként a literálok sorrendjében különböznek.

Tétel

Minden formulához létezik ekvivalens konjunktív és diszjunktív normálforma.

Bizonyítás

1. A formula felépítése szerinti indukcióval.
2. Adott F formulára először fejezzük ki az előforduló $\rightarrow$ és $\leftrightarrow$ műveleteket a $\vee$, $\wedge$, $\neg$ műveletekkel, majd küszöböljük ki a konstansokat.
   Ezek után vigyük a $\neg$ jeleket a változók elé és eliminájuk a többszörös negációkat.
   Végül alkalmazzuk a disztributív azonosságokat.
3. Alkalmazzuk az ,,igazságtábla" módszert.

Boole függvények

Definíció

Tegyük fel, hogy az F formula változói a $\{p_{i_1}, \ldots, p_{i_n}\}$, $n \geq 1$ halmazba esnek, ahol $i_1 < \cdots < i_n$. Ekkor F egy n-változós Boole függvényt **indukál**:

$$\begin{aligned} f : \{0,1\}^n &\rightarrow \{0,1\} \\ f(x_1, \ldots, x_n) &= \mathcal{A}(F), \end{aligned}$$

ahol $\mathcal{A}$ **tetszőleges** olyan értékelés, melyre $\mathcal{A}(p_{i_j}) = x_j$, $j = 1, \ldots, n$.

Megjegyzés

f független azon x_j változóitól, melyekre p_{i_j} nem fordul elő F-ben.

Példa

- $F = p_1$, $n = 2$: $f(x_1, x_2) = x_1$
- $F = p_1 \vee (\neg p_1 \leftrightarrow p_2)$, $n = 2$: $f(x_1, x_2) = x_1 \vee x_2$
- $F = p_1 \vee \neg p_1$, $n = 1$: $f(x_1) = 1$

Tétel

Minden Boole függvény indukálható valamely formulával.

Bizonyítás

Minden igazságtáblához készíthető konjunktív, vagy diszjunktív normálforma.

Következmény

Az alábbi rendszerek **teljesek**:

- $\{\vee, \wedge, \neg\}$
- $\{\wedge, \neg\}$ és $\{\vee, \neg\}$
- $\{\rightarrow, \downarrow\}$

Definíció

Tetszőleges $x, y \in \{0, 1\}$ esetén legyen

$$x \mid y \quad = \quad \neg(x \wedge y) \quad = \quad \neg x \vee \neg y$$

$$x \mid\mid y \quad = \quad \neg(x \vee y) \quad = \quad \neg x \wedge \neg y$$

Tétel

Egy • kétváltozós Boole függvény akkor és csak akkor alkot önmagában teljes rendszert, ha megegyezik a $\mid$ és $\mid\mid$ függvények valamelyikével.

Elegendőség bizonyítása

$$\neg x = x|x \quad x \wedge y = \neg(x|y) = (x|y)|(x|y)$$

Szükségesség bizonyítása

Tegyük fel, hogy $\bullet$ önmagában teljes.

- Ha $1 \bullet 1 = 1$, akkor minden egyváltozós f kifejezhető függvényre fennáll, hogy $f(1) = 1$. Ezért $1 \bullet 1 = 0$. Hasonlóan, $0 \bullet 0 = 1$.
- Ha $1 \bullet 0 = 1$ és $0 \bullet 1 = 0$, akkor $x \bullet y = \neg y$ és csak olyan kétváltozós függvény fejezhető ki, mely csak az egyik argumentumától függ.
- Szimmetrikusan, ha $1 \bullet 0 = 0$ és $0 \bullet 1 = 1$, akkor $x \bullet y = \neg x$, és így ismét ellentmondáshoz jutunk.
- Így $1 \bullet 0 = 0 \bullet 1 = 1$, azaz $\bullet = |$, vagy $1 \bullet 0 = 0 \bullet 1 = 0$, amikor $\bullet = ||$.

Az ítéletkalkulus kompaktsági tétele

A kompaktsági tétel

Tétel

Formulák egy halmaza akkor és csak akkor kielégíthető, ha minden **véges** részhalmaza kielégíthető.

Következmény

Egy F formula akkor és csak akkor következménye formulák egy Σ halmazának, ha a Σ egy **véges** részhalmazának következménye.

A következmény bizonyítása

$$\begin{aligned}
\Sigma \models F \quad &\Leftrightarrow \quad \Sigma \cup \{\neg F\} \text{ nem kielégíthető} \\
&\Leftrightarrow \quad \exists \Sigma_0 \subseteq \Sigma \cup \{\neg F\} \text{ véges } \Sigma_0 \text{ nem kielégíthető} \\
&\Leftrightarrow \quad \exists \Sigma_0 \subseteq \Sigma \text{ véges } \Sigma_0 \cup \{\neg F\} \text{ nem kielégíthető} \\
&\Leftrightarrow \quad \exists \Sigma_0 \subseteq \Sigma \text{ véges } \Sigma_0 \models F.
\end{aligned}$$

A kompaktsági tétel

Kőnig lemmája

Ha egy végtelen irányított T fa minden csúcsa véges fokú, akkor T tartalmaz végtelen utat.

Bizonyítás

Minden $n \geq 0$ számra megadható olyan x_n csúcs, hogy

- $x_0, \ldots, x_n$ egy (gyökértől induló) utat határoznak meg és
- az x_n csúcsból induló részfa végtelen.

Ekkor $x_0, x_1, \ldots$ egy végtelen utat határoznak meg.
Az x_n csúcsokat n szerinti indukcióval adjuk meg:

- x_0 a T gyökere.
- Ha $n > 0$, x_n az x_{n-1} olyan közvetlen leszármazottja, hogy az x_n-ből induló részfa végtelen. (Ilyen x_n létezik.)

A kompaktsági tétel bizonyítása

- Elegendő belátni, hogy amennyiben Σ formulák olyan végtelen halmaza, melynek minden véges részhalmaza kielégíthető, akkor Σ kielégíthető.
- Minden $n \geq 0$ számra jelölje Σ_n a Σ azon formuláinak halmazát, melyekben legfeljebb az első n, $p_1, \ldots, p_n$ változó fordul elő.
- Mivel ekvivalencia erejéig véges sok ($\leq 2^{2^n}$) olyan formula van, melyben legfeljebb az első n változó fordul elő, ezért feltevésünk szerint mindegyik Σ_n kielégíthető.
- A teljes végtelen bináris fában minden végtelen út megfelel a változók egy értékelésének, és minden n mélységű csúcs az első n változó egy értékelésének.

A kompaktsági tétel

- Minden $n \geq 0$ számra jelöljük meg a teljes végtelen bináris fa azon n mélységű csúcsait, amelyeknek megfelelő értékelések kielégítik a Σ_n formulahalmazt.
- Ekkor minden n-re megjelöltünk legalább egy csúcsot, és amennyiben egy olyan y csúcs megjelölt, mely az x csúcs (közvetlen) leszármazottja, akkor x is megjelölt.
- Tehát a megjelölt csúcsok egy olyan végtelen fát határoznak meg, melyben minden csúcs véges fokú.
- Kőnig lemmája szerint ez a fa tartalmaz végtelen utat. E végtelen út által meghatározott értékelés a Σ modellje.

Eldöntési kérdések az ítéletkalkulusban

Eldöntési kérdések

Alapvető eldöntési kérdések:

- Adott F formula kielégíthető-e?
- Adott F formula érvényes-e?
- Adott az F formula és a $\Sigma = \{F_1, \ldots, F_n\}$ véges formulahalmaz, teljesül-e $\Sigma \models F$?

A fenti kérdések ekvivalensek, hiszen:

- F kielégíthető $\Leftrightarrow$ $\neg F$ nem érvényes,
- F érvényes $\Leftrightarrow$ $\neg F$ nem kielégíthető,
- $\Sigma \models F \;\Leftrightarrow\; (F_1 \wedge \cdots \wedge F_n) \to F$ érvényes.

Megjegyzés

Nem ismert, hogy a fenti kérdések megoldhatóak-e polinomidejű algoritmussal. A kielégíthetőség $\mathbf{NP}$-teljes, az érvényesség co$\mathbf{NP}$-teljes. (Ld. Bonyolultságelmélet kurzus.)

Horn formulák

Horn formulák

Definíció

Horn formula egy olyan $F = C_1 \wedge \cdots \wedge C_n$ konjunktív normálforma, melyben minden C_i tag legfeljebb egy pozitív literált tartalmaz.

Megjegyzés

$$\begin{aligned} \neg q_1 \vee \ldots \vee \neg q_k \vee q &\equiv (q_1 \wedge \ldots \wedge q_k) \to q \\ \neg q_1 \vee \ldots \vee \neg q_k &\equiv (q_1 \wedge \ldots \wedge q_k) \to \downarrow \end{aligned}$$

Ha $k = 0$, akkor a $q \equiv \uparrow \to q$ és $\downarrow \equiv \uparrow \to \downarrow$ összefüggések adódnak.

Állítás

Horn formulák kielégíthetősége **polinomidőben** eldönthető.

Algoritmus

- **Bemenet:** F Horn formula
- **Kimenet:** F kielégítő értékelés, ha F kielégíthető, egyébként ,,nem".
- **Algoritmus:**
  1. Mindaddig, amíg F-ben van olyan $(q_1 \wedge \ldots \wedge q_n) \to q$ alakú tag, hogy minden q_i megjelölt, de q nem, jelöljük meg q minden F-beli előfordulását.
  2. Ha létezik olyan $(q_1 \wedge \ldots \wedge q_n) \to\downarrow$ alakú tag F-ben, melyre a $q_1, \ldots, q_n$ mindegyike megjelölt, akkor a válasz ,,nem".
  3. Ellenkező esetben legyen $\mathcal{A}$ az alábbi (parciális) értékelés:

$$\mathcal{A}(p) = \begin{cases} 1 & \text{ha } p \text{ meg van jelölve} \\ 0 & \text{különben} \end{cases}$$

Időigény

- A ciklus legfeljebb annyiszor fut le, mint az F-ben előforduló változók száma.
- A ciklus egyszeri lefutásának időigénye lineáris.
- A teljes időigény négyzetes.

Példa

$$\begin{aligned} F &= p \wedge q \wedge (\neg p \vee \neg q \vee r) \wedge (\neg q \vee \neg r \vee s) \wedge \\ &\quad (\neg s \vee r) \wedge (\neg q \vee \neg s \vee t) \wedge (\neg s \vee \neg t \vee u) \wedge \\ &\quad (\neg u \vee \neg t) \\ &= [\uparrow \rightarrow p] \wedge [\uparrow \rightarrow q] \wedge [(p \wedge q) \rightarrow r] \wedge \\ &\quad [(q \wedge r) \rightarrow s] \wedge [s \rightarrow r] \wedge [(q \wedge s) \rightarrow t] \wedge \\ &\quad [(s \wedge t) \rightarrow u] \wedge [(u \wedge t) \rightarrow \downarrow] \end{aligned}$$

Megjelölt változók: p, q, r, s, t, u. A formula nem kielégíthető.

Helyesség

F akkor és csak akkor kielégíthető, ha az algoritmus egy $\mathcal{A}$ kielégítő értékeléssel áll meg.

- **Elegendőség**
  Ha az algoritmus egy $\mathcal{A}$ kiértékeléssel áll meg, akkor $\mathcal{A}$ kielégítő kiértékelés.
  Valóban, ha C egy $(q_1 \wedge \ldots \wedge q_n) \to q$ alakú tag, és megálláskor mindegyik q_i megjelölt, akkor q is az, így $\mathcal{A}(q_1) = \ldots = \mathcal{A}(q_n) = \mathcal{A}(q) = 1$ miatt $\mathcal{A} \models C$.
  Ha megálláskor valamely i-re q_i nincs megjelölve, akkor $\mathcal{A}(q_i) = 0$ és ismét $\mathcal{A} \models C$.
  Ha pedig C a $(q_1 \wedge \ldots \wedge q_n) \to\downarrow$ tag, akkor valamelyik q_i nincs megjelölve. Így $\mathcal{A}(q_i) = 0$ és $\mathcal{A} \models C$.

- **Szükségesség**
  Tegyük fel, hogy $\mathcal{A}'$ kielégíti a formulát, de az algoritmus ,,nem"-mel áll meg.
  Ekkor $\mathcal{A}'(p) = 1$, valahányszor az algoritmus megjelöli a p változót. Ez könnyen igazolható a ciklus futásának száma szerinti indukcióval.
  Mivel az algoritmus ,,nem"-mel áll meg, létezik olyan $(q_1 \wedge \ldots \wedge q_n) \rightarrow\downarrow$ alakú tag, hogy az algoritmus a q_i-k mindegyikét megjelöli.
  Így $\mathcal{A}'$ nem elégíti ki ezt a tagot, hiszen $\mathcal{A}'(q_1) = \ldots = \mathcal{A}'(q_n) = 1$. Ellentmondás.

Megjegyzés

Tegyük fel, hogy F nem tartalmazza a $\uparrow\rightarrow\downarrow$ tagot. Ekkor F kielégíthető, ha nem tartalmaz $\uparrow\rightarrow p$ alakú tagot, vagy nem tartalmaz $(q_1 \wedge \ldots \wedge q_n) \rightarrow\downarrow$ alakú tagot.

Rezolúciós módszer

A **rezolúciós módszer** konjunktív normálformák (k.n.f.) kielégíthetőségének eldöntésére szolgáló módszer.

Minden

$$F = C_1 \wedge \ldots \wedge C_k$$

$$C_i = \ell_{i1} \vee \ldots \vee \ell_{in_i}, \quad i = 1, \ldots, k$$

k.n.f. felfogható úgy, mint tagok, vagy **klózok** egy $\{C_1, \ldots, C_k\}$ halmaza, és minden C_i klóz mint literálok egy $\{\ell_{i1}, \ldots, \ell_{in_i}\}$ halmaza.

Jelölje $\square$ az **üres klózt** és $\emptyset$ az **üres formulát**: $\square$ azonosan hamis (kielégíthetetlen), $\emptyset$ azonosan igaz (tautológia).

Felhasználás: Legyenek $F_1, \ldots, F_n$ és G formulák, és jelölje rendre $F_1', \ldots, F_n'$ az $F_1, \ldots, F_n$ egy k.n.f.-jét, G' pedig a $\neg G$ egy k.n.f.-jét. Így

$$\{F_1, \ldots, F_n\} \models G \;\Leftrightarrow\; F_1' \cup \ldots \cup F_n' \cup G' \text{ kielégíthetetlen.}$$

Rezolúció

Definíció

Legyenek C_1, C_2 klózok, $\ell \in C_1$, $\bar{\ell} \in C_2$. Ekkor az

$$R \;=\; (C_1 - \{\ell\}) \cup (C_2 - \{\bar{\ell}\})$$

klózt a C_1 és C_2 egy **rezolvensének** nevezzük.

Lemma

Legyen Σ klózok halmaza, $C_1, C_2 \in \Sigma$ és tegyük fel, hogy R a C_1 és C_2 egy rezolvense. Ekkor

$$\Sigma \;\equiv\; \Sigma \cup \{R\}.$$

(Itt az ekvivalencia azt jelenti, hogy a két formulahalmaznak ugyanazok a modelljei.)

Bizonyítás

A rezolúciós következtetés helyességéből.

Rezolúciós algoritmus

- **Bemenet:** F k.n.f. (ill. véges klózhalmaz)
- **Kérdés:** F kielégíthető-e?
- Mindaddig, amíg új klózt kapunk, képezzük két F-beli klóz valamely rezolvensét, és ezt adjuk az F halmazhoz.
  Ha valamikor a $\square$ klózt kapjuk, F nem kielégíthető.
  Különben F kielégíthető.

Kérdések

- Mindig véget ér-e az algoritmus?
- Helyes-e?

Példa

$F = (p \vee q) \wedge (\neg p \vee r) \wedge (p \vee \neg r) \wedge (\neg p \vee \neg q) \wedge (r \vee \neg q) \wedge (\neg r \vee q)$

1. $\{p, q\}$ F-beli klóz
2. $\{\neg p, r\}$ F-beli klóz
3. $\{q, r\}$ 1. és 2. rezolvense
4. $\{\neg r, q\}$ F-beli klóz
5. $\{q\}$ 3. és 4. rezolvense
6. $\{p, \neg r\}$ F-beli klóz
7. $\{\neg p, \neg q\}$ F-beli klóz
8. $\{\neg r, \neg q\}$ 6. és 7. rezolvense
9. $\{r, \neg q\}$ F-beli klóz
10. $\{\neg q\}$ 8. és 9. rezolvense
11. $\square$ 5. és 10. rezolvense

Tehát F nem kielégíthető.

Definíció

Legyen Σ klózok véges vagy végtelen halmaza. Ekkor
$\mathbf{Res(\Sigma) = \Sigma \cup \{R : \exists\, C_1, C_2 \in \Sigma, R \text{ a } C_1 \text{ és } C_2 \text{ rezolvense}\}}$
Jelölje $\mathbf{Res^*(\Sigma)}$ a legszűkebb olyan Δ halmazt, melyre $\Sigma \subseteq \Delta$ és $\mathbf{Res}(\Delta) \subseteq \Delta$.

Állítás

Legyen Σ klózok halmaza, C klóz.

- $\mathbf{Res}^*(\Sigma) = \bigcup_{n \geq 0} \mathbf{Res}^n(\Sigma)$, ahol

$$\mathbf{Res}^0(\Sigma) = \Sigma,$$

$$\mathbf{Res}^{n+1}(\Sigma) = \mathbf{Res}(\mathbf{Res}^n(\Sigma)), \quad n \geq 0.$$

- $C \in \mathbf{Res}^*(\Sigma)$ akkor és csak akkor, ha létezik klózok olyan véges $C_0, \ldots C_n$ sorozata, hogy $C_n = C$ és tetszőleges C_i-re $C_i \in \Sigma$ vagy valamely $j, k < i$ indexekre C_i a C_j és C_k egy rezolvense.

Állítás

Ha Σ klózok véges halmaza, akkor létezik olyan $n \geq 0$ szám, amelyre

$$\mathbf{Res}^n(\Sigma) = \mathbf{Res}^*(\Sigma).$$

Bizonyítás

$$\Sigma = \mathbf{Res}^0(\Sigma) \subseteq \mathbf{Res}^1(\Sigma) \subseteq \mathbf{Res}^2(\Sigma) \subseteq \ldots \subseteq \mathbf{Res}^*(\Sigma).$$

Továbbá, ha a Σ-beli klózokban legfeljebb a $q_1, \ldots, q_k$ változók fordulnak elő, akkor

$$|\mathbf{Res}^*(\Sigma)| \leq 2^{2k}.$$

Így létezik olyan n, melyre $\mathbf{Res}^n(\Sigma) = \mathbf{Res}^{n+1}(\Sigma)$, és ezért $\mathbf{Res}^n(\Sigma) = \mathbf{Res}^*(\Sigma)$.

Lemma

Legyen Σ klózok véges vagy végtelen halmaza. Ekkor $\Sigma \equiv \mathbf{Res}(\Sigma)$.

Állítás

Klózok tetszőleges véges vagy végtelen Σ halmazára fennállnak a következők:

- Minden $n \geq 0$ számra $\Sigma \equiv \mathbf{Res}^n(\Sigma)$.
- $\Sigma \equiv \mathbf{Res}^*(\Sigma)$.

Tétel

Klózok egy véges vagy végtelen Σ halmaza akkor és csak akkor kielégíthetetlen, ha $\square \in \mathbf{Res}^*(\Sigma)$.

Bizonyítás

A kompaktsági tétel miatt elegendő csak véges Σ halmazokra elvégezni a bizonyítást.

Elegendőség: Tegyük fel, hogy $\square \in \mathbf{Res}^*(\Sigma)$. Ekkor $\mathbf{Res}^*(\Sigma)$ kielégíthetetlen, mert $\square$ az. De $\Sigma \equiv \mathbf{Res}^*(\Sigma)$, ezért Σ is kielégíthetetlen.

Szükségesség: Legyen Σ kielégíthetetlen.Jelölje n a Σ-beli klózokban előforduló változók számát. Teljes indukcióval belátjuk, hogy $\square \in \mathbf{Res}^*(\Sigma)$.

- $n = 0$. Ekkor $\Sigma = \emptyset$ vagy $\Sigma = \{\square\}$. Mivel Σ kielégíthetetlen, ezért $\Sigma = \{\square\}$. Így $\square \in \Sigma \subseteq \mathbf{Res}^*(\Sigma)$.

Bizonyítás folytatása

- $n > 0$. Legyen p olyan változó, mely előfordul Σ-beli klózban. Ha van olyan $C \in \Sigma$, melyre $p, \neg p \in C$, akkor C azonosan igaz. Így Σ akkor és csak akkor kielégíthetetlen, ha $\Sigma - \{C\}$ az, és C elhagyható. Ezért feltehetjük, hogy nincs olyan $C \in \Sigma$, melyre $p, \neg p \in C$.
  Legyen

$$\begin{aligned}\Sigma_1 =& \{C : C \in \Sigma, p \notin C, \neg p \notin C\} \cup \\ & \{C : C \notin \Sigma, C \cup \{p\} \in \Sigma\}, \\ \Sigma_2 =& \{C : C \in \Sigma, p \notin C, \neg p \notin C\} \cup \\ & \{C : C \notin \Sigma, C \cup \{\neg p\} \in \Sigma\}.\end{aligned}$$

Bizonyítás folytatása

Σ_1 és Σ_2 egyike sem kielégíthető. Valóban, ha pl. Σ_1-et kielégít egy (parciális) értékelés, akkor Σ-t kielégíti ugyanez az értékelés azzal, hogy p értéke 0.

Így az indukciós feltevés szerint

$$\square \in \mathbf{Res}^*(\Sigma_1) \cap \mathbf{Res}^*(\Sigma_2).$$

Ezért $\square \in \mathbf{Res}^*(\Sigma)$, vagy

$$\{p\} \in \mathbf{Res}^*(\Sigma) \text{ és } \{\neg p\} \in \mathbf{Res}^*(\Sigma).$$

Ebből $\square \in \mathbf{Res}^*(\Sigma)$.

Deduktív rendszerek

A következőkben olyan rendszereket mutatunk be, melyekben **formálisan bizonyítható**, hogy egy F formula tautológia, vagy kielégíthetetlen, vagy hogy F formulák egy Σ halmazának következménye.

Hilbert rendszere

Hilbert rendszere

Olyan formulákat tekintünk, amelyekben nem fordul elő $\wedge$, $\vee$, $\leftrightarrow$, $\neg$ és $\uparrow$.

Axiómák

1. $(F \to (G \to H)) \to ((F \to G) \to (F \to H))$
2. $F \to (G \to F)$
3. $((F \to \downarrow) \to \downarrow) \to F$

ahol F, G, H tetszőleges formulák.

Szabály

Leválasztás, vagy **modus ponens**

$$\frac{F,\ F \to G}{G},$$

ahol F, G tetszőleges formulák.

Definíció

Az érvényesség Hilbert-féle **bizonyításának** vagy **levezetésnek** nevezünk egy olyan

$$F_1, F_2, \ldots, F_n$$

sorozatot, ahol az F_i formulák mindegyike

1. axióma, vagy
2. előáll az őt megelőző formulákból leválasztással.

Azt mondjuk, hogy F **bizonyítható**, vagy **levezethető**, ha létezik olyan $F_1, \ldots, F_n$ bizonyítás, melyre $F = F_n$.
Jelölés: $\vdash_{\mathcal{H}} \boldsymbol{F}$.

Legyen Σ formulák halmaza.

Definíció

Σ feletti Hilbert-féle **bizonyításnak** vagy **levezetésnek** nevezünk egy olyan

$$F_1, F_2, \ldots, F_n$$

sorozatot, ahol az F_i formulák mindegyike

1. axióma, vagy
2. Σ-beli formula, vagy
3. előáll az őt megelőző formulákból leválasztással.

Azt mondjuk, hogy F **bizonyítható**, vagy **levezethető** Σ-ból, ha létezik olyan $F_1, \ldots, F_n$ Σ feletti bizonyítás, melyre $F = F_n$. Jelölés: $\boldsymbol{\Sigma \vdash_{\mathcal{H}} F}$.

Tehát $\vdash_{\mathcal{H}} F$ akkor és csak akkor, ha $\emptyset \vdash_{\mathcal{H}} F$.

Példa

$F \to F$ bizonyítása, ahol F tetszőleges.
Legyen $G = F \to F$.

1. $F \to (G \to F)$, Ax 2.
2. $F \to G$, Ax 2.
3. $(F \to (G \to F)) \to ((F \to G) \to (F \to F))$, Ax 1.
4. $(F \to G) \to (F \to F)$, MP 1 és 3.
5. $F \to F$, MP 2 és 4.

Tehát tetszőleges F-re: $\vdash_{\mathcal{H}} F \to F$.

Példa

$$\vdash_{\mathcal{H}} (G \to H) \to ((F \to G) \to (F \to H)).$$

Legyen $P = G \to H$, $Q = F \to (G \to H)$,
$R = (F \to G) \to (F \to H)$. Be kell látnunk, hogy $\vdash_{\mathcal{H}} P \to R$.

1. $P \to Q$, Ax 2.
2. $Q \to R$, Ax 1.
3. $(Q \to R) \to (P \to (Q \to R))$, Ax 2.
4. $P \to (Q \to R)$, MP 2 és 3.
5. $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$, Ax 1.
6. $(P \to Q) \to (P \to R)$, MP 4 és 5.
7. $P \to R$, MP 1 és 6.

Példa

$$\vdash_{\mathcal{H}} \downarrow \rightarrow F.$$

Jelölje $\neg F$ az $F \rightarrow \downarrow$ formulát, és $\neg\neg F$ az $(F \rightarrow \downarrow) \rightarrow \downarrow$ formulát.

1. $\downarrow \rightarrow \neg\neg F$, Ax 2.
2. $\neg\neg F \rightarrow F$, Ax 3.
3. $(\neg\neg F \rightarrow F) \rightarrow ((\downarrow \rightarrow \neg\neg F) \rightarrow (\downarrow \rightarrow F))$, előző példa.
4. $(\downarrow \rightarrow \neg\neg F) \rightarrow (\downarrow \rightarrow F)$, MP 2 és 3.
5. $\downarrow \rightarrow F$, MP 1 és 4.

Hilbert rendszerének helyességi és teljességi tétele

Tetszőleges Σ formulahalmazra és F formulára $\Sigma \models F$ akkor és csak akkor, ha $\Sigma \vdash_{\mathcal{H}} F$.

Az elegendőség következik abból, hogy az axiómák tautológiák, és az MP helyes következtetési szabály.
A szükségesség bizonyítását később végezzük el.

Következmény

Tetszőleges F formulára $\models F$ akkor és csak akkor, ha $\vdash_{\mathcal{H}} F$.

Dedukciós tétel

Legyen Σ formulák halmaza és legyenek F, G formulák.

$$\Sigma \cup \{F\} \vdash_{\mathcal{H}} G \;\Leftrightarrow\; \Sigma \vdash_{\mathcal{H}} F \to G.$$

Bizonyítás

Elegendőség: Ha $\Sigma \vdash_{\mathcal{H}} F \to G$, akkor $\Sigma \cup \{F\} \vdash_{\mathcal{H}} F \to G$. De $\Sigma \cup \{F\} \vdash_{\mathcal{H}} F$, így MP szerint $\Sigma \cup \{F\} \vdash_{\mathcal{H}} G$.

Szükségesség: Tegyük fel, hogy $\Sigma \cup \{F\} \vdash_{\mathcal{H}} G$. A levezetés hossza szerinti indukcióval igazolható, hogy $\Sigma \vdash_{\mathcal{H}} F \to G$.

Tekintsük a levezetés utolsó lépését.

Bizonyítás folytatása

- **Az utolsó lépésben $G \in \Sigma$, vagy G axióma.** Ekkor $\Sigma \vdash_{\mathcal{H}} G$. A 2. axióma miatt $\Sigma \vdash_{\mathcal{H}} G \to (F \to G)$. Így MP felhasználásával $\Sigma \vdash_{\mathcal{H}} F \to G$.
- **Az utolsó lépésben $G = F$.** Ekkor $\Sigma \vdash_{\mathcal{H}} F \to F$ az egyik korábbi példa szerint.
- **Az utolsó lépésben G az MP-vel adódik.** Ekkor valamely H formulára léteznek rövidebb $\Sigma \cup \{F\} \vdash_{\mathcal{H}} H \to G$ és $\Sigma \cup \{F\} \vdash_{\mathcal{H}} H$ levezetések.
  Indukciós feltevésből: $\Sigma \vdash_{\mathcal{H}} F \to (H \to G)$ és $\Sigma \vdash_{\mathcal{H}} F \to H$.
  Az 1. axióma szerint:
  $$\Sigma \vdash_{\mathcal{H}} (F \to (H \to G)) \to ((F \to H) \to (F \to G)).$$
  Az MP kétszeri alkalmazásával: $\Sigma \vdash_{\mathcal{H}} F \to G$.

Definíció

Formulák egy Σ halmaza **konzisztens a Hilbert rendszerben**, vagy **H-konzisztens**, ha nem teljesül, hogy $\Sigma \vdash_{\mathcal{H}} \downarrow$.

Állítás

Σ akkor és csak akkor H-konzisztens, ha nem létezik olyan F formula, hogy $\Sigma \vdash_{\mathcal{H}} F$ és $\Sigma \vdash_{\mathcal{H}} F \to \downarrow$ is teljesül.

Bizonyítás

Ha $\Sigma \vdash_{\mathcal{H}} F$ és $\Sigma \vdash_{\mathcal{H}} F \to \downarrow$ valamely F-re, akkor MP miatt $\Sigma \vdash_{\mathcal{H}} \downarrow$.
Tegyük fel, hogy $\Sigma \vdash_{\mathcal{H}} \downarrow$. Ekkor az egyik előző példából $\Sigma \vdash_{\mathcal{H}} F$ minden F formulára.

Állítás

Σ akkor és csak akkor H-konzisztens, ha minden véges részhalmaza az.

Bizonyítás

Minden levezetés csak véges sok Σ-beli formulát használ.

Definíció

Egy Σ formulahalmazt **maximális H-konzisztens** halmaznak nevezünk, ha H-konzisztens és nem létezik olyan F formula, hogy $F \notin \Sigma$ és $\Sigma \cup \{F\}$ H-konzisztens.

Lemma

Minden H-konzisztens formulahalmaz kiterjeszthető maximális H-konzisztens formulahalmazzá.

Bizonyítás

Legyen Σ H-konzisztens, $F_1, F_2, \ldots$ pedig a formulák egy felsorolása. Legyen $\Sigma_0 = \Sigma$ és $i \geq 1$ esetén

$$\Sigma_i = \begin{cases} \Sigma_{i-1} \cup \{F_i\} & \text{ha ez a halmaz H-konzisztens,} \\ \Sigma_{i-1} & \text{különben.} \end{cases}$$

Legyen $\Delta = \bigcup_{n \geq 0} \Sigma_n$.

Bizonyítás folytatása

Δ H-konzisztens, mert minden véges részhalmaza az.
Bármely F formulára, $F \in \Delta$ és $F \to\downarrow \in \Delta$ közül pontosan az egyik teljesül.
Valóban, ha mindkettő teljesülne, akkor MP miatt $\downarrow$ levezethető lenne Δ-ból, ellentmondás.
Ha egyik formula sincs Δ-ban, akkor $\Delta \cup \{F\}$ és $\Delta \cup \{F \to\downarrow\}$ nem H-konzisztensek. Így $\Delta \cup \{F\} \vdash_{\mathcal{H}} \downarrow$ és $\Delta \cup \{F \to\downarrow\} \vdash_{\mathcal{H}} \downarrow$.
A dedukciós tétel szerint: $\Delta \vdash_{\mathcal{H}} F \to\downarrow$ és $\Delta \vdash_{\mathcal{H}} (F \to\downarrow) \to\downarrow$, ellentmondás.
Így Δ maximális H-konzisztens halmaz.
Vegyük észre, hogy $\Delta \vdash_{\mathcal{H}} F$ esetén $F \in \Delta$. Továbbá, a fentiek szerint, tetszőleges F formulára, F és $F \to\downarrow$ közül valamelyik Δ-ban van.

Tétel

Formulák egy Σ halmaza akkor és csak akkor kielégíthető, ha H-konzisztens.

Bizonyítás

Ha Σ nem H-konzisztens, akkor $\Sigma \vdash_{\mathcal{H}} \downarrow$.
Ezért $\Sigma \models \downarrow$ is teljesül, és így Σ kielégíthetetlen.
Tegyük fel, hogy Σ H-konzisztens. Ekkor Σ kiterjeszthető egy Δ maximális H-konzisztens formulahalmazzá. Legyen

$$\mathcal{A}(p) = \begin{cases} 1 & \text{ha } p \in \Delta, \\ 0 & \text{ha } p \notin \Delta. \end{cases}$$

Belátjuk, hogy $\mathcal{A} \models \Delta$.

Bizonyítás folytatása

Az F formula felépítése szerinti indukcióval belátjuk, hogy $\mathcal{A} \models F$ akkor és csak akkor, ha $F \in \Delta$.

- F egy változó: triviális.
- $F = \downarrow$. Mivel Δ H-konzisztens, $\downarrow \notin \Delta$. Továbbá $\mathcal{A} \not\models \downarrow$.
- $F = G \to H$. $\mathcal{A}(F) = 1$ pontosan akkor, ha $\mathcal{A}(G) = 0$ vagy $\mathcal{A}(H) = 1$, ami az indukciós feltevés szerint azzal ekvivalens, hogy $G \notin \Delta$ vagy $H \in \Delta$. Belátjuk, hogy pontosan ebben az esetben teljesül $F \in \Delta$.
  1. Ha $G \notin \Delta$, akkor $G \to \downarrow \in \Delta$, mivel Δ maximális H-konzisztens halmaz. Mivel $\downarrow \to H \in \Delta$, adódik, hogy $F \in \Delta$.
  2. Ha $H \in \Delta$, akkor mivel $H \to (G \to H) \in \Delta$, MP felhasználásával kapjuk, hogy $F \in \Delta$.
  3. Különben $G \in \Delta$ és $H \notin \Delta$. Ha $F \in \Delta$, akkor MP miatt $H \in \Delta$, ellentmondás. Tehát $F \notin \Delta$.

Most újra kimondjuk korábbi tételünket:

Tétel

Legyen Σ formulák halmaza, F formula.

$$\Sigma \models F \;\Leftrightarrow\; \Sigma \vdash_{\mathcal{H}} F.$$

Bizonyítás

Elegendőség triviális. Szükségesség:

$$\begin{aligned}
\Sigma \models F &\Rightarrow \Sigma \cup \{F \to\!\downarrow\} \text{ nem kielégíthető} \\
&\Rightarrow \Sigma \cup \{F \to\!\downarrow\} \text{ nem H-konzisztens} \\
&\Rightarrow \Sigma \vdash_{\mathcal{H}} (F \to\!\downarrow) \to\!\downarrow \text{ (Dedukciós tétel)} \\
&\Rightarrow \Sigma \vdash_{\mathcal{H}} F \text{ (Ax 3, MP)}
\end{aligned}$$

Megjegyzés

Az előző teljességi tételből (melyet a kompaktsági tétel nélkül bizonyítottunk) következik a kompaktsági tétel.
Valóban, ha $\Sigma \models F$, akkor $\Sigma \vdash_{\mathcal{H}} F$. De minden levezetésben csak véges sok Σ-beli formulát használunk, így létezik olyan véges $\Sigma_0 \subseteq \Sigma$ halmaz, hogy $\Sigma_0 \vdash_{\mathcal{H}} F$.

Megjegyzés

Ha a 3. axiómát kicseréljük a gyengébb $\downarrow\rightarrow F$ axiómára, akkor az ún. **intuícionista logikát** kapjuk.

Helyettesítés újból

Helyettesítés

Az elsőrendű logikában a már megismert helyettesítésen kívül helyettesíthetünk termeket az elsőrendű változók helyére.

Definíció

Legyenek u, t termek, x változó. Ekkor az $\boldsymbol{u[x/t]}$ **termet** az u felépítése szerinti indukcióval adjuk meg.

$$u[x/t] = \begin{cases} t & \text{ha } u = x \\ u & \text{különben} \end{cases} \quad \text{ha } u \text{ változó},$$

$$u[x/t] = f(u_1[x/t], \ldots, u_n[x/t]), \text{ ha } u = f(u_1, \ldots, u_n).$$

Állítás

$u[x/t]$ úgy áll elő u-ból, hogy benne x minden előfordulását t-vel helyettesítjük.

Definíció

Legyen F formula, t term, x változó. Az $\boldsymbol{F[x/t]}$ **formulát** a következő módon definiáljuk:

- Ha $F = p(t_1, \ldots, t_n)$ atomi formula, akkor $F[x/t] = p(t_1[x/t], \ldots, t_n[x/t])$.
- Ha $F = \uparrow$ vagy $F = \downarrow$, akkor a két esetnek megfelelően $F[x/t] = \uparrow$ vagy $F[x/t] = \downarrow$.
- Ha $F = \neg G$, akkor $F[x/t] = \neg(G[x/t])$.
- Ha $F = G \bullet H$, ahol $\bullet \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$, akkor $F[x/t] = G[x/t] \bullet H[x/t]$.
- Ha $F = QxG$, ahol $Q \in \{\exists, \forall\}$, akkor $F[x/t] = F$.
- Ha $F = QyG$, ahol $Q \in \{\exists, \forall\}$ és $y \neq x$, akkor:
  1. Ha y nem fordul elő t-ben, akkor $F[x/t] = Qy(G[x/t])$.
  2. Ellenkező esetben legyen z az első olyan változó, mely nem fordul elő t-ben és F-ben. Ekkor $F[x/t] = Qz(G[y/z][x/t])$.

Helyettesítés

Példa

$$(\exists y p(x,y))[x/g(y)] \;=\; \exists z p(g(y),z).$$

Lemma

Legyenek u, t termek, x változó, $\mathcal{A} = (A, I, \varphi)$ struktúra. Ekkor:

$$\mathcal{A}(u[x/t]) \;=\; \mathcal{A}_{[x\mapsto a]}(u),$$

ahol $a = \mathcal{A}(t)$.

Bizonyítás

- $u = x$. Ekkor $u[x/t] = t$. Így:
$$\mathcal{A}(u[x/t]) = \mathcal{A}(t) = a = \mathcal{A}_{[x\mapsto a]}(x) = \mathcal{A}_{[x\mapsto a]}(u).$$

- u változó, $u \neq x$. Ekkor $u[x/t] = u$. Így:
$$\mathcal{A}(u[x/t]) = \mathcal{A}(u) = \mathcal{A}_{[x\mapsto a]}(u).$$

Bizonyítás folytatása

- $u = f(u_1, \ldots, u_n)$. Ekkor $u[x/t] = f(u_1[x/t], \ldots, u_n[x/t])$. Az indukciós feltevés szerint

$$\mathcal{A}(u_i[x/t]) = \mathcal{A}_{[x \mapsto a]}(u_i), \quad i = 1, \ldots, n.$$

Így:

$$\begin{aligned}
\mathcal{A}(u[x/t]) &= \mathcal{A}(f(u_1[x/t], \ldots, u_n[x/t])) \\
&= I(f)(\mathcal{A}(u_1[x/t]), \ldots, \mathcal{A}(u_n[x/t])) \\
&= I(f)(\mathcal{A}_{[x \mapsto a]}(u_1), \ldots, \mathcal{A}_{[x \mapsto a]}(u_n)) \\
&= \mathcal{A}_{[x \mapsto a]}(f(u_1, \ldots, u_n)) \\
&= \mathcal{A}_{[x \mapsto a]}(u).
\end{aligned}$$

Helyettesítés

Lemma

Legyen F egy formula, x egy változó, t egy term. Ekkor tetszőleges $\mathcal{A}$ struktúrára

$$\mathcal{A}(F[x/t]) \;=\; \mathcal{A}_{[x\mapsto a]}(F),$$

ahol $a = \mathcal{A}(t)$.

Bizonyítás

F hossza szerinti teljes indukcióval, ahol atomi formula hossza 1.

- $F = p(u_1, \ldots, u_n)$. Ekkor $F[x/t] = p(u_1[x/t], \ldots, u_n[x/t])$. Így:

$$\begin{aligned}
\mathcal{A}(F[x/t]) &= \mathcal{A}(p(u_1[x/t], \ldots, u_n[x/t])) \\
&= I(p)(\mathcal{A}(u_1[x/t]), \ldots, \mathcal{A}(u_n[x/t])) \\
&= I(p)(\mathcal{A}_{[x\mapsto a]}(u_1), \ldots, \mathcal{A}_{[x\mapsto a]}(u_n)) \\
&= \mathcal{A}_{[x\mapsto a]}(p(u_1, \ldots, u_n)) \\
&= \mathcal{A}_{[x\mapsto a]}(F).
\end{aligned}$$

Bizonyítás folytatása

- $F = \uparrow$ vagy $F = \downarrow$. Triviális.
- $F = G \bullet H$. Ekkor $F[x/t] = G[x/t] \bullet H[x/t]$. Így:

$$\begin{aligned}
\mathcal{A}(F[x/t]) &= \mathcal{A}(G[x/t] \bullet H[x/t]) \\
&= \mathcal{A}(G[x/t]) \bullet \mathcal{A}(H[x/t]) \\
&= \mathcal{A}_{[x \mapsto a]}(G) \bullet \mathcal{A}_{[x \mapsto a]}(H) \\
&= \mathcal{A}_{[x \mapsto a]}(G \bullet H) \\
&= \mathcal{A}_{[x \mapsto a]}(F).
\end{aligned}$$

- $F = \neg G$. Hasonló az előző esethez.

Bizonyítás folytatása

Legyen $Q \in \{\exists, \forall\}$.

- $F = QxG$. Ekkor $F[x/t] = F$. Így:
$$\mathcal{A}(F[x/t]) = \mathcal{A}(F) = \mathcal{A}_{[x \mapsto a]}(F),$$
mert x nem fordul elő szabadon F-ben.
- $F = QyG$, ahol $y \neq x$, y nem fordul elő t-ben. Ekkor $F[x/t] = Qy(G[x/t])$. Így:
$$\begin{aligned}
\mathcal{A} \models F[x/t] &\Leftrightarrow Qb \in A\ \mathcal{A}_{[y \mapsto b]} \models G[x/t] \\
&\Leftrightarrow Qb \in A\ \mathcal{A}_{[y \mapsto b][x \mapsto a]} \models G \\
&\Leftrightarrow Qb \in A\ \mathcal{A}_{[x \mapsto a][y \mapsto b]} \models G \\
&\Leftrightarrow \mathcal{A}_{[x \mapsto a]} \models QyG \\
&\Leftrightarrow \mathcal{A}_{[x \mapsto a]} \models F.
\end{aligned}$$

Bizonyítás folytatása

- $F = QyG$, $y \neq x$, y előfordul t-ben. Legyen z az első olyan változó, mely nem fordul elő t-ben és F-ben, $G' = G[y/z]$. Ekkor $F[x/t] = Qz(G'[x/t]) = (QzG')[x/t]$.
  Mivel QzG' hossza megegyezik az F hosszával és z nem fordul elő t-ben, ezért az előző eset szerint:
  $$\mathcal{A} \models (QzG')[x/t] \;\Leftrightarrow\; \mathcal{A}_{[x\mapsto a]} \models QzG'.$$
  De az indukciós feltevést használva a 2. sorban,
  $$\begin{aligned} \mathcal{A}_{[x\mapsto a]} \models QzG' &\Leftrightarrow Qc \in A\ \mathcal{A}_{[x\mapsto a][z\mapsto c]} \models G[y/z] \\ &\Leftrightarrow Qc \in A\ \mathcal{A}_{[x\mapsto a][z\mapsto c][y\mapsto c]} \models G \\ &\Leftrightarrow Qc \in A\ \mathcal{A}_{[x\mapsto a][y\mapsto c]} \models G \\ &\Leftrightarrow \mathcal{A}_{[x\mapsto a]} \models QyG. \end{aligned}$$

Bizonyítás folytatása

- Így:

$$\begin{aligned} \mathcal{A} \models F[x/t] &\Leftrightarrow \mathcal{A} \models (QzG')[x/t] \\ &\Leftrightarrow \mathcal{A}_{[x \mapsto a]} \models QzG' \\ &\Leftrightarrow \mathcal{A}_{[x \mapsto a]} \models QyG \\ &\Leftrightarrow \mathcal{A}_{[x \mapsto a]} \models F. \end{aligned}$$

Következmény

Legyen $F = QxG$ egy formula és y egy olyan változó, mely nem fordul elő szabadon G-ben. Ekkor $F \equiv Qy(G[x/y])$.

Bizonyítás

Minden $\mathcal{A}$ struktúrára,

$$\begin{aligned} \mathcal{A} \models Qy(G[x/y]) &\Leftrightarrow Qb \in A\ \mathcal{A}_{[y\mapsto b]} \models G[x/y] \\ &\Leftrightarrow Qb \in A\ \mathcal{A}_{[y\mapsto b][x\mapsto b]} \models G \\ &\Leftrightarrow Qb \in A\ \mathcal{A}_{[x\mapsto b]} \models G \\ &\Leftrightarrow \mathcal{A} \models F. \end{aligned}$$

Normálformák

Definíció

Egy formulát **kiigazítottnak** nevezünk, ha

1. Nincs olyan változó, mely kötötten és szabadon is előfordul.
2. Különböző kvantor-előfordulások rendre különböző változókat kötnek le.

Következmény

Minden formula ekvivalens egy olyan kiigazított formulával, mely előáll a formulából a változók átnevezésével.

Definíció

Egy F formula **prenex** alakú, ha

$$F = Q_1 y_1 \dots Q_n y_n G,$$

ahol G kvantormentes és minden Q_i kvantor.

Állítás

Minden F formulához létezik ekvivalens prenex alakú kiigazított formula.

Bizonyítás

F felépítése szerinti indukcióval. Feltehetjük, hogy F-ben nem fordulnak elő a $\rightarrow$ és $\leftrightarrow$ logikai jelek.

- F atomi formula. Ekkor F prenex alakú és kiigazított.
- $F = \uparrow$ vagy $F = \downarrow$. Ekkor F ismét prenex alakú és kiigazított.

Bizonyítás folytatása

- $F = \neg G$. Legyen $Q_1 y_1 \dots Q_n y_n H$ a G-vel ekvivalens prenex alakú kiigazított formula, mely az indukciós feltevés szerint létezik. Minden i-re legyen Q_i' egzisztenciális kvantor, ha Q_i univerzális kvantor, és univerzális kvantor, ha Q_i egzisztenciális kvantor. Ekkor
$$Q_1' y_1 \dots Q_n' y_n (\neg H)$$
F-fel ekvivalens prenex alakú kiigazított formula.

Bizonyítás folytatása

- $F = G_1 \vee G_2$. Legyenek
$$Q_1 y_1 \ldots Q_n y_n H_1 \quad \text{és} \quad Q'_1 z_1 \ldots Q'_m z_m H_2$$
a G_1-gyel és G_2-vel ekvivalens prenex alakú kiigazított formulák. Feltehető, hogy az y_i és z_j változók páronként különböznek. Ekkor
$$Q_1 y_1 \ldots Q_n y_n Q'_1 z_1 \ldots Q'_m z_m (H_1 \vee H_2)$$
F-fel ekvivalens prenex alakú kiigazított formula.
- $F = G_1 \wedge G_2$. Az előző esethez hasonlóan.

Bizonyítás folytatása

- $F = QxG$. Legyen $Q_1y_1 \dots Q_ny_nH$ a G-vel ekvivalens prenex alakú kiigazított formula. Feltehető, hogy $x \notin \{y_1, \dots, y_n\}$. Ekkor

$$QxQ_1y_1 \dots Q_ny_nH$$

F-fel ekvivalens prenex alakú kiigazított formula.

Megjegyzés

Az is elérhető, hogy az F-fel ekvivalens prenex alakú kiigazított formula magja konjunktív vagy diszjunktív normálforma legyen (azaz literálok diszjunkcióinak konjunkciója, vagy literálok konjunkcióinak diszjunkciója).

Definíció

Skolem normálforma egy

$$\forall x_1 \dots \forall x_n F$$

alakú kiigazított formula, ahol F kvantormentes.

Definíció

Azt mondjuk, hogy az F és G formulák $\boldsymbol{s}$**-ekvivalensek**, jelölés $\boldsymbol{F \equiv {}_s G}$, ha F akkor és csakis akkor kielégíthető, ha G az.

Tehát a $\equiv {}_s$ ekvivalenciareláció nagyon durván osztályozza a formulákat. Két osztály: a kielégíthető és a kielégíthetetlen formulák.

A következőkben feltesszük, hogy az elsőrendű nyelv minden n-re elegendően sok n-rangú függvényszimbólumot tartalmaz.

Tétel

Minden F formulához **effektíven megadható** vele s-ekvivalens Skolem normálforma.

Bizonyítás

Feltehető, hogy $F = Q_1 x_1 \dots Q_n x_n G$ alakú prenex alakú kiigazított formula.

- Minden olyan i-re, amelyre $Q_i = \exists$, elvégezzük a következő átalakítást:
  Legyenek $z_1, \dots, z_k$ az $x_1, \dots, x_{i-1}$ változók közül azok, amelyek univerzális kvantorral vannak lekötve.
  1. Töröljük a Q_i kvantort a mellette levő x_i-vel együtt.
  2. G-ben az x_i minden előfordulását $f(z_1, \dots, z_k)$-val helyettesítjük, ahol f **új** függvényszimbólum.

Az előző konstrukció helyessége az alábbi lemmán múlik.

Lemma

Legyen F egy $\forall x_1 \ldots \forall x_n \exists y G$ alakú kiigazított formula, ahol G nem feltétlenül kvantormentes. Tegyük fel, hogy az f n-rangú új függvényszimbólum. Ekkor

$$F \equiv {}_s\forall x_1 \ldots \forall x_n (G[y/f(x_1, \ldots, x_n)]).$$

Bizonyítás

F minden modelljéhez elkészíthető a jobboldalon álló formula egy modellje, és fordítva.

Bizonyítás folytatása

Jelölje H a jobboldalon álló formulát.
Ha $\mathcal{A} \models F$, akkor legyen $\mathcal{B}$ ugyanaz, mint $\mathcal{A}$, azzal a különbséggel, hogy tetszőleges $a_1, \ldots, a_n$ elemekhez $I(f)$ rendeljen olyan b elemet, melyre

$$\mathcal{A}_{[x_1 \mapsto a_1] \ldots [x_n \mapsto a_n][y \mapsto b]} \models G.$$

Ekkor $\mathcal{B} \models H$.
Ha $\mathcal{B} \models H$, akkor $\mathcal{B} \models F$.

Következmény

Minden F formulához effektíven konstruálható s-ekvivalens zárt Skolem normálforma, melynek a magja konjunktív (vagy diszjunktív) normálforma.

Legyen Σ tetszőleges formulahalmaz.
Megadunk egy olyan Skolem normálformákból álló Δ halmazt, hogy Σ akkor és csak akkor kielégíthető, ha Δ az.
Ha $\Sigma = \{F_1, \ldots, F_n\}$, akkor legyen G az $F_1 \wedge \ldots \wedge F_n$ Skolem normálformája, és $\Delta = \{G\}$.
Ha Σ végtelen, akkor pl. eljárhatunk úgy, hogy Σ minden F formulájában minden x szabad változót egy **új** c konstansjellel helyettesítünk, majd minden formulát Skolem normálformára hozunk úgy, hogy mindig **új** függvényjeleket használunk.

Az elsőrendű logika eldönthetősége

Ebben a részben belátjuk azt, hogy az elsőrendű logika algoritmikusan eldönthetetlen.
Ehhez feltesszük majd, hogy a nyelv egy bizonyos minimális bonyolultsággal rendelkezik.
Ismert, hogy a **Post megfelelkezési probléma, PMP** algoritmikusan eldönthetetlen.

Definíció

- **Adott**: a $\{0, 1\}$ halmaz feletti nemüres szavakból álló rendezett párok egy $(u_1, v_1), \ldots, (u_k, v_k)$ sorozata.
- **Kérdés**: Létezik-e **megoldás**, azaz olyan $i_1, \ldots, i_n, n \geq 1$ indexsorozat, hogy

$$u_{i_1} \ldots u_{i_n} = v_{i_1} \ldots v_{i_n}.$$

Eldönthetőség

Tétel (Church)

Nem létezik olyan algoritmus, mely tetszőleges formuláról eldönti, hogy tautológia-e.

Következmény

Nem létezik olyan algoritmus, mely tetszőleges formuláról eldönti, hogy a formula

1. kielégíthető-e, ill.
2. azonosan hamis-e.

Következmény

Nem létezik olyan algoritmus, mely formulák egy tetszőleges Σ véges halmazáról és egy további F formuláról eldönti, hogy $\Sigma \models F$ teljesül-e.

Bizonyítás

Adott

$$K = (u_1, v_1), \ldots, (u_k, v_k) \in \{0,1\}^+ \times \{0,1\}^+$$

sorozathoz elkészítünk egy olyan F_K formulát, hogy F_K akkor és csak akkor tautológia, ha K-nak létezik megoldása.
Felhasználjuk az f_0, f_1 1-rangú függvényszimbólumokat, a c konstansszimbólumot és a p 2-rangú predikátumszimbólumot.
Tetszőleges $u = a_1 \ldots a_m \in \{0,1\}^*$ szóra és t termre legyen $f_u(t)$ az

$$f_{a_1}(f_{a_2}(\ldots(f_{a_m}(t))\ldots))$$

term.

Bizonyítás folytatása

Legyen

$$F_K = (F_1 \wedge F_2) \to F_3,$$

ahol

$$\begin{aligned} F_1 &= \bigwedge_{i=1}^{k} p(f_{u_i}(c), f_{v_i}(c)), \\ F_2 &= \forall x \forall y (p(x,y) \to \bigwedge_{i=1}^{k} p(f_{u_i}(x), f_{v_i}(y))), \\ F_3 &= \exists z p(z,z). \end{aligned}$$

Példa

Legyen K a következő sorozat: $(0, 01)$, $(100, 001)$, $(10, 0)$. Ekkor:

$$\begin{aligned}
F_1 &= p(f_0(c), f_0(f_1(c))) \wedge \\
&\quad p(f_1(f_0(f_0(c))), f_0(f_0(f_1(c)))) \wedge \\
&\quad p(f_1(f_0(c)), f_0(c)), \\
F_2 &= \forall x \forall y (p(x, y) \rightarrow \\
&\quad (p(f_0(x), f_0(f_1(y))) \wedge \\
&\quad p(f_1(f_0(f_0(x))), f_0(f_0(f_1(y))))) \wedge \\
&\quad p(f_1(f_0(x)), f_0(y))), \\
F_3 &= \exists z p(z, z).
\end{aligned}$$

Állítás

Ha F_K tautológia, akkor K-nak van megoldása.

Bizonyítás

Tekintsük az $\mathcal{A} = (A, I)$ struktúrát, ahol a harmadik komponenst azért nem jelöltük, mert F_K mondat.

1. $A = \{0,1\}^*$
2. $I(c) = \lambda$, az üres szó.
   $I(f_j) : A \to A$, $u \mapsto ju$, $j = 0, 1$.
   $I(p) : A^2 \to \{0,1\}$,
   $$I(p)(u,v) = 1 \quad \Leftrightarrow \quad \exists n > 0 \exists i_1, \ldots, i_n : u = u_{i_1} \ldots u_{i_n}, v = v_{i_1} \ldots v_{i_n}.$$

Bizonyítás folytatása

Könnyen látható, hogy

$$\mathcal{A} \models F_1 \text{ és } \mathcal{A} \models F_2.$$

Valóban, $\mathcal{A} \models F_1$, mert $I(p)(u_i, v_i)$ teljesül minden i-re.
Ha pedig $I(p)(u, v)$ teljesül az u, v szavakra, akkor létezik olyan $n > 0$, $i_1, \ldots, i_n$, hogy $u = u_{i_1} \ldots u_{i_n}$, $v = v_{i_1} \ldots v_{i_n}$.
Így tetszőleges i-re $I(p)(u_i u, v_i v)$ is teljesül, hiszen $u_i u = u_i u_{i_1} \ldots u_{i_n}$ és $v_i v = v_i v_{i_1} \ldots v_{i_n}$.
Tehát $\mathcal{A} \models F_2$.
Így $\mathcal{A} \models F_K$ miatt $\mathcal{A} \models F_3$.
Ez éppen azt jelenti, hogy K-nak van megoldása.

Állítás

Ha K-nak van megoldása, akkor F_K tautológia.

Bizonyítás

Legyen $\mathcal{A} = (A, I)$ tetszőleges struktúra. Be kell látnunk, hogy $\mathcal{A} \models F_K$.
Ha $\mathcal{A} \not\models F_1$ vagy $\mathcal{A} \not\models F_2$, ez nyilvánvaló.
Tegyük fel, hogy $\mathcal{A} \models F_1$ és $\mathcal{A} \models F_2$. Jelölje $i_1, \ldots, i_n$ a K egy megoldását.

- Mivel $\mathcal{A} \models F_1$, ezért $\mathcal{A} \models p(f_{u_{i_n}}(c), f_{v_{i_n}}(c))$.
- Mivel $\mathcal{A} \models F_2$, indukcióval adódik, hogy $\mathcal{A} \models p(f_{u_{i_j} \ldots u_{i_n}}(c), f_{v_{i_j} \ldots v_{i_n}}(c))$, $j = 1, \ldots, n$.
- Speciálisan $\mathcal{A} \models p(f_{u_{i_1} \ldots u_{i_n}}(c), f_{v_{i_1} \ldots v_{i_n}}(c))$. Mivel $u_{i_1} \ldots u_{i_n} = v_{i_1} \ldots v_{i_n}$, ezért $\mathcal{A}(f_{u_{i_1} \ldots u_{i_n}}(c)) = \mathcal{A}(f_{v_{i_1} \ldots v_{i_n}}(c))$, tehát $\mathcal{A} \models F_3$.

Herbrand struktúrák

Herbrand struktúrák

Tekintsünk egy tetszőleges olyan elsőrendű nyelvet, mely legalább egy konstans szimbólumot tartalmaz. Jelölje T_0 a zárt termek (vagy **alap termek**) nemüres halmazát.

Definíció

Herbrand struktúrának nevezünk egy olyan $\mathcal{T}_0 = (T_0, I_0, \varphi)$ struktúrát, melyben

$$I_0(f)(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$$

minden f n-rangú függvényszimbólumra és $t_1, \ldots, t_n$ alaptermre. A predikátumszimbólumok interpretációja és φ nem rögzítettek.

Lemma

Tetszőleges t alaptermre

$$\mathcal{T}_0(t) = t.$$

Bizonyítás

A t felépítése szerinti indukcióval.

Lemma

Tetszőleges F formulára, x változóra és t alaptermre

$$\mathcal{T}_0(F[x/t]) = \mathcal{T}_{0[x \mapsto t]}(F).$$

Bizonyítás

A helyettesítési lemmát alkalmazzuk.

$$\begin{aligned} \mathcal{T}_0(F[x/t]) &= \mathcal{T}_{0[x \mapsto \mathcal{T}_0(t)]}(F) \\ &= \mathcal{T}_{0[x \mapsto t]}(F). \end{aligned}$$

Herbrand struktúrák

Tekintsük ugyanazt az elsőrendű nyelvet, mint amelyet Church tételében megismertünk.
Minden $f_u(c)$ alaptermet, ahol $u \in A^*$, $A = \{0, 1\}$, azonosíthatunk az u szóval. Így T_0 azonosítható az A^* halmazzal.
Tetszőleges $a = 0, 1$ és u szó esetén

$$\mathcal{T}_0(f_a(f_u(c))) = au.$$

Tehát egy $\mathcal{T}_0$ Herbrand struktúra $I_0(f_a)$ függvénye felfogható, mint az $u \mapsto au$, $u \in A^*$ függvény. Ezek szerepeltek a Church tétel bizonyításában.
Tehát a Church tétel bizonyításában lényegében Herbrand struktúrával dolgoztunk (**izomorfizmus**).

Tétel

Zárt Skolem normálformák egy Σ halmaza akkor és csak akkor kielégíthető, ha létezik Herbrand modellje.

Bizonyítás

Az elegendőség nyilvánvaló.
A szükségesség bizonyításához tegyük fel, hogy Σ-nak létezik egy $\mathcal{A} = (A, I)$ modellje. Ezt felhasználva megadjuk a Σ egy $\mathcal{T}_0 = (T_0, I_0)$ Herbrand modelljét.
Legyen tetszőleges n-rangú p predikátumszimbólumra és $t_1, \ldots, t_n$ alaptermekre

$$I_0(p)(t_1, \ldots, t_n) = I(p)(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_n)).$$

Azt, hogy $\mathcal{T}_0 \models \Sigma$, úgy igazoljuk, hogy a kvantorok n száma szerinti indukcióval belátjuk, hogy $\mathcal{T}_0 \models F$, valahányszor $\mathcal{A} \models F$, minden F zárt Skolem normálformára.

Bizonyítás folytatása

$n = 0$. F felépítése szerinti indukcióval belátjuk, hogy $\mathcal{T}_0(F) = \mathcal{A}(F)$.

- $F = p(t_1, \ldots, t_m)$ alakú, ahol a t_i-k alaptermek. Ekkor

$$\begin{aligned} \mathcal{T}_0(F) &= I_0(p)(\mathcal{T}_0(t_1), \ldots, \mathcal{T}_0(t_m)) \\ &= I_0(p)(t_1, \ldots, t_m) \\ &= I(p)(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_m)) \\ &= \mathcal{A}(F). \end{aligned}$$

- $F = \uparrow, \downarrow$ nyilvánvaló.
- $F = G \bullet H$. Ekkor

$$\mathcal{T}_0(F) = \mathcal{T}_0(G) \bullet \mathcal{T}_0(H) = \mathcal{A}(G) \bullet \mathcal{A}(H) = \mathcal{A}(F).$$

- $F = \neg G$ hasonló.

Bizonyítás folytatása

$n > 0$. Ekkor F $\forall x G$ alakú. Tegyük fel, hogy $\mathcal{A} \models F$.
Ekkor tetszőleges $a \in A$ esetén $\mathcal{A}_{[x \mapsto a]} \models G$.
Így minden t alaptermre, $\mathcal{A}_{[x \mapsto \mathcal{A}(t)]} \models G$, azaz $\mathcal{A} \models G[x/t]$.
Az indukciós feltevés szerint ebből $\mathcal{T}_0 \models G[x/t]$, azaz
$\mathcal{T}_{0[x \mapsto \mathcal{T}_0(t)]} \models G$.
Mivel ez minden $t \in T_0$ alaptermre igaz, ezért $\mathcal{T}_0 \models \forall x G$, így
$\mathcal{T}_0 \models F$.

Következmény

Formulák egy Σ halmaza akkor és csak akkor kielégíthető, ha létezik megszámlálható modellje.

Bizonyítás

Az elegendőség triviális.
Tegyük fel, hogy Σ kielégíthető.
Akkor az a Σ' formulahalmaz is kielégíthető, melyet úgy kapunk, hogy Σ minden formulájában minden x szabad változót egy csak x-től függő új konstansszimbólummal helyettesítünk.
Ezek után ,,skolemizáljuk" az összes Σ'-beli formulát úgy, hogy mindig **új** függvényszimbólumokat vezetünk be.
Az előálló Δ is kielégíthető, így létezik Herbrand modellje, ami megszámlálható.
Ez egyben Σ' modellje is. Megfelelő változó-hozzárendeléssel ebből előáll a Σ egy megszámlálható modellje.

Definíció

Legyen $F = \forall x_1 \ldots \forall x_n F^*$ zárt Skolem normálforma. Az F **Herbrand kiterjesztése** az

$$E(F) = \{F^*[x_1/t_1] \ldots [x_n/t_n] : t_i \in T_0\}$$

alapformula-halmaz.

Ha Σ zárt Skolem normálformák halmaza, akkor

$$\boldsymbol{E(\Sigma) = \bigcup_{F \in \Sigma} E(F).}$$

Herbrand struktúrák

Következmény

Zárt Skolem normálformák egy Σ halmaza akkor és csak akkor kielégíthető, ha $E(\Sigma)$ kielégíthető.

Bizonyítás

1. Σ kielégíthető $\Leftrightarrow$
2. Σ-nak létezik Herbrand modellje $\Leftrightarrow$
3. Van olyan $\mathcal{T}_0$ Herbrand struktúra, hogy $\mathcal{T}_0 \models F$ minden $F \in E(\Sigma)$ formulára $\Leftrightarrow$
4. $E(\Sigma)$-nak létezik Herbrand modellje $\Leftrightarrow$
5. $E(\Sigma)$ kielégíthető.

Megjegyzés

$E(\Sigma)$ akkor és csak akkor kielégíthető, ha ítéletkalkulusi értelemben az.

Herbrand struktúrák

A fenti eredmények egyenlőséges elsőrendű logikára is érvényesek a Herbrand struktúra definíciójának megfelelő módosításával.
A módosítás abban áll, hogy nem a T_0 alaphalmazt kell venni, hanem ennek egy megfelelő kongruenciareláció szerinti **hányadosát**.
A megszámlálható modell létezésére vonatkozó eredmény függ attól, hogy a függvényszimbólumok halmaza megszámlálható.

Ismét az eldönthetőségről

Tétel

Formulák kielégíthetetlensége **félig eldönthető**: létezik olyan algoritmus, mely tetszőleges F formulára ,,igen" válasszal áll meg, ha F kielégíthetetlen, és ,,nem" válasszal áll meg, vagy nem áll meg, ha F kielégíthető.

Bizonyítás

Készítsünk F-fel s-ekvivalens zárt Skolem normálformát. Jelölje ezt G.
Végtelen ciklusban generáljuk $n = 1, 2, \ldots$-re $E(G)$ első n elemét: $G_1, \ldots, G_n$. (Ha $E(G)$ véges, valahonnan ugyanazokat a formulákat generáljuk.)
Ha $\{G_1, \ldots, G_n\}$ valamely n-re kielégíthetetlen, akkor G és F is. $\{G_1, \ldots, G_n\}$ akkor és csak akkor kielégíthetetlen, ha az ítéletkalkulusi értelemben az. Ez eldönthető.
Ekvivalens megfogalmazás: A kielégíthetetlen formulák halmaza rekurzívan felsorolható: létezik olyan algoritmus, mely felsorolja a kielégíthetetlen formulákat.

Következmény

A kielégíthető formulák halmaza **nem** félig eldönthető.

Bizonyítás

Ellenkező esetben a kielégíthetőség eldönthető lenne, ami ellentmond Church tételének.
Tegyük fel, hogy a kielégíthetőség félig eldönthető egy A algoritmussal. Legyen B a kielégíthetetlenséget félig eldöntő B algoritmus.
Adott F formulára futtassuk az A és B algoritmust párhuzamosan lépésenként. Valamelyik ,,igen" válasszal megáll F-en. Ha ez az A algoritmus, akkor F kielégíthető. Ha ez a B, akkor F kielégíthetetlen.

Megjegyzés

Ha egy probléma és ellentettje is félig eldönthető, akkor a probléma eldönthető.

Következmény

A tautológiák halmaza rekurzívan felsorolható.

Bizonyítás

F akkor és csak akkor tautológia, ha $\neg F$ kielégíthetetlen.

Következmény

Legyen Σ véges halmaz. Azon F formulák halmaza, melyekre $\Sigma \models F$, rekurzívan felsorolható.

Bizonyítás

Legyen $\Sigma = \{F_1, \ldots, F_n\}$. $\Sigma \models F$ akkor és csak akkor, ha

$$(F_1 \wedge \ldots \wedge F_n) \to F$$

tautológia.

Megjegyzés

Az előző állítás akkor is igaz, ha Σ rekurzívan felsorolható.

A kompaktsági tétel

A kompaktsági tétel

Tétel

Egy Σ formulahalmaz akkor és csak akkor kielégíthető, ha minden véges részhalmaza az.

Bizonyítás

A szükségesség nyilvánvaló. Az elegendőség bizonyítása:
Minden formulában minden szabad változó helyébe helyettesítsünk egy **új**, csak a változótól függő konstansszimbólumot. Ezáltal elérhető, hogy Σ mondatokból álljon.
Minden Σ-beli mondatot hozzunk Skolem normálformára **új** függvényszimbólumok segítségével.
Σ akkor és csak akkor kielégíthető, ha az előálló Σ' az. (Σ' minden modellje a Σ modellje is, és Σ minden modelljéhez elkészíthető a Σ' egy modellje.)
Teljesen hasonlóan, a Σ egy véges Σ_0 részhalmaza akkor és csak akkor kielégíthető, ha a belőle előálló Σ_0' az.

Bizonyítás folytatása

De Σ minden véges részhalmaza kielégíthető, így a Σ' és az $E(\Sigma')$ minden véges részhalmaza is.
Az ítéletkalkulus kompaktsági tétele szerint így $E(\Sigma')$ kielégíthető.
Így Σ' és Σ is kielégíthetőek.

Következmény

Legyen Σ formulák egy halmaza, F egy formula. $\Sigma \models F$ akkor és csak akkor teljesül, ha létezik olyan véges $\Sigma_0 \subseteq \Sigma$ halmaz, hogy $\Sigma_0 \models F$.

A kompaktsági tétel

Ebben a részben struktúrán $\mathcal{A} = (A, I)$ alakú rendezett párt értünk, tehát elhagyjuk a változó-hozzárendelést. Ha $\mathcal{K}$ struktúrák osztálya, Σ mondatok halmaza és $\mathcal{A} \models \Sigma$ minden $\mathcal{A} \in \mathcal{K}$ struktúrára, akkor azt is írjuk, hogy $\mathcal{K} \models \Sigma$.

Mint korábban, ha $\mathcal{K}$ struktúrák egy osztálya, akkor $\mathrm{Th}(\mathcal{K})$ jelöli a $\mathcal{K}$ elméletét, azaz azon mondatok halmazát, melyek teljesülnek minden $\mathcal{K}$-beli struktúrában:

$$\mathrm{Th}(\mathcal{K}) = \{F : \mathcal{K} \models F\}.$$

Ha pedig Σ mondatok halmaza, akkor $\mathrm{Mod}(\Sigma)$ azon struktúrák osztálya, melyekben érvényes Σ:

$$\mathrm{Mod}(\Sigma) = \{\mathcal{A} : \mathcal{A} \models \Sigma\}.$$

Példa

$\mathcal{N} = (N, +, \cdot, \underline{0}, \underline{1}, <)$ a természetes számok szokásos struktúrája, $\mathbf{Ar} = \mathrm{Th}(\mathcal{N})$.

A kompaktsági tétel

Állítás

Ar-nak létezik olyan (megszámlálható) modellje, mely **nem izomorf** az $\mathcal{N}$ struktúrával (nemsztenderd modell).

Bizonyítás

Legyen c új konstansszimbólum és jelölje $\underline{n}$ az $(((\underline{1}+\underline{1})+\underline{1})+\ldots+\underline{1})$ termet minden n természetes számra. (Az $\underline{1}$ n-szer szerepel. Ha $n=0$, akkor ez a term $\underline{0}$.)
Minden adott n_0-ra $\mathbf{Ar} \cup \{\neg(c=\underline{n}) : 0 \leq n \leq n_0\}$ érvényes abban a struktúrában, melyet úgy kapunk, hogy $\mathcal{N}$-ben a c konstansjelet n_0-nál nagyobb számmal interpretáljuk.
Így a kompaktsági tétel miatt a $\Sigma = \mathbf{Ar} \cup \{\neg(c=\underline{n}) : n \geq 0\}$ halmaz kielégíthető, azaz létezik modellje.
De Σ minden modellje végtelen. Ezért létezik megszámlálhatóan végtelen modellje.
Egy ilyen struktúra $\mathbf{Ar}$ nemsztenderd megszámlálható modellje.

Állítás

Egyenlőséges nyelvben legyen Σ olyan mondathalmaz, melynek minden n természetes számra létezik legalább n elemszámú véges modellje. Akkor Σ-nak létezik megszámlálhatóan végtelen modellje.

Bizonyítás

Legyen adott n-re F_n olyan mondat, mely azt fejezi ki, hogy legalább n elem van, pl.

$$\exists x_1 \dots \exists x_n \bigwedge_{i<j} \neg(x_i = x_j).$$

A kompaktsági tétel felhasználásával a $\Sigma' = \Sigma \cup \{F_n : n \geq 1\}$ halmaz kielégíthető, így van megszámlálható modellje, mondjuk $\mathcal{A}$. $\mathcal{A}$ nem lehet véges, így a Σ megszámlálhatóan végtelen modellje.

Következmény

Ha a struktúrák egy $\mathcal{K}$ osztályában minden n-re létezik legalább n számosságú véges struktúra, akkor a $\mathcal{K}$-ban lévő véges modellek osztálya nem gyengén axiomatizálható.

Bizonyítás

Az állítás az, hogy nem létezik olyan Σ mondathalmaz, hogy $\mathrm{Mod}(\Sigma)$ pontosan a $\mathcal{K}$-beli véges struktúrák halmaza. Ez nyilvánvaló az előző állításból.

A kompaktsági tétel

Állítás

Ha $\mathcal{K} = \mathrm{Mod}(\Sigma)$ és ha $\mathcal{K}$ végesen axiomatizálható, akkor létezik olyan $\Sigma_0 \subseteq \Sigma$ véges halmaz, melyre $\mathcal{K} = \mathrm{Mod}(\Sigma_0)$.

Bizonyítás

Röviden kimondva azt kell igazolnunk, hogy végesen axiomatizálható osztály minden axiómarendszere tartalmaz véges axiómarendszert.
Legyen Δ véges axiómarendszer. Ekkor $\Sigma \models F$ teljesül minden $F \in \Delta$ formulára.
Mivel Δ véges, a kompaktsági tétel felhasználásával adódik, hogy van olyan $\Sigma_0 \subseteq \Sigma$ véges halmaz, hogy minden $F \in \Delta$ formulára $\Sigma_0 \models F$.
$\mathrm{Mod}(\Sigma_0) \supseteq \mathrm{Mod}(\Sigma) = \mathcal{K}$.
$\mathrm{Mod}(\Sigma_0) \subseteq \mathrm{Mod}(\Delta) = \mathcal{K}$.

Állítás

A struktúrák egy $\mathcal{K}$ osztálya akkor és csak akkor végesen axiomatizálható, ha $\mathcal{K}$ és a $\mathcal{K}$ komplemense, $\overline{\mathcal{K}}$ is gyengén axiomatizálható.

Bizonyítás

Szükségesség: triviális.
Elegendőség: tegyük fel, hogy $\mathcal{K} = \mathrm{Mod}(\Sigma)$ és $\overline{\mathcal{K}} = \mathrm{Mod}(\Delta)$.

$$\mathrm{Mod}(\Sigma \cup \Delta) = \mathrm{Mod}(\Sigma) \cap \mathrm{Mod}(\Delta) = \emptyset.$$

A kompaktsági tétel miatt így van olyan $\Sigma_0 \subseteq \Sigma$ és $\Delta_0 \subseteq \Delta$ véges halmaz, hogy

$$\mathrm{Mod}(\Sigma_0) \cap \mathrm{Mod}(\Delta_0) = \mathrm{Mod}(\Sigma_0 \cup \Delta_0) = \emptyset.$$

Mivel $\mathrm{Mod}(\Sigma_0) \supseteq \mathcal{K}$, $\mathrm{Mod}(\Delta_0) \supseteq \overline{\mathcal{K}}$ és $\mathrm{Mod}(\Sigma_0) \cap \mathrm{Mod}(\Delta_0) = \emptyset$, ezért $\mathrm{Mod}(\Sigma_0) = \mathcal{K}$, $\mathrm{Mod}(\Delta_0) = \overline{\mathcal{K}}$.

Példa

Minden p prímszámra a p karakterisztikájú testek osztálya végesen axiomatizálható: $\mathcal{F} \cup \{\underline{p} = \underline{0}\}$, ahol $\mathcal{F}$ a test axiómák véges halmaza.

Példa

A 0 karakterisztikájú testek osztálya gyengén axiomatizálható, de nem axiomatizálható végesen.
Valóban, egy axiómarendszer: $\mathcal{F} \cup \{\neg(\underline{p} = \underline{0}) : p \text{ prímszám}\}$. Ez nem tartalmaz véges axiómarendszert, mert minden p prímszámra létezik p karakterisztikájú test.

Példa

Így a pozitív karakterisztikájú testek osztálya nem gyengén axiomatizálható.

Alap rezolúció

Alap rezolúció

Legyen Σ zárt Skolem normálformák halmaza úgy, hogy minden Σ-beli formula magja konjunktív normálforma. Az előzőek szerint Σ akkor és csak akkor kielégíthetetlen, ha $E(\Sigma)$ az. Jelölje $\boldsymbol{E'(\Sigma)}$ az $E(\Sigma)$-beli formulák klózainak halmazát. Az ítéletkalkulus rezolúciós tételéből kapjuk az alábbi eredményt.

Tétel

Σ akkor és csak akkor kielégíthetetlen, ha $E'(\Sigma)$-ból levezethető az üres klóz az alábbi **alap rezolúciós szabállyal**:

$$\frac{C_1 \cup \{\ell\}, \quad C_2 \cup \{\neg\ell\}}{C_1 \cup C_2},$$

ahol C_1, C_2 alap klózok és ℓ alap literál.

Példa

$\Sigma = \{F\}, \quad F = \forall x\big(p(x) \wedge \neg p(f(x))\big).$
$T_0 = \{a, f(a), f^2(a), \ldots, f^n(a), \ldots\}.$
$E'(\Sigma) = \{\{p(a)\}, \{\neg p(f(a))\}, \{p(f(a))\}, \{\neg p(f(f(a)))\}, \ldots\}$

1. $\{p(f(a))\}$, $E'(\Sigma)$ klóza
2. $\{\neg p(f(a))\}$, $E'(\Sigma)$ klóza
3. $\square$, 1 és 2, rezolúcióval

Példa

$\Sigma = \{F\}, F =$
$\forall x \forall y \big((\neg p(x) \vee \neg p(f(a)) \vee q(y)) \ \wedge \ p(y) \ \wedge \ (\neg p(g(b,x)) \vee \neg q(b)) \big)$

1. $\{\neg p(f(a)), q(b)\}$
2. $\{p(f(a))\}$
3. $\{q(b)\}$, 1. és 2.
4. $\{p(g(b,a))\}$
5. $\{\neg p(g(b,a)), \neg q(b)\}$
6. $\{\neg q(b)\}$, 4. és 5.
7. $\square$, 3. és 6.

Az alapklózok használata elkerülhető.

Példa

$\Sigma = \{F\}$, $F = \forall x \forall y \big(p(x, g(y)) \wedge \neg p(f(y), x)\big)$
$C_1 = \{p(x, g(y))\}$, $C_2 = \{\neg p(f(y), x)\}$

1. $\{p(f(z), g(y))\}$, $C_1[x/f(z)]$ helyettesítéssel
2. $\{\neg p(f(z), g(y))\}$, $C_2[y/z][x/g(y)]$ helyettesítéssel
3. $\square$, 1. és 2.

Egyesítés

Definíció

Legyen $s = [x_1/t_1] \dots [x_n/t_n]$ helyettesítések sorozata. Ekkor tetszőleges t termre a ts termet n szerinti indukcióval definiáljuk:

- $n = 0$: $ts = t$.
- $n > 0$: $ts = (t[x_1/t_1] \dots [x_{n-1}/t_{n-1}])[x_n/t_n]$.

Az $n = 0$ esetben s-et []-val is jelöljük. Ha a t_i-k mindegyike alapterm, s-et **alaphelyettesítésnek** nevezzük.

Példa

$$\begin{aligned} f(x, g(y))[x/g(y)][y/a] &= f(g(a), g(a)) \\ f(x, g(y))[y/a][x/g(y)] &= f(g(y), g(a)) \end{aligned}$$

Definíció

Legyen ℓ literál, C klóz (azaz literálok véges halmaza), s helyettesítés. Ekkor

$$\ell s = \begin{cases} p(t_1 s, \ldots, t_n s), & \text{ha } \ell = p(t_1, \ldots, t_n) \\ \neg p(t_1 s, \ldots, t_n s) & \text{ha } \ell = \neg p(t_1, \ldots, t_n). \end{cases}$$

Továbbá $Cs = \{\ell s : \ell \in C\}$.

Definíció

Legyen $C = \{\ell_1, \ldots, \ell_n\}$ klóz, s helyettesítés. Azt mondjuk, hogy s a C **egyesítője**, ha $\ell_1 s = \ldots = \ell_n s$. Azt mondjuk, hogy C **egyesíthető**, ha létezik egyesítője.

Példa

A $C = \{p(g(x), y), p(y, g(a))\}$ klóz egyesíthető:

$$\begin{aligned} p(g(x), y)[y/g(x)][x/a] &= p(g(a), g(a)) \\ p(y, g(a))[y/g(x)][x/a] &= p(g(a), g(a)) \end{aligned}$$

Lemma

Legyenek ℓ_1, ℓ_2 literálok, $\ell_1 \neq \ell_2$. Így létezik olyan pozíció, ahol ℓ_1 és ℓ_2 különböznek. Ha $\{\ell_1, \ell_2\}$ egyesíthető, akkor

- az első olyan pozíción, ahol különböznek, az egyik literálban egy változó van,
- a másik literálban pedig olyan t term első szimbóluma, amelyben ez a változó nem fordul elő.

Tétel

Létezik olyan algoritmus, mely tetszőleges C klózra eldönti, hogy C egyesíthető-e, és ha egyesíthető, akkor elkészít egy **legáltalánosabb egyesítőt**, azaz egy olyan s egyesítőt, hogy valahányszor s' egy másik egyesítő, $s' = ss''$ valamely s'' helyettesítésre.

Megjegyzés

A legáltalánosabb egyesítő, ha létezik, lényegében egyértelműen meghatározott.

Az egyesítési algoritmus

- $s := []$.
- Mindaddig, míg $|Cs| > 1$,
  1. Hasonlítsuk össze Cs elemeit, és keressük meg az első olyan pozíciót, ahol két literál különbözik.
  2. Ha ezen a pozíción egyik literálban sem változó van, akkor C nem egyesíthető.
  3. Ha az egyik literál mondjuk az x változót tartalmazza ezen a pozíción, a másik literálban pedig egy t term első szimbóluma áll, akkor
     - ha x előfordul t-ben, akkor C nem egyesíthető,
     - különben legyen $s := s[x/t]$.
- Ha a ciklus sikeresen lefut, s a C legáltalánosabb egyesítője.

Példa

$C = \{\neg p(f(z, g(a, y)), h(z)), \neg p(f(f(u, v), w), h(f(a, b)))\}$

$s_0 = [].$

$s_1 = [z/f(u, v)].$

$$Cs_1 = \{ \neg p(f(f(u, v), g(a, y)), h(f(u, v))), \neg p(f(f(u, v), w), h(f(a, b)))\}$$

$s_2 = s_1[w/g(a, y)] = [z/f(u, v)][w/g(a, y)].$

$$Cs_2 = \{ \neg p(f(f(u, v), g(a, y)), h(f(u, v))), \neg p(f(f(u, v), g(a, y)), h(f(a, b)))\}$$

$s_3 = s_2[u/a].$

$s_4 = s_3[v/b] = [z/f(u, v)][w/g(a, y)][u/a][v/b].$

$$Cs_4 = \{\neg p(f(f(a, b), g(a, y)), h(f(a, b)))\}.$$

C egyesíthető, s_4 a legáltalánosabb egyesítő.

Elsőrendű rezolúció

Definíció

Legyenek C_1 és C_2 klózok. Egy R klózt a C_1 és C_2 **rezolvensének** nevezünk, ha:

- Léteznek olyan s_1, s_2 **változóátnevezések**, hogy $C_1 s_1$ és $C_2 s_2$ nem tartalmaznak közös változót.
- Léteznek olyan $\ell_1, \ldots, \ell_m \in C_1 s_1$ és $\ell'_1, \ldots, \ell'_n \in C_2 s_2$ literálok, ahol $m, n \geq 1$, hogy
$$C = \{\ell_1, \ldots, \ell_m, \overline{\ell'_1}, \ldots, \overline{\ell'_n}\}$$
egyesíthető az s legáltalánosabb egyesítővel, és ezek az összes olyan literálok, amelyeket az s egyesít.
- $$R = \big((C_1 s_1 - \{\ell_1, \ldots, \ell_m\}) \cup (C_2 s_2 - \{\ell'_1, \ldots, \ell'_n\})\big) s.$$

Példa

$C_1 = \{p(f(x)), \neg q(z), p(z)\}$ és $C_2 = \{\neg p(x), r(g(x), a)\}$ egy rezolvense

$$R = \{\neg q(f(x)), r(g(f(x), a))\}.$$

Ehhez először C_2-ben nevezzük át x-et y-ra.

$$\begin{aligned} C_1 s_1 &= \{p(f(x)), \neg q(z), p(z)\} \\ C_2 s_2 &= \{\neg p(y), r(g(y), a)\} \end{aligned}$$

Tekintsük a $\{p(f(x)), p(z), p(y)\}$ klózt.
Legáltalánosabb egyesítő: $s = [z/f(x)][y/f(x)]$.

$$\big((C_1 s_1 - \{p(f(x)), p(z)\}) \cup (C_2 s_2 - \{\neg p(y)\})\big) s = R.$$

Definíció

Legyen Σ klózok halmaza.

$$\begin{aligned}
\mathbf{Res}^0(\Sigma) &= \Sigma \\
\mathbf{Res}^{n+1}(\Sigma) &= \mathbf{Res}^n(\Sigma) \cup \{R : \exists C_1, C_2 \in \mathbf{Res}^n(\Sigma), \\
&\quad R \text{ a } C_1 \text{ és } C_2 \text{ egy rezolvense}\} \\
\mathbf{Res}^*(\Sigma) &= \bigcup_{n \geq 0} \mathbf{Res}^n(\Sigma).
\end{aligned}$$

Tudjuk, hogy $\mathbf{Res}^*(\Sigma)$ a legszűkebb olyan klózhalmaz, mely tartalmazza Σ-t és zárt az elsőrendű rezolúcióra.

Elsőrendű rezolúció

Definíció

Az alábbiakban azt mondjuk, hogy klózok egy Σ halmaza kielégíthető, vagy kielégíthetetlen, ha univerzális lezártjaik halmaza az.

Tétel (az elsőrendű logika rezolúciós tétele)

Klózok egy Σ halmaza akkor és csak akkor kielégíthetetlen, ha $\square \in \mathbf{Res}^*(\Sigma)$.

Átfogalmazás

Klózok egy Σ halmaza akkor és csak akkor kielégíthetetlen, ha $\square$ levezethető Σ-ból a rezolúciós szabály ismételt felhasználásával.

Példa

$$\begin{aligned} F \quad = \forall x \forall y \forall z \quad & \big((\neg p(x) \vee q(x) \vee r(x, f(x))) \\ & \wedge (\neg p(x) \vee q(x) \vee s(f(x))) \\ & \wedge p(a) \wedge t(a) \wedge (\neg r(a, z) \vee t(z)) \\ & \wedge (\neg t(x) \vee \neg q(x)) \wedge (\neg t(y) \vee \neg s(y))\big) \end{aligned}$$

F kielégíthetetlen-e?

$$\begin{aligned} \Sigma \quad = \big\{ \quad & \{\neg p(x), q(x), r(x, f(x))\}, \{\neg p(x), q(x), s(f(x))\}, \\ & \{p(a)\}, \{t(a)\}, \{\neg r(a, z), t(z)\}, \\ & \{\neg t(x), \neg q(x)\}, \{\neg t(y), \neg s(y)\}\big\} \end{aligned}$$

Σ kielégíthetetlen-e?

1. $\{\neg t(x), \neg q(x)\}$
2. $\{t(a)\}$
3. $\{\neg q(a)\}$ (1,2)
4. $\{p(a)\}$
5. $\{\neg p(x), q(x), s(f(x))\}$
6. $\{q(a), s(f(a))\}$ (4,5)
7. $\{\neg p(x), q(x), r(x, f(x))\}$
8. $\{s(f(a))\}$ (3,6)
9. $\{q(a), r(a, f(a))\}$ (4,7)
10. $\{r(a, f(a))\}$ (3,9)
11. $\{\neg r(a, z), t(z)\}$
12. $\{t(f(a))\}$ (10,11)
13. $\{\neg t(y), \neg s(y)\}$
14. $\{\neg s(f(a))\}$ (12,13)
15. $\square$ (8,14)

Lemma (Lift lemma)

Legyenek C_1, C_2 klózok, és legyenek C_1' és C_2' a C_1 és C_2 alappéldányai. Ha R' a C_1' és C_2' egy rezolvense (az ítéletkalkulusi értelemben), akkor létezik a C_1 és C_2 egy olyan R rezolvense, melynek R' egy alappéldánya.

Bizonyítás

Legyenek s_1 és s_2 olyan változóátnevezések, hogy $C_1 s_1$ és $C_2 s_2$ változói különböznek.
Világos, hogy C_1' és C_2' rendre a $C_1 s_1$ és $C_2 s_2$ alappéldányai is.
Továbbá létezik olyan s alaphelyettesítés, hogy $C_1' = C_1 s_1 s$, $C_2' = C_2 s_2 s$.
Mivel R' a C_1' és C_2' egy rezolvense, létezik olyan ℓ alapliterál, hogy

$$\ell \in C_1', \overline{\ell} \in C_2', \quad R' = (C_1' - \{\ell\}) \cup (C_2' - \{\overline{\ell}\}).$$

Bizonyítás folytatása

Mivel $\ell \in C_1' = C_1 s_1 s$, léteznek olyan $\ell_1, \ldots, \ell_m \in C_1 s_1$ literálok, ahol $m > 0$, hogy

$$\ell = \ell_1 s = \ldots = \ell_m s.$$

Hasonlóan, léteznek olyan $\ell_1', \ldots, \ell_n' \in C_2 s_2$, $n > 0$ literálok, hogy

$$\overline{\ell} = \ell_1' s = \ldots = \ell_n' s.$$

Mivel $C = \{\ell_1, \ldots, \ell_m, \overline{\ell_1'}, \ldots, \overline{\ell_n'}\}$ egyesíthető, ezért létezik a C_1 és C_2 alábbi R rezolvense.

Legyen s_0 a C legáltalánosabb egyesítője. Ekkor

$$R = \big((C_1 s_1 - \{\ell_1, \ldots, \ell_m\}) \cup (C_2 s_2 - \{\ell_1', \ldots, \ell_n'\})\big) s_0.$$

Bizonyítás folytatása

Mivel s_0 a legáltalánosabb egyesítő, létezik olyan r helyettesítés, hogy $s = s_0 r$.

Ekkor:

$$\begin{aligned} R' &= (C_1' - \{\ell\}) \cup (C_2' - \{\bar{\ell}\}) \\ &= (C_1 s_1 s - \{\ell\}) \cup (C_2 s_2 s - \{\bar{\ell}\}) \\ &= \big((C_1 s_1 - \{\ell_1, \ldots, \ell_m\}) \cup (C_2 s_2 - \{\ell_1', \ldots, \ell_n'\})\big) s \\ &= \big((C_1 s_1 - \{\ell_1, \ldots, \ell_m\}) \cup (C_2 s_2 - \{\ell_1', \ldots, \ell_n'\})\big) s_0 r \\ &= Rr. \end{aligned}$$

Tehát R' a C_1 és C_2 egy rezolvensének alappéldánya.

A rezolúciós tétel bizonyítása

Elegendőség

Tetszőleges F formula univerzális lezártját jelölje $\forall F$.

Elegendő azt megmutatni, hogy amennyiben R a C_1 és C_2 egy rezolvense, akkor $\{\forall C_1, \forall C_2\} \models \forall R$.

Legyen

$$\begin{aligned} R &= \big((C_1 s_1 - \{\ell_1, \ldots, \ell_m\}) \cup (C_2 s_2 - \{\ell'_1, \ldots, \ell'_n\})\big) s \\ &= (C_1 s_1 s - \{\ell\}) \cup (C_2 s_2 s - \{\overline{\ell}\}), \end{aligned}$$

ahol s az $\{\ell_1, \ldots, \ell_m, \overline{\ell'_1}, \ldots, \overline{\ell'_n}\}$ legáltalánosabb egyesítője és $\ell = \ell_1 s$.

Bizonyítás folytatása

Tegyük fel, hogy $\mathcal{A} \models \forall C_1$ és $\mathcal{A} \models \forall C_2$, de $\mathcal{A} \not\models \forall R$.
Ekkor létezik olyan $\mathcal{A}'$ struktúra, mely abban különbözik $\mathcal{A}$-tól, hogy a változóknak is értéket ad, és amelyre $\mathcal{A}' \not\models R$.
Ekkor $\mathcal{A}' \not\models C_1 s_1 s - \{\ell\}$ és $\mathcal{A}' \not\models C_2 s_2 s - \{\overline{\ell}\}$, mert különben $\mathcal{A} \models R$ (hiszen $(C_1 s_1 s - \{\ell\}) \cup (C_2 s_2 s - \{\overline{\ell}\})$ az R alappéldánya).
Ugyanakkor, mivel $\mathcal{A} \models \forall C_1$ és $\mathcal{A} \models \forall C_2$, ezért $\mathcal{A}' \models C_1 s_1 s$ és $\mathcal{A}' \models C_2 s_2 s$.
Így $\mathcal{A}' \models \ell$ és $\mathcal{A}' \models \overline{\ell}$. Ellentmondás.

Szükségesség (teljesség)
Tegyük fel, hogy Σ kielégíthetetlen.
Az alaprezolúciós tétel szerint létezik az alapklózok olyan $C'_1, \ldots, C'_n = \square$ sorozata, hogy minden i-re C'_1 egy Σ-beli klóz alappéldánya, vagy valamely $j < k < i$-re a C'_j és C'_k rezolvense.
A lift lemma felhasználásával ebből elkészíthető a klózok egy olyan $C_1, \ldots, C_n$ sorozata, hogy minden i-re C'_i a C_i egy példánya, és minden i-re $C_i \in \Sigma$ vagy valamely $j, k < i$ mellett a C_i a C_j és C_k egy rezolvense.

Lineáris rezolúció

Definíció

Legyen Σ klózok halmaza. Azt mondjuk, hogy egy C klóz **lineáris** rezolúcióval levezethető Σ-ból, ha létezik egy olyan

$$C_0, \ldots, C_n$$

klózsorozat, hogy $C_0 \in \Sigma$, $C_n = C$, és $i > 0$ esetén C_i a C_{i-1} és egy $\Sigma \cup \{C_0, \ldots, C_{i-1}\}$-beli ún. **oldalklóz** rezolvense. A C_0 klózt a levezetés **bázisának** nevezzük.

Példa

$\Sigma = \{\{p, q\}, \{p, \neg q\}, \{\neg p, q\}, \{\neg p, \neg q\}\}$.
Lineáris rezolúciós levezetés:

1. $\{p, q\}$
2. $\{p\}$ 1.,$\{p, \neg q\}$
3. $\{q\}$ 2.,$\{\neg p, q\}$
4. $\{\neg p\}$ 3.,$\{\neg p, \neg q\}$
5. $\square$ 4.,2.

Lineáris rezolúció

Ha lineáris rezolúcióval levezethető Σ-ból $\square$, akkor rezolúcióval is, így Σ kielégíthetetlen (azaz a Σ-beli klózok univerzális lezártjainak halmaza kielégíthetetlen).

A fordított irányú állítás a lineáris rezolúció teljessége. Ennek igazolásához, a lift lemma miatt, szorítkozhatunk az ítéletkalkulus klózaira.

Definíció

Legyen Σ az ítéletkalkulus klózainak halmaza, ℓ egy literál.

- $\Sigma_{\ell=0}$ az a halmaz, melyet úgy kapunk Σ-ból, hogy elhagyunk minden $\overline{\ell}$-et tartalmazó klózt, majd a maradék klózokból elhagyjuk ℓ minden előfordulását.
- $\Sigma_{\ell=1}$ az a halmaz, melyet úgy kapunk Σ-ból, hogy elhagyunk minden ℓ-et tartalmazó klózt, majd a maradék klózokból elhagyjuk $\overline{\ell}$ minden előfordulását.

Világos, hogy $\mathcal{A} \models \Sigma$ akkor és csak akkor, ha $\mathcal{A}(\ell) = 1$ és $\mathcal{A} \models \Sigma_{\ell=1}$, vagy $\mathcal{A}(\ell) = 0$ és $\mathcal{A} \models \Sigma_{\ell=0}$.

Így Σ akkor és csak akkor kielégíthető, ha $\Sigma_{\ell=0}$ vagy $\Sigma_{\ell=1}$ kielégíthető.

Tétel (A lineáris rezolúció helyességi és teljességi tétele)

Klózok egy Σ halmaza akkor és csak akkor kielégíthetetlen, ha Σ-ból levezethető az üres klóz lineáris rezolúcióval.

Bizonyítás

Csak az ítéletkalkulus esetére.
Az elegendőség nyilvánvaló.
A szükségesség bizonyításához tegyük fel, hogy Σ kielégíthetetlen.
A kompaktsági tétel miatt az is feltehető, hogy Σ véges.
A Σ-ban szereplő változók n száma szerinti indukcióval belátjuk az alábbit:

Ha $\Sigma' \subseteq \Sigma$ minimális kielégíthetetlen halmaz és $C \in \Sigma'$, akkor $\square$ levezethető Σ'-ből olyan lineáris rezolúciós levezetéssel, melynek bázisa C.

$n = 0$. Ekkor $\Sigma = \{\square\}$ és az állítás nyilvánvaló.

Bizonyítás folytatása

$n > 0$. Legyen $\Sigma' \subseteq \Sigma$ minimális kielégíthetetlen halmaz. Ha Σ'-ben $\leq n-1$ változó fordul elő, akkor az indukciós feltevés alkalmazásával készen vagyunk. Tegyük tehát fel, hogy Σ'-ben n változó fordul elő. Legyen $C \in \Sigma'$.

1. eset. $|C| = 1$, azaz $C = \{\ell\}$ valamely ℓ literálra.

Ekkor $\Sigma'_{\ell=1}$ kielégíthetetlen.

Legyen Σ'' a $\Sigma'_{\ell=1}$ minimális kielégíthetetlen részhalmaza.

Létezik olyan $C' \in \Sigma''$ klóz, amelyre $C' \cup \{\overline{\ell}\} \in \Sigma'$.

(Ellenkező esetben Σ'' a $\Sigma' - \{C\}$ kielégíthetetlen részhalmaza, ellentmondva Σ' minimalitásának.)

Bizonyítás folytatása

Mivel Σ''-ben legfeljebb $n-1$ változó fordul elő, létezik Σ'' feletti $C' = C_0, C_1, \ldots, C_m = \square$ lineáris rezolúciós levezetés.
Mivel C' a $C = \{\ell\}$ és $C' \cup \{\bar{\ell}\}$ Σ'-beli klózok rezolvense, ezért $C, C', C_1, \ldots, C_m = \square$ a $\Sigma' \cup \Sigma''$ feletti lineáris rezolúciós levezetés.

Bizonyítás folytatása

Vegyük vissza a C_i, $i \geq 1$ klózokba az $\overline{\ell}$ literált, ahol esetleg elhagytuk. Így egy Σ'-feletti $C, C', C'_1, \ldots, C'_m$ lineáris rezolúciós levezetéshez jutunk, ahol $C'_m = \square$ vagy $C'_m = \{\overline{\ell}\}$.
Ha $C'_m = \square$, készen vagyunk. Ha $C'_m = \{\overline{\ell}\}$, akkor a sorozatot az üres klózzal folytatva Σ' feletti lineáris levezetéshez jutunk (mert $\{\ell\} \in \Sigma'$).

Bizonyítás folytatása

2. eset $|C| > 1$. Legyen $\ell \in C$, $C' = C - \{\ell\}$.
Ekkor $C' \in \Sigma'_{\ell=0}$.
$\Sigma'_{\ell=0} - \{C'\}$ kielégíthető. (Valóban, mivel $\Sigma' - \{C\}$ kielégíthető, létezik olyan $\mathcal{A}$, melyre $\mathcal{A} \models \Sigma' - \{C\}$. Mivel $\mathcal{A} \not\models \Sigma'$, ezért $\mathcal{A} \not\models C$. Így $\ell \in C$ miatt $\mathcal{A}(\ell) = 0$. Következésképp $\mathcal{A} \models \Sigma'_{\ell=0} - \{C'\}$.)
Ugyanakkor $\Sigma'_{\ell=0}$ kielégíthetetlen. Legyen Σ'' a $\Sigma'_{\ell=0}$ minimális kielégíthetetlen részhalmaza. Az előzőek miatt $C' \in \Sigma''$.
Az indukciós feltevés miatt létezik Σ'' felett egy $C' = C_0, C_1, \ldots, C_m = \square$ lineáris rezolúciós levezetés.

Bizonyítás folytatása

Vegyük vissza ℓ-et mindenhova, ahonnan elhagytuk. Így előáll egy Σ' feletti $C = C'_0, C'_1, \ldots, C'_m$ lineáris rezolúciós levezetés.
Ha $C'_m = \square$, készen vagyunk. Ellenkező eseten $C'_m = \{\ell\}$.
Már láttuk, hogy a $\Sigma' - \{C\}$ minden modellje 0-t rendel ℓ-hez.
Ezért $(\Sigma' - \{C\}) \cup \{\ell\}$ kielégíthetetlen.
Az 1. eset szerint létezik $(\Sigma' - \{C\}) \cup \{\ell\}$ felett egy $\{\ell\} = C''_0, C''_1, \ldots, C''_k = \square$ lineáris rezolúciós levezetés.
Feltehető, hogy $C''_1, \ldots, C''_k$ $\{\ell\}$-től különböznek.
$C = C'_0, C'_1, \ldots, C'_m = \{\ell\}, C''_1, \ldots, C''_k = \square$ a keresett levezetés.

SLD rezolúció

SLD rezolúció

Csak Horn-klózok halmazaira teljes.
(Logikai programozásban fontos eset.)

Definíció

Horn-klóz: olyan klóz, melyben legfeljebb egy literál pozitív.
Negatív klóz: minden literál negatív.
Program klóz vagy **definit klóz**: nem negatív Horn-klóz.

Definíció

Legyen Σ Horn-klózok halmaza. Egy $C_0, C_1, \ldots, C_n$ Σ feletti lineáris rezolúciós levezetést **SLD levezetésnek** nevezünk, ha C_0 negatív klóz.

Így $i > 0$ esetén a C_i a C_{i-1} és egy Σ-beli program klóz rezolvense.

Tétel

Legyen Σ Horn-klózok halmaza. Ha a $C \in \Sigma$ negatív bázisklózból levezethető az üres klóz, akkor Σ kielégíthetetlen. Fordítva, ha a C negatív klóz benne van Σ valamely minimális kielégíthetetlen részhalmazában, akkor az üres klóz SLD rezolúcióval levezethető Σ felett a C bázisklózból.

Bizonyítás

Az 1. állítás nyilvánvaló. A 2. bizonyításához tekintsünk egy olyan minimális kielégíthetetlen Σ' részhalmazt, mely tartalmazza C-t. Az előző tétel bizonyítása szerint létezik olyan Σ' feletti lineáris rezolúciós levezetése az üres klóznak, melynek bázisa C. Ez egyben SLD rezolúciós levezetés is.

SLD rezolúció

Következmény

Horn-klózok egy Σ halmaza akkor és csak akkor kielégíthetetlen, ha SLD rezolúcióval levezethető belőle az üres klóz.

Megjegyzés

Amennyiben Σ egy kivétellel programklózokból áll, úgy akkor és csak akkor kielégíthetetlen, ha a benne levő negatív klózból indulva SLD rezolúcióval levezethető az üres klóz.

A logikai programozás alapjai

Alapfeladat

Adott $\forall((Q_1 \wedge \ldots \wedge Q_n) \rightarrow P)$ alakú univerzális formulák Σ véges halmaza, ahol $Q_1, \ldots, Q_n, P$ atomi formulák, és adott egy $\exists(R_1 \wedge \ldots \wedge R_m)$ egzisztenciális formula, ahol $R_1, \ldots, R_m$ atomi formulák, igaz-e, hogy

$$\Sigma \models \exists(R_1 \wedge \ldots \wedge R_m)?$$

Átfogalmazás

Adott $\{P, \neg Q_1, \ldots, \neg Q_n\}$ programklózok egy véges Σ halmaza (azaz egy **logikai program**), és egy $\{\neg R_1, \ldots, \neg R_m\}$ **kérdésklóz** vagy **célklóz**, kielégíthetetlen-e a $\Sigma \cup \{\{\neg R_1, \ldots, \neg R_m\}\}$ klózhalmaz?

Példa

$$\Sigma \quad : \quad (a)\{\text{szereti}(\text{Éva}, \text{alma})\}$$
$$(b)\{\text{szereti}(\text{Éva}, \text{bor})\}$$
$$(c)\{\text{szereti}(\text{Ádám}, x), \neg\text{szereti}(x, \text{bor})\}$$

Cél: $\{\neg\text{szereti}(\text{Ádám}, y)\}$.

1. $\{\neg\text{szereti}(\text{Ádám}, y)\}$
2. $\{\neg\text{szereti}(y, \text{bor})\}$ 1., (c), $[x/y]$ helyettesítéssel
3. $\square$ 2., (b), $[y/\text{Éva}]$ helyettesítéssel

Tehát:
$\{\text{szereti}(\text{Éva}, \text{alma}), \text{szereti}(\text{Éva}, \text{bor}), \forall x(\text{szereti}(x, \text{bor}) \rightarrow \text{szereti}(\text{Ádám}, x))\} \models \exists y\ \text{szereti}(\text{Ádám}, y)$. Pl. $y = \text{Éva}$.

Prolog szintaxissal az előző példa:

$$\begin{aligned}
&\text{szereti}(\text{éva}, \text{alma}).\\
&\text{szereti}(\text{éva}, \text{bor}).\\
&\text{szereti}(\text{ádám}, X) \quad :- \quad \text{szereti}(X, \text{bor}).\\
&\qquad\qquad\qquad\qquad\quad ?- \quad \text{szereti}(\text{ádám}, Y).
\end{aligned}$$

Példa

$\Sigma : \{\{x + 0 = x\}, \{x + y' = (x + y)'\}\}$
Cél: $\{\neg(0''' + 0'' = u)\}$

Átfogalmazás

$\Sigma : (a)\ \{A(x, 0, x)\}, \quad (b)\ \{A(x, y', z'), \neg A(x, y, z)\}$
Cél: $\{\neg A(0''', 0'', u)\}$

1. $\{\neg A(0''', 0'', u)\}$
2. $\{\neg A(0''', 0', z)\} \quad (b),\ s_1 = [x/0'''][y/0'][u/z']$
3. $\{\neg A(0''', 0, w)\} \quad (b),\ s_2 = [x/0'''][y/0][z/w']$
4. $\square \quad (a),\ s_3 = [x/0'''][w/0''']$

A 3. lépésben a (b) klózra a $[z/w]$ változóátnevezést alkalmaztuk.
Tehát: $us_1s_2s_3 = 0'''''$, azaz $A(0''', 0'', 0''''')$.

Definíció

Legyen Σ logikai program, $G = \{\neg R_1, \ldots, \neg R_n\}$ kérdésklóz.
Konfiguráció: (G, s), ahol G negatív klóz, s helyettesítés.
Legyenek (G, s) és (G', s') konfigurációk. $\boldsymbol{(G, s) \vdash (G', s')}$ akkor és csak akkor, ha van olyan programklóz, melynek G' a G-vel alkotott rezolvense, melynek képzésében az r legáltalánosabb egyesítőt használtuk, továbbá $s' = sr$.
Kiszámítás: Minden $(G, []) \vdash (G_1, s_1) \vdash \ldots \vdash (G_m, s_m)$ véges sorozat, ahol G a kérdésklóz.
Egy kiszámítás **sikeres**, ha utolsó tagja $(\square, s)$ alakú.
Sikeres kiszámítás **eredménye**: $(R_1 \wedge \ldots \wedge R_n)s$, ahol $(\square, s)$ az utolsó tag.

Tétel

A Σ-beli klózok univerzális lezártjai halmazának akkor és csak akkor logikai következménye $\exists(R_1 \wedge \ldots \wedge R_n)$, ha létezik sikeres kiszámítás.
Sikeres kiszámítás eredményének minden alap példánya a Σ-beli klózok univerzális lezártjai halmazának logikai következménye.
Ha valamely s' helyettesítésre $(R_1 \wedge \ldots \wedge R_n)s'$ minden alap példánya a Σ-beli klózok univerzális lezártjaiból álló halmaz logikai következménye, akkor létezik olyan sikeres kiszámítás, melynek $(R_1 \wedge \ldots \wedge R_n)s$ eredményére

$$(R_1 \wedge \ldots \wedge R_n)s' = (R_1 \wedge \ldots \wedge R_n)ss''$$

valamely s'' mellett.

Heterogén elsőrendű logika

Heterogén elsőrendű logika

Legyen S **típusok** (megszámlálható) halmaza, és minden $s \in S$ típusra $x_1^s, \ldots, x_n^s, \ldots$ $\boldsymbol{s}$ **típusú változók** végtelen sorozata. (Amennyiben a típus impliciten adott, gyakran csak x_i-t írunk x_i^s helyett.)

Minden $(s_1 \ldots s_n, s) \in S^* \times S$ rendezett párra legyen adott az $\boldsymbol{(s_1 \ldots s_n, s)}$ **típusú függvényszimbólumok** vagy **műveleti szimbólumok** megszámlálható halmaza.

Minden $s_1 \ldots s_n \in S^*$-ra legyen adott az $\boldsymbol{s_1 \ldots s_n}$ **típusú relációszimbólumok** vagy **predikátumszimbólumok** megszámlálható halmaza.

Definíció

Minden $s \in S$-re az $\boldsymbol{s}$ **típusú termek** a következők:

- Minden s típusú változó.
- Minden $f(t_1, \ldots, t_n)$ alakú kifejezés, ahol f valamely $s_1, \ldots, s_n \in S$ típusokra $(s_1 \ldots s_n, s)$ típusú műveleti szimbólum és t_i s_i típusú term, $i = 1, \ldots, n$.

Definíció

Az **atomi formulák** az

$$r(t_1, \ldots, t_n)$$

alakú kifejezések, ahol r egy $s_1 \ldots s_n$ típusú relációszimbólum, t_i pedig s_i típusú term, $i = 1, \ldots, n$.

Definíció

Formulák azok a kifejezések, melyek előállnak az atomi formulákból a $\wedge, \vee, \rightarrow, \leftrightarrow$ és $\neg$ logikai összetevők és az egzisztenciális és univerzális kvantifikáció használatával.

S típusú struktúrán egy $\mathcal{A} = (A, I, \varphi)$ rendszert értünk, ahol $A = (A_s)_{s \in S}$ nemüres halmazok rendszere, az I **interpretációs függvény** minden f $(s_1 \dots s_n, s)$ típusú függvényszimbólumhoz egy

$$I(f) : A_{s_1} \times \ldots \times A_{s_n} \to A_s$$

függvényt, és minden $s_1 \dots s_n$ típusú predikátumszimbólumhoz egy

$$I(r) : A_{s_1} \times \ldots \times A_{s_n} \to \{0, 1\}$$

predikátumot (vagy $I(r) \subseteq A_{s_1} \times \ldots \times A_{s_n}$ relációt) rendel.

A **homogén** esethez hasonlóan definiáljuk azt, hogy mikor elégít ki egy $\mathcal{A}$ struktúra egy F formulát, azaz mikor teljesül az $\mathcal{A} \models F$ reláció.

Példa

$S = \{i, b\}$.

Függvényszimbólumok:

- (λ, i) típusú: $\underline{0}, \underline{1}$
- (λ, b) típusú: $\mathrm{true}, \mathrm{false}$
- (ii, i) típusú: $+, \times, \ldots$
- (bb, b) típusú: $\underline{\wedge}, \underline{\vee}, \ldots$
- (b, b) típusú: $\underline{\neg}$
- (ii, b) típusú: $\underline{\leq}, \underline{\geq}, \ldots$
- (bii, i) típusú: ite (az „if then else” rövidítése)

Példa folytatása

Predikátumszimbólumok:

- ii típusú: $<, >, \ldots$
- bb típusú: $=$

Termek:

- $t_1 :\ \mathrm{ite}((x + \underline{1}) \underline{\leq} y \ \underline{\vee}\ x \underline{\geq} z, x, y + \underline{2})$, ahol $\underline{2} = \underline{1} + \underline{1}$.
- $t_2 :\ \mathrm{ite}(x \underline{\geq} y, y, x) + \underline{1}$.

Formulák:

- $F_1 :\ t_1 < t_2 \vee t_2 < t_1$
- $F_2 :\ \exists x t_1 < t_2$

Példa folytatása

Struktúra: $\mathcal{D} = (D, I, \varphi)$

- $D_i = \mathbb{N}$, $D_b = \{0, 1\}$
- I: a szokásos függvények, relációk,

$$\mathrm{ite}(b, x, y) = \begin{cases} x & \text{ha } b = 1 \\ y & \text{ha } b = 0 \end{cases}$$

- $\varphi : x \mapsto 1, y \mapsto 2, z \mapsto 3, \ldots$

$\mathcal{D}(t_1) = 4$, $\mathcal{D}(t_2) = 2$.
$\mathcal{D}(F_1) = 1$.

Heterogén elsőrendű logika

A homogén esetre bizonyított eredmények érvényben maradnak a heterogén elsőrendű logikára is.

Másodrendű logika

Az elsőrendű logika bővitése **relációváltozókkal** (**predikátumváltozókkal**).

Formulák

Az elsőrendű logika formulaképzési szabályai plusz:

- Ha R n rangú predikátumváltozó és $t_1, \ldots, t_n$ termek, akkor $R(t_1, \ldots, t_n)$ is atomi formula.
- Ha R n rangú predikátumváltozó és F formula, akkor $\exists R\ F$ és $\forall R\ F$ is formulák.

Struktúra

$\mathcal{A} = (A, I, \varphi)$, ahol A, I mint az elsőrendű esetben, a φ értékelés pedig minden x elsőrendű változóhoz az A egy elemét, minden R n rangú predikátumváltozóhoz pedig egy $A^n \to \{0, 1\}$ predikátumot rendel.

Legyen $\mathcal{A} = (A, I, \varphi)$ struktúra, F formula. Az $\mathcal{A} \models F$ relációt az elsőrendű esethez hasonlóan definiáljuk az alábbiak figyelembe vételével:

- $\mathcal{A} \models R(t_1, \ldots, t_n)$ akkor és csakis akkor, ha $\varphi(R)(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_n)) = 1$.
- $\mathcal{A} \models \exists R\ F$ akkor és csak akkor, ha létezik olyan φ', mely legfeljebb az R-en tér el φ-től, amelyre $(A, I, \varphi') \models F$.
- $\mathcal{A} \models \forall R\ F$ akkor és csak akkor, ha bármely olyan φ' esetén, mely legfeljebb az R-en tér el φ-től, $(A, I, \varphi') \models F$.

Az, hogy $\mathcal{A} \models F$ fennáll-e, ismét független azon változók értékétől, melyek nem fordulnak elő szabadon F-ben.

Példa

A természetes számok szokásos struktúrája kielégíti a

$$\forall X((X(\underline{0}) \wedge \forall x(X(x) \to X(x'))) \to \forall x X(x))$$

indukciós axiómát.

A fenti formula **monadikus**, mert X 1-rangú relációváltozó. (Monadikus másodrendű logika)

A másodrendű logika sok tekintetben az elsőrendű logikától eltérően viselkedik. Pl. nem igaz a kompaktsági tétel.

Legyen A véges nemüres halmaz (abc). A^+ jelöli az A feletti véges, nemüres szavak halmazát.

Tekintsük azt az egyenlőséges másodrendű nyelvet, mely tartalmazza a suc kétváltozós, és a P_a, $a \in A$ egyváltozós relációszimbólumokat.

Minden $u \in A^+$ n-hosszú szó felfogható olyan struktúrának, mely tartóhalmaza az $\{1, \ldots, n\}$ halmaz, melyben $\mathrm{suc}(i, j)$ akkor és csak akkor, ha $j = i + 1$, és $P_a(i)$ akkor és csak akkor, ha u i-dik betűje a.

Példa

$u = aab$ mint struktúra:

tartóhalmaz: $\{1, 2, 3\}$

$\mathsf{suc}(1, 2)$, $\mathsf{suc}(2, 3)$

$P_a(1), P_a(2), P_b(3)$

Példa

$\mathsf{First}(x) : \quad \neg(\exists y\ \mathsf{suc}(y, x))$

$\mathsf{Last}(x) : \quad \neg(\exists y\ \mathsf{suc}(x, y))$

$F : \quad \forall x((\mathsf{First}(x) \to P_a(x) \wedge (\mathsf{Last}(x) \to P_b(x))$

$G : \quad F \wedge \forall x \forall y(\mathsf{suc}(x, y) \to (P_a(x) \leftrightarrow P_b(y))$

$H : \quad \exists X((\mathsf{First}(x) \to X(x)) \wedge (\mathsf{Last}(x) \to$
$\neg X(x)) \wedge \forall x \forall y(\mathsf{suc}(x, y) \to (X(x) \leftrightarrow \neg X(y))))$

Tétel

Egy $L \subseteq A^+$ nyelv akkor és csak akkor reguláris, ha a **monadikus másodrendű logika** valamely mondatának összes moddelljéből áll.

Példa

$F: \quad a(a+b)^*b$
$G: \quad (ab)^+$
$H: ((a+b)(a+b))^+$

Tétel

Egy $L \subseteq A^+$ nyelv akkor és csak akkor van NP-ben, ha az **egzisztenciális másodrendű logika** valamely mondatának összes moddelljéből áll.

Hardware és software rendszerek verifikációja

Verifikáció

Verifikáció előtérbe kerülése:

- Biztonsági szempontból kritikus rendszerek
- Kereskedelmi szempontból kritikus rendszerek

A formális verifikáció fő részei

- A rendszer leírása (modell leíró nyelv)
- Az elvárt tulajdonságok leírása (specifikációs nyelv)
- Verifikációs módszer (az adott modell kielégíti-e az adott specifikációt)

A formális verifikáció fajtái

- Bizonyítás alapú vagy modell alapú
- Automatizált, manuális vagy ezek kombinációja
- A tulajdonságok teljes vagy részleges verifikációja
- Elsődleges vagy utólagos

Alkalmazási terület

- Hardware és software rendszerek
- Szekvenciális és konkurrens rendszerek
- Reaktív és termináló rendszerek

Verifikáció

Két verifikációs módszerrel ismerkedünk meg:

- Modell ellenőrzés: modell alapú, automatikus, konkurrens és reaktív rendszerek.
- Hoare kalkulus: bizonyítás alapú, félig automatikus, szekvenciális programok verifikációjára alkalmas. (Létezik konkurrens kiterjesztés is.)

A Hoare kalkulushoz hasonló, de nem axiomatikus módszert vezetett be Floyd.

Modell ellenőrzés

Legyen adott az alaptulajdonságok egy A halmaza, melyet rögzítettnek tekintünk.

Kripke modellnek, vagy **modellnek** nevezünk egy

$$M = (S, \rightarrow, L)$$

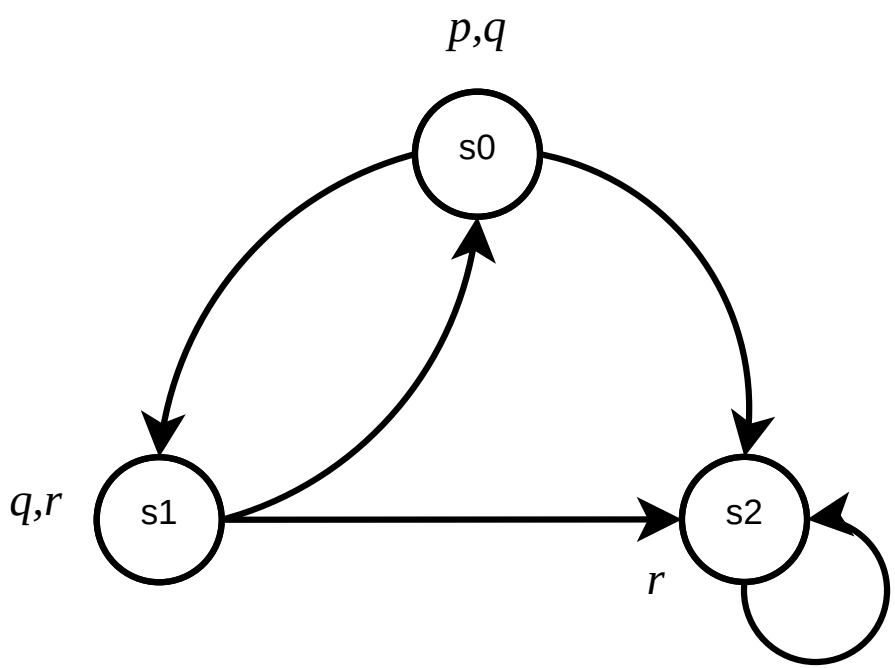
rendszert, ahol

- S az állapotok nemüres halmaza (általában véges),
- $\rightarrow \subseteq S \times S$ az átmeneti reláció,
- $L : S \rightarrow P(A) = \{B : B \subseteq A\}$ a címkefüggvény.

Kikötjük, hogy $\forall s \exists s' \; s \rightarrow s'$.
Elegendő lenne famodellekre szorítkozni.

Példa

- $A = \{p, q, r\}$
- $S = \{s_0, s_1, s_2\}$
- $\rightarrow = \{(s_0, s_1), (s_0, s_2), (s_1, s_0), (s_1, s_2), (s_2, s_2)\}$
- $L(s_0) = \{p, q\}$, $L(s_1) = \{q, r\}$, $L(s_2) = \{r\}$



Specifikációs nyelvek

1. **L**inear **T**emporal **L**ogic vagy **L**ineáris **T**emporális **L**ogika (LTL)
2. **C**omputation **T**ree **L**ogic (CTL)
3. μ-kalkulus

stb.

Mi csak a CTL-lel foglalkozunk.

Formulák

A CTL (állapot)formulái:

- $\uparrow$, $\downarrow$
- p, $p \in A$
- $\neg F$, $F \wedge G$, $F \vee G$, $\ldots$
- $\mathrm{AX}\ F$, $\mathrm{EX}\ F$
- $\mathrm{AF}\ F$, $\mathrm{EF}\ F$
- $\mathrm{AG}\ F$, $\mathrm{EG}\ F$
- $\mathrm{A}(F\ \mathrm{U}\ G)$, $\mathrm{E}(F\ \mathrm{U}\ G)$

Informális jelentés

- $\mathrm{AX}\ F$: Minden rákövetkező állapotban érvényes F.
- $\mathrm{EX}\ F$: Létezik olyan rákövetkező állapot, melyben érvényes F.
- $\mathrm{AF}\ F$: Minden, az állapotból induló végtelen út tartalmaz olyan állapotot, melyben érvényes F.
- $\mathrm{EF}\ F$: Létezik olyan, az állapotból induló végtelen út, mely tartalmaz olyan állapotot, melyben érvényes F.
- $\mathrm{AG}\ F$: Minden, az állapotból induló végtelen út minden állapotában érvényes F.
- $\mathrm{EG}\ F$: Létezik olyan, az állapotból induló végtelen út, melynek minden állapotában érvényes F.

Informális jelentés folytatása

- $\mathrm{A}(F\ \mathrm{U}\ G)$: Minden, az állapotból kiinduló végtelen úton van olyan állapot, ahol érvényes G, és az úton ezt megelőző állapotok mindegyikében érvényes F.
- $\mathrm{E}(F\ \mathrm{U}\ G)$: Létezik olyan, az állapotból induló végtelen út, melyen van olyan állapot, ahol érvényes G, és az úton ezt megelőző állapotok mindegyikében érvényes F.

Példa

A korábbi modell s_0 állapotában érvényesek: p, $\mathrm{AX}\ r$, $\mathrm{EX}\ q$, $\mathrm{EG}\ q$, $\mathrm{AXEG}\ r$, $\mathrm{A}(q\ \mathrm{U}\ r)$.

Példa

- EF(started $\wedge$ $\neg$ready)
- AG(requested $\rightarrow$ acknowledged)
- AGEF enabled
- EFAG deadlock

A szemantika formális definíciója

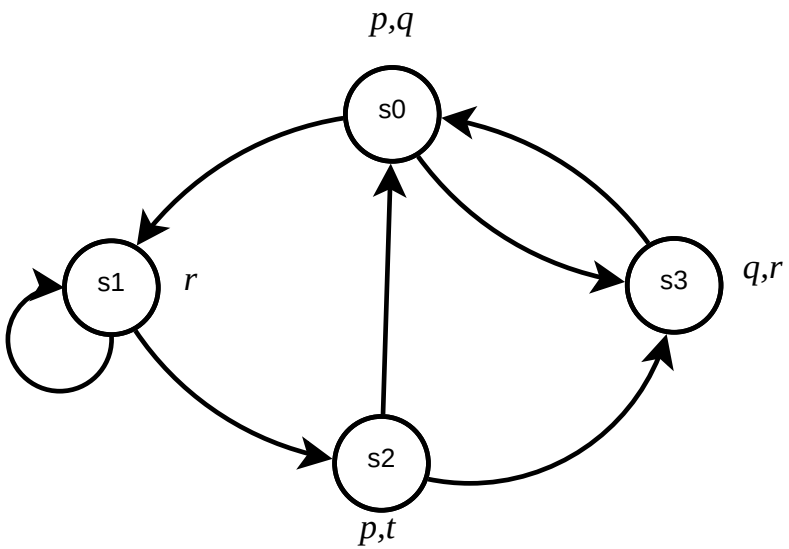
Tetszőleges M modellre, s állapotra és F formulára definiáljuk, hogy mikor érvényes (vagy teljesül) az F formula az M adott s állapotában. Jelölés: $\boldsymbol{M, s \models F}$.

$$
\begin{array}{lcll}
M, s & \models \uparrow & \text{és} & M, s \not\models \downarrow \\
M, s & \models p & \Leftrightarrow & p \in L(s) \\
M, s & \models \neg F & \Leftrightarrow & M, s \not\models F \\
M, s & \models F \wedge G & \Leftrightarrow & M, s \models F \text{ és } M, s \models G \\
M, s & \models F \vee G & \Leftrightarrow & M, s \models F \text{ vagy } M, s \models G \\
M, s & \models \mathrm{AX}\ F & \Leftrightarrow & \forall s \to s'\ M, s' \models F \\
M, s & \models \mathrm{EX}\ F & \Leftrightarrow & \exists s \to s'\ M, s' \models F
\end{array}
$$

A szemantika formális definíciója, folytatás

$$
\begin{aligned}
M, s &\models \mathrm{AG}\ F \quad \Leftrightarrow \quad \forall s = s_0 \to s_1 \to \ldots\ \forall i\ M, s_i \models F \\
M, s &\models \mathrm{EG}\ F \quad \Leftrightarrow \quad \exists s = s_0 \to s_1 \to \ldots\ \forall i\ M, s_i \models F \\
M, s &\models \mathrm{AF}\ F \quad \Leftrightarrow \quad \forall s = s_0 \to s_1 \to \ldots\ \exists i\ M, s_i \models F \\
M, s &\models \mathrm{EF}\ F \quad \Leftrightarrow \quad \exists s = s_0 \to s_1 \to \ldots\ \exists i\ M, s_i \models F \\
M, s &\models \mathrm{A}(F\ \mathrm{U}\ G) \quad \Leftrightarrow \quad \forall s = s_0 \to s_1 \to \ldots \exists i \\
&\qquad M, s_i \models G \text{ és } \forall j < i\ M, s_j \models F \\
M, s &\models \mathrm{E}(F\ \mathrm{U}\ G) \quad \Leftrightarrow \quad \exists s = s_0 \to s_1 \to \ldots \exists i \\
&\qquad M, s_i \models G \text{ és } \forall j < i\ M, s_j \models F
\end{aligned}
$$

Példa



s_0 kielégíti: AF q, AF r, EXEX r, AGEF$(p \vee r)$.
s_0 nem elégíti ki: AXEX r, AGAF q.

Definíció

Ekvivalensnek nevezzük az F és G formulákat, ha tetszőleges M modellre és s állapotra

$$M, s \models F \quad \Leftrightarrow \quad M, s \models G.$$

Jelölés: $F \equiv G$.

Néhány ekvivalencia

- $\neg\mathrm{AF}\ F \equiv \mathrm{EG}\neg F$ és $\neg\mathrm{EG}\ F \equiv \mathrm{AF}\neg F$
- $\neg\mathrm{EF}\ F \equiv \mathrm{AG}\neg F$ és $\neg\mathrm{AG}\ F \equiv \mathrm{EF}\neg F$
- $\neg\mathrm{AX}\ F \equiv \mathrm{EX}\neg F$ és $\neg\mathrm{EX}\ F \equiv \mathrm{AX}\neg F$
- $\mathrm{AF}\ F \equiv \mathrm{A}(\uparrow\ \mathrm{U}\ F)$ és $\mathrm{EF}\ F \equiv \mathrm{E}(\uparrow\ \mathrm{U}\ F)$
- $\mathrm{A}(F\ \mathrm{U}\ G) \equiv \neg\big(\mathrm{EG}\neg G \vee \mathrm{E}(\neg G\ \mathrm{U}(\neg F \wedge \neg G))\big)$
  $\mathrm{A}(F\ \mathrm{U}\ G)$ akkor és csak akkor nem teljesül, ha van olyan végtelen út, amelyen végig nem teljesül G, vagy az első olyan helyre, ahol G teljesül, $\neg F$ teljesül egy megelőző helyen.

Az utolsó ekvivalencia bizonyítása

Tegyük fel, hogy $(M, s) \models \mathrm{A}(F\ \mathrm{U}\ G)$.
Minden s-ből induló végtelen úton kielégül valahol G, azaz $M, s \not\models \mathrm{EG}\neg G$.
Belátjuk még, hogy $M, s \not\models \mathrm{E}\big(\neg G\ \mathrm{U}\ (\neg F \wedge \neg G)\big)$.
Ellenkező esetben létezik olyan s-ből induló végtelen út, melyre:

- $\neg F \wedge \neg G$ kielégül valahol
- az első olyan állapotra, ahol $\neg F \wedge \neg G$ kielégül, fennáll, hogy előtte $\neg G$ mindig teljesül:
$$\neg G, \neg G, \ldots, \neg G, \neg F \wedge \neg G, \ldots$$
- De akkor:
$$F \wedge \neg G, F \wedge \neg G, \ldots, F \wedge \neg G, \neg F \wedge \neg G, \ldots$$
ellentmondásban azzal, hogy $M, s \models \mathrm{A}(F\ \mathrm{U}\ G)$.

A fordított irány hasonló.

Következmény

Az AG, EX, EU modalitások **adekvát** halmazt alkotnak.
Hasonlóan AG, AX, AU és AF, EX, EU is adekvátak.

Modell ellenőrzési algoritmus

- **Bemenet**: $M = (S, \to, L)$ véges modell, F formula.
- **Kimenet**: Azon $s \in S$ állapotok S_F halmaza, melyekre $M, s \models F$.
- **Módszer**:
  Először lineáris időben olyan alakra hozzuk F-et, hogy benne legfeljebb az AF, EX, EU modalitások és a $\wedge$, $\neg$, $\downarrow$ és $p \in A$ jelek forduljanak elő.
  Majd F minden egyes G részformulájára meghatározzuk az S_G halmazt.

Modell ellenőrzés

Módszer

- $G = \downarrow$: $S_G = \emptyset$.
- $G = p$: $S_G = \{s \in S : \ p \in L(s)\}$.
- $G = \neg H$: $S_G = S - S_H$.
- $G = H_1 \wedge H_2$: $S_G = S_{H_1} \cap S_{H_2}$.

Módszer

- $G = \mathrm{AF}\ H$: S_G a legszűkebb olyan halmaz, mely tartalmazza S_H-t, és amelyre teljesül, hogy ha s olyan állapot, melynek minden rákövetkezője S_G-ben van, akkor s is S_G-ben van. Tehát, ha $|S| = n$, akkor

$$\begin{aligned} S_G &= \bigcup_{i=0}^{n} S_i \\ S_0 &= S_H \\ S_{j+1} &= S_j \cup \{s : \forall s \to s'\ s' \in S_j\} \end{aligned}$$

Módszer

- $G = \mathrm{EX}\ H$: $S_G = \{s : \exists s \to s'\ s' \in S_H\}$
- $G = \mathrm{E}(H_1\ \mathrm{U}\ H_2)$: Ekkor S_G a legszűkebb olyan halmaz, mely tartalmazza S_{H_2}-t és amelyre tetszőleges $s \to s'$ esetén, ha $s \in S_{H_1}$ és $s' \in S_G$, akkor $s \in S_G$. Tehát:

$$\begin{aligned} S_G &= \bigcup_{i=0}^{n} S_i \\ S_0 &= S_{H_2} \\ S_{j+1} &= S_j \cup \{s : s \in S_{H_1} \wedge \exists s \to s'\ s' \in S_j\} \end{aligned}$$

Megjegyzés

Az algoritmus lineáris a formula és négyzetes a modell méretében. Létezik olyan algoritmus is, mely a modell méretében is lineáris.

Probléma

Az **állapotrobbanás** problémája: egy 100 bináris komponensből álló rendszer modelljének állapotszáma 2^{100}.

Szimbolikus modell ellenőrzési módszerekkel mégis lehetséges ilyen nagy állapotszámú rendszerek verifikációja.

Floyd-Hoare logika

Legyen adott egy elsőrendű nyelv (azaz a függvény- és relációszimbólumok egy-egy megszámlálható halmaza).

Definíció

A **while programok** az alábbiak:

- $x := t$, ahol x változó, t term,
- $P_1; P_2$, ahol P_1, P_2 while programok,
- $\text{if } r \text{ then } P_1 \text{ else } P_2$, ahol r kvantormentes formula, P_1, P_2 programok,
- $\text{while } r \text{ do } P$, ahol r kvantormentes formula, P program.

Legyen P program, $\mathcal{A} = (A, I)$ struktúra. Ekkor P indukál az értékelések felett egy $[[P]]$ relációt: tetszőleges φ és ψ értékelésekre a $\varphi[[P]]\psi$ akkor és csakis akkor, ha a P programot a φ által adott kezdeti értékeken futtatva P végrehajtása befejeződik, és a változók végértékét ψ adja.

Megjegyzés

Bármely φ-hez legfeljebb egy olyan ψ létezik, melyre $\varphi[[P]]\psi$.

A szemantika formális definíciója

Legyen P program, $\mathcal{A}$ elsőrendű struktúra. Tetszőleges φ változóértékelésre legyen $\mathcal{A}_\varphi = (A, I, \varphi)$. Ekkor tetszőleges φ, ψ értékelésekre $\varphi[[P]]\psi$ akkor és csak akkor, ha az alábbi esetek valamelyike teljesül:

- $P = x := t$ és $\psi = \varphi[x \mapsto \mathcal{A}_\varphi(t)]$.
- $P = P_1; P_2$ és $\exists \tau\ \varphi[[P_1]]\tau$ és $\tau[[P_2]]\psi$.
- $P = \text{if } r \text{ then } P_1 \text{ else } P_2$ és

$$\begin{array}{llll} \varphi[[P_1]]\psi & \text{és} & \mathcal{A}_\varphi(r) = 1 & \text{, vagy} \\ \varphi[[P_2]]\psi & \text{és} & \mathcal{A}_\varphi(r) = 0. & \end{array}$$

A szemantika formális definíciója, folytatás

- $P = \text{while } r \text{ do } P_1$ és $\exists \varrho_0, \ldots, \varrho_n$, $n \geq 0$, $\varrho_0 = \varphi$, $\varrho_n = \psi$, $\varrho_i [[P_1]] \varrho_{i+1}$, $\mathcal{A}_{\varrho_i}(r) = 1$, $i = 0, \ldots, n-1$, $\mathcal{A}_{\varrho_n}(r) = 0$.

Definíció

Parciális helyességi kifejezések az

$$\{F\}P\{G\}$$

alakú hármasok, ahol P program, F és G elsőrendű formulák.

Definíció

Azt mondjuk, hogy az $\{F\}P\{G\}$ parciális helyességi kifejezés **teljesül** (vagy **érvényes**) az $\mathcal{A} = (A, I)$ struktúrában, vagy $\mathcal{A}$ **kielégíti** az $\{F\}P\{G\}$ parciális helyességi kifejezést, jelben $\boldsymbol{\mathcal{A} \models \{F\}P\{G\}}$, ha valahányszor φ, ψ olyan értékelések, hogy

$$(A, I, \varphi) \models F \text{ és } \varphi[[P]]\psi,$$

fennáll, hogy

$$(A, I, \psi) \models G.$$

Példa

$$P = y := 1; \text{while } x > 0 \text{ do } (y := y \times x;\ x := x - 1)$$

Ekkor a standard struktúrában:

$$\begin{aligned} \varphi[[P]]\psi \quad \Leftrightarrow \quad & \big((\varphi(x) < 0,\ \psi(x) = \varphi(x), \psi(y) = 1) \\ & \vee(\varphi(x) \geq 0,\ \psi(x) = 0,\ \psi(y) = x!)\big) \\ & \wedge(\varphi(z) = \psi(z),\ z \notin \{x, y\}) \end{aligned}$$

Az előző P programra és az egész számok standard $\mathcal{A}$ struktúrájára:

$$\begin{aligned} \mathcal{A} \quad &\models \quad \{x = z \wedge x \geq 0\}P\{y = z! \wedge x = 0\} \\ \mathcal{A} \quad &\models \quad \{x = z\}P\{y = z! \vee y = 1\} \end{aligned}$$

Példa

Az egész számok szokásos struktúrájában érvényes:

$$\{a \geq 0\}$$
$$x := 0;$$
$$y := 1;$$
$$\text{while } y \leq a \text{ do}$$
$$\quad x := x + 1;\ y := y + 2x + 1$$
$$\{0 \leq x^2 \leq a < (x+1)^2\}$$

Példa

$$P' = \text{while } x \neq 100 \text{ do } x := x + 2$$

Ekkor a standard struktúrában érvényesek:

$$\{x = z\}P'\{x = 100\}, \quad \{\uparrow\}P'\{x = 100\}$$

Definíció

Totális helyességi kifejezésnek nevezünk egy

$$[F]P[G]$$

hármast, ahol P program, F, G formulák.
Azt mondjuk, hogy az $\mathcal{A} = (A, I)$ struktúra **kielégíti** az $[F]P[G]$ totális helyességi kifejezést, ha tetszőleges olyan φ értékelésre, melyre $\mathcal{A}_\varphi \models F$, létezik olyan (egyértelműen meghatározott) ψ értékelés, hogy $\varphi[[P]]\psi$ és $\mathcal{A}_\psi \models G$. Jelölés: $\boldsymbol{\mathcal{A} \models [F]P[G]}$.

Példa

Az előző P, P' programokra és az $\mathcal{A}$ standard struktúrára:

$$\begin{aligned} \mathcal{A} &\models [x = z \wedge x \geq 0]P[y = z!] \\ \mathcal{A} &\not\models [\uparrow]P'[x = 100] \\ \mathcal{A} &\models [x \leq 100 \wedge (\exists u\ x = 2u)]P'[x = 100] \end{aligned}$$

Megjegyzés

$\mathcal{A} \models [F]P[\uparrow]$ akkor és csakis akkor teljesül, ha P **megáll** minden olyan φ esetén, amelyre $\mathcal{A}_\varphi \models F$. Jelölés: $[\boldsymbol{F}]\boldsymbol{P}\searrow$.
Tehát $\mathcal{A} \models [F]P[G]$ akkor és csak akkor, ha $\mathcal{A} \models \{F\}P\{G\}$ és $\mathcal{A} \models [F]P\searrow$.

A Hoare-féle szabályok

- **Értékadás**

$$\frac{}{\{F[x/t]\}x := t\{F\}}$$

- **Kompozíció**

$$\frac{\{F\}P_1\{H\} \quad \{H\}P_2\{G\}}{\{F\}P_1; P_2\{G\}}$$

- **Feltételes utasítás**

$$\frac{\{F \wedge r\}P_1\{G\} \quad \{F \wedge \neg r\}P_2\{G\}}{\{F\}\text{if } r \text{ then } P_1 \text{ else } P_2\{G\}}$$

A Hoare-féle szabályok, folytatás

- **Ciklus**

$$\frac{\{F \wedge r\}P\{F\}}{\{F\}\text{while } r \text{ do } P\{F \wedge \neg r\}}$$

- **Monotonitás** Tegyük fel, hogy $\forall(F \to F')$ és $\forall(G' \to G)$ az $\mathcal{A}$ elsőrendű elméletében vannak. Akkor:

$$\frac{\{F'\}P\{G'\}}{\{F\}P\{G\}}$$

Definíció

Legyen $\mathcal{A}$ elsőrendű struktúra. Azt mondjuk, hogy az $\{F\}P\{G\}$ parciális helyességi kifejezés **levezethető** (vagy **bizonyítható**) $\mathrm{Th}(\mathcal{A})$-ból,

$$\mathrm{Th}(\mathcal{A}) \vdash \{F\}P\{G\},$$

ha létezik a parciális helyességi kifejezések olyan

$$E_0, E_1, \ldots, E_n$$

sorozata, hogy $E_n = \{F\}P\{G\}$ és minden $i > 0$-ra E_i a fenti szabályok valamelyikével áll elő az $E_0, E_1, \ldots, E_{i-1}$ kifejezésekből és a $\mathrm{Th}(\mathcal{A})$ formulahalmazból.

Tétel

Ha $\mathrm{Th}(\mathcal{A}) \vdash \{F\}P\{G\}$, akkor $\mathcal{A} \models \{F\}P\{G\}$.

A tétel megfordítása általában nem igaz, de érvényes az ún. **expresszív** struktúrákra, azaz azon $\mathcal{A} = (A, I)$ struktúrákra, amelyekre igaz a következő: Tetszőleges P programhoz és G formulához létezik olyan F formula, hogy bármely φ értékelésre $\mathcal{A}_\varphi \models F$ akkor és csak akkor, ha $[[P]]$ nem értelmezett φ-n, vagy ha értelmezett, akkor arra a ψ-re, melyre $\varphi[[P]]\psi$, teljesül, hogy $\mathcal{A}_\psi \models G$.
Pl. az egész számok (vagy a természetes számok) standard struktúrája expresszív.

Tétel (Cook)

Ha $\mathcal{A}$ expresszív, akkor $\mathcal{A} \models \{F\}P\{G\}$ esetén $\mathrm{Th}(\mathcal{A}) \vdash \{F\}P\{G\}$.

A totális helyesség szabályai

A ciklus szabály kivételével hasonlóak a parciális helyesség szabályaihoz.

Az új ciklus szabály: tegyük fel, hogy az $\mathcal{A} = (A, I)$ struktúrában $I(<)$ egy **jól megalapozott** részbenrendezés. Ekkor:

$$\frac{[F \wedge r \wedge t = z_0]P[F \wedge t < z_0]}{[F]\text{while } r \text{ do } P[F \wedge \neg r]},$$

ahol z_0 máshol nem fordul elő.