Logikai programok

Logikai program

Programklóz: $p_1 \wedge p_2 \wedge \ldots p_n \;\rightarrow\; q$ alakú formula, $p_1, \ldots, p_n, q$ atomi formulák

Ítéletkalkulusban: $p_1, \ldots, p_n, q$ (ítélet)változók

Program: programklózok egy (akár végtelen) $\mathcal{P}$ halmaza

$p_1 \wedge \ldots \wedge p_n$: a klóz törzse (lehet üres is!)

q: a klóz feje

Példa

$$\begin{aligned} &\rightarrow \mathrm{even}(0)\\ \mathrm{even}(x) &\rightarrow \mathrm{odd}(\mathrm{s}(x))\\ \mathrm{odd}(x) &\rightarrow \mathrm{even}(\mathrm{s}(x)) \end{aligned}$$

Szintaxis, szemantika

Recap: elsőrendű logika szintaxis

Az előző dián even, odd (egyváltozós) predikátumjelek, 0 konstansjel, s (egyváltozós) függvényjel, x (objektum)változó.
Úgy képzeljük, mintha a klózokban a változók univerzálisan lennének kvantálva.

Modell

A program modellje egy struktúra, ami minden programklózt kielégít.

- Alaphalmaz: $\mathbb{N}$, s: $n \mapsto n + 1$, odd(n): ha n páratlan, even(n): ha n páros
- Alaphalmaz: $\mathbb{N}$, s: $n \mapsto 2n$, odd(n) és even(n) mindig igaz

Szemantika

A sok modell közül melyiket válasszuk? (ez a program „jelentése")

Herbrand-kiterjesztés

Alaptermek

A konstansokból és függvényjelekből felépíthető kifejezések
A példában: $\{0, s(0), s(s(0)), s(s(s(0))), \ldots\}$

A program Herbrand-kiterjesztése

Ahányféleképp lehet, a programklózok változóinak helyébe alaptermeket írunk

A példában

$$
\begin{aligned}
&\rightarrow \mathrm{even}(0) \\
\mathrm{even}(0) &\rightarrow \mathrm{odd}(s(0)) \\
\mathrm{odd}(0) &\rightarrow \mathrm{even}(s(0)) \\
\mathrm{even}(s(0)) &\rightarrow \mathrm{odd}(s(s(0))) \\
\mathrm{odd}(s(0)) &\rightarrow \mathrm{even}(s(s(0))) \\
\mathrm{even}(s(s(0))) &\rightarrow \mathrm{odd}(s(s(s(0)))) \quad \text{stb}
\end{aligned}
$$

Herbrand-tétel

Herbrand-tétel recap

Az eredeti program pontosan akkor kielégíthető, ha
Herbrand-kiterjesztésének van Herbrand-modellje
és a modellek közt oda-vissza tudunk transzformálni

Herbrand-modell

Minden atomi alapformula kap egy igazságértéket, egymástól függetlenül

A példában

even(0), odd(0), even(s(0)), odd(s(0)), even(s(s(0))), ...

Rövidebben

$p_0, p_1, p_2, \ldots$: $\mathrm{even}(\mathrm{s}^n(0))$ $q_0, q_1, q_2, \ldots$: $\mathrm{odd}(\mathrm{s}^n(0))$

Ítéletkalkulus

A példában

$$\rightarrow p_0$$
$$p_0 \rightarrow q_1$$
$$q_0 \rightarrow p_1$$
$$p_1 \rightarrow q_2$$
$$q_1 \rightarrow p_2$$
$$p_2 \rightarrow q_3$$
$$\ldots$$

(végtelen sok változó, végtelen sok programklóz)

Horn-algoritmus

Ciklusban:

- kiértékeljük a törzseket
- a következő menetben azokat állítjuk igazra, akiknek ebben a menetben van igaz törzse

A példában

1. Üres törzs igaz: $p_0 = 1$
2. Üres törzs igaz: $p_0 = 1$, $p_0 \rightarrow q_1$ törzse igaz: $q_1 = 1$
3. $\ldots q_1 \rightarrow p_2$ törzse is igaz: $p_2 = 1$
4. $\ldots$

„Végén": p_n igaz, ha n páros, q_n igaz, ha n páratlan

A Horn-algoritmusról

Csak azt állítja igazra, amit ,,feltétlenül muszáj''
Ez (tapasztalat szerint) általában is ,,jó'' modellt ad

Az alapszabály

Egy ,,jó'' szemantika minimalizálja az igazságértéket.

Lássuk a matekot.

Posetek

Poset

Egy P alaphalmazon a $\leq$ reláció részbenrendezés (partial order), ha

- reflexív: $x \leq x$
- tranzitív: $x \leq y$, $y \leq z \Rightarrow x \leq z$
- antiszimmetrikus: $x \leq y$, $y \leq x \Rightarrow x = y$

Ekkor P egy részbenrendezett halmaz, magyarul poset. (partially ordered set)

Ha még dichotóm is: $x \leq y \ \vee \ y \leq x$, akkor lineáris rendezés.

Példák

- Az $(\mathbb{N}, \leq)$ számhalmaz a ,,szokásos" rendezéssel lineárisan rendezett.
- Ha X egy halmaz, $X_\perp := (X \uplus \{\perp\}, \perp \leq x)$ ($\perp$ mindenkinél kisebb, többi nem összehasonlítható) (általában) nem lineárisan rendezett
- Ha X egy halmaz, akkor $(P(X), \subseteq)$ az X hatványhalmaza, (általában) ez se lineárisan rendezett

Két poset: $\mathbf{2}$ és $\mathbf{2}^Z$

Az igazságértékek

$\mathbf{2}$ a $(\{0,1\}, 0 \leq 1)$ poset

A változók

esetleg végtelen halmazát Z fogja jelölni

Az értékadások

halmazát pedig $\mathbf{2}^Z$

P^I

Ha P egy poset és I egy (nem rendezett!) indexhalmaz, akkor P^I az $I \to P$ függvények posetje a pontonkénti rendezéssel:

$$f \leq g \;\leftrightarrow\; \forall i \in I : f(i) \leq g(i).$$

Értékadások posetje

Példa

Ha $Z = \{p, q, r\}$, akkor $\mathbf{2}^Z$ elemei $(0,0,0)$, $(0,0,1)$, $\ldots$, $(1,1,1)$ (p értéke, q értéke és r értéke egy ,,vektorban")
$(0,0,1) \leq (1,0,1)$
$(1,0,1)$ és $(0,1,1)$ nem összehasonlíthatóak

tehát $\mathbf{2}$ lineárisan rendezett, de $\mathbf{2}^Z$ (általában) nem az

Minimális és legkisebb elemek

Ha P egy poset és $X \subseteq P$, akkor $x \in X \ldots$

- az X-nek a legkisebb eleme, ha $\forall y \in X: \; x \leq y$ (mindenki másnál kisebb)
- az X-nek egy minimális eleme, ha $\forall y \in X: \; y \leq x \Rightarrow y = x$ (nincs nála kisebb)
- az X-nek a legnagyobb eleme, ha $\forall y \in X: \; y \leq x$ (mindenki másnál nagyobb)
- az X-nek egy maximális eleme, ha $\forall y \in X: \; x \leq y \Rightarrow y = x$ (nincs nála nagyobb)

Legkisebb/legnagyobb elemből legfeljebb egy van, minimális/maximálisból lehet több is.
Ha van legkisebb, akkor az az egyetlen minimális.

Jó szemantika

Példa

Ha a $p \vee q \vee r$ formula modelljei közül nézzük a minimális modelleket: $(0, 0, 1)$, $(0, 1, 0)$, $(1, 0, 0)$, nincs köztük „legkisebb”, se „legjobb”.

Az alapszabályunk, még egyszer

Egy „jó” szemantika a $\mathcal{P}$ programhoz egy minimális modelljét adja meg.

„egy jó szemantika minimalizálja az igazságértéket”

A Horn-algoritmus mint iterált függvény

$T_{\mathcal{P}}$

A Horn-algoritmus egy iterációját mint egy $T_{\mathcal{P}} : \mathbf{2}^Z \to \mathbf{2}^Z$ függvényt felírva:

$$T_{\mathcal{P}}(u)(q) := \bigvee_{p_1 \wedge \ldots \wedge p_n \to q \in \mathcal{P}} u(p_1) \wedge \ldots \wedge u(p_n)$$

(még ha az „éselés” világos is... végtelen vagyolás? nulla-tagú vagyolás? nulla-tagú éselés?)

Infimum, szuprémum

Ha P poset, $X \subseteq P$ és $y \in P$, akkor y az X-nek...

- egy alsó korlátja, ha $\forall x \in X: \ y \leq x$ (jele $y \leq X$)
- egy felső korlátja, ha $\forall x \in X: \ x \leq y$ (jele $X \leq y$)
- az infimuma, ha a legnagyobb alsó korlátja (jele $y = \bigwedge X$)
- a szuprémuma, ha a legkisebb felső korlátja (jele $y = \bigvee X$)

Vagyolás, éselés

Pl. $\mathbf{2}$-ben $\bigvee\{0,1\} = 0 \vee 1$, $0 \vee 0 \vee 0 = \bigvee\{0\}$ stb.
vagyolás = szuprémum, éselés = infimum

ezzel a „végtelen" éselés/vagyolás letudva

$\bigvee \emptyset$

- az $\emptyset$-nek P minden eleme felső korlátja
- akkor $\bigvee \emptyset$ ezeknek a legkisebb eleme $\Rightarrow$ P legkisebb eleme

üresklóz

Tehát pl. $\mathbf{2}$-n az üres vagyolás ezért hamis (a legkisebb elem), az üres éselés (0-tagú törzs) ezért igaz (a legnagyobb elem)

$\mathbf{2}$-ben minden halmaznak van infimuma és szuprémuma $\Rightarrow$ a $T_{\mathcal{P}}$ függvénynek minden $u \in \mathbf{2}^Z$-re van értelme

A $T_{\mathcal{P}}$ függvény és $\mathcal{P}$ modelljei

Állítás

$$u \in \mathbf{2}^Z \text{ modellje } \mathcal{P}\text{-nek} \Leftrightarrow T_{\mathcal{P}}(u) \leq u.$$

Bizonyítás

u modellje $\mathcal{P}$-nek $\Leftrightarrow$
minden $p_1 \wedge \ldots \wedge p_n \rightarrow q$ klózt u igazzá tesz $\Leftrightarrow$
minden klózra ha $u(p_1) \wedge \ldots \wedge u(p_n) = 1$, akkor $u(q) = 1$ $\Leftrightarrow$
minden q-ra ha van $p_1 \wedge \ldots \wedge p_n \rightarrow q$, amire $u(p_1) \wedge \ldots \wedge u(p_n) = 1$, akkor $u(q) = 1$ $\Leftrightarrow$
minden q-ra ha $\bigvee u(p_1) \wedge \ldots \wedge u(p_n) = 1$, akkor $u(q) = 1$ $\Leftrightarrow$
minden q-ra ha $T_{\mathcal{P}}(u)(q) = 1$, akkor $u(q) = 1$ $\Leftrightarrow$
minden q-ra $T_{\mathcal{P}}(u)(q) \leq u(q)$ $\Leftrightarrow$
$T_{\mathcal{P}}(u) \leq u$.

Prefixpontok

Ha P poset és $f : P \to P$ függvény, akkor $x \in P$ az f-nek...

- prefixpontja, ha $f(x) \leq x$;
- posztfixpontja, ha $x \leq f(x)$;
- fixpontja, ha $x = f(x)$.

Ha van legkisebb elem, az mindig posztfixpont; ha van legnagyobb, az mindig prefixpont.

Az alapszabályunk szerint

Egy „jó" szemantika a $\mathcal{P}$ programhoz a $T_{\mathcal{P}}$ függvénynek egy minimális prefixpontját adja vissza.

Első célunk

Meg fogjuk mutatni, hogy $T_{\mathcal{P}}$-nek mindig van legkisebb fixpontja.
$\Rightarrow$ csak egyetlen ,,jó'' szemantika van, az pedig pont a Horn-algoritmusé.

Ehhez

- Megmutatjuk, hogy $T_{\mathcal{P}}$,,folytonos'' függvény;
- Megmutatjuk, hogy $\mathbf{2}^Z$,,teljes háló'';
- Megmutatjuk, hogy teljes hálón folytonos függvénynek mindig van legkisebb prefixpontja.

Teljes háló

A P poset teljes háló, ha minden X részhalmazának van szuprémuma.

Példa

- $P(X)$ teljes háló, a szuprémum az unió;
- $\mathbf{2}$ teljes háló, $\bigvee \emptyset = \bigvee\{0\} = 0$, $\bigvee\{0,1\} = \bigvee\{1\} = 1$;
- $\mathbb{N}$ a szokásos rendezéssel nem teljes háló: a végtelen részhalmazoknak nincs szuprémumuk;
- $\mathbb{N}_\perp$ nem teljes háló: pl. $\{1,2\}$-nek nincs felső korlátja (így szuprémuma se)

Nekünk most az kell, hogy $\mathbf{2}^Z$ teljes háló legyen.

Állítás

Ha P teljes háló, akkor P^I is az, a szuprémumot pedig pontonként kell venni: ha $U \subseteq P^I$, akkor

$$(\bigvee U)(i) = \bigvee_{u \in U} u(i).$$

Bizonyítás

- Először is, ha P teljes háló, akkor minden U-ra és i-re a $\bigvee_{u \in U} u(i)$ kifejezés létezik.
- Legyen u^* az a függvény, amire $u^*(i) = \bigvee_{u \in U} u(i)$.
- u^* felső korlátja U-nak: ha $u \in U$, akkor minden i-re $u(i) \leq u^*(i)$, mert $u(i) \leq \bigvee_{u \in U} u(i)$. Tehát $u \leq u^*$.
- u^* a legkisebb: legyen $U \leq v$ felső korlát. Akkor minden $u \in U$-ra $u \leq v$, azaz minden i-re $u(i) \leq v(i)$, tehát $\bigvee u(i) \leq v(i)$, vagyis $u^*(i) \leq v(i)$, így $u^* \leq v$.

Folytonos és monoton függvények

Folytonos függvények

Ha P, Q posetek és $f : P \to Q$ olyan függvény, amire a következő igaz:

- minden olyan $X \subseteq P$-re,
- ami lineárisan rendezett,
- és amire létezik $\bigvee X$,
- arra $f(\bigvee X) = \bigvee f(x)$,

akkor f-et folytonos függvénynek hívjuk.

Monoton függvények

Ha P, Q posetek és $f : P \to Q$ olyan függvény, amire

$$x \leq y \;\Rightarrow\; f(x) \leq f(y),$$

akkor f-et monoton függvénynek hívjuk.

Folytonos függvény monoton is

Állítás

Ha f folytonos, akkor monoton is.

Bizonyítás

Vegyük észre, hogy

$$x \leq y \;\Leftrightarrow\; y = \bigvee\{x, y\}$$

és ilyenkor $\{x, y\}$ lineárisan rendezett halmaz. Akkor ha f folytonos:

$$\begin{aligned} x \leq y \quad &\Rightarrow \quad y = \bigvee\{x, y\} \\ &\Rightarrow \quad f(y) = \bigvee\{f(x), f(y)\} \\ &\Rightarrow \quad f(x) \leq f(y). \end{aligned}$$

Monoton függvény iterációja

Állítás

Ha $f : P \to P$ monoton függvény, akkor prefixpont képe prefixpont, posztfixponté posztfixpont.

Bizonyítás

Ha $x \leq f(x)$ (azaz x posztfixpont), és f monoton, akkor alkalmazva f-et mindkét oldalon $f(x) \leq f(f(x))$, vagyis $f(x)$ is posztfixpont.
Prefixpontra ugyanígy.

Következmény

Ha $f : P \to P$ monoton függvény és $\perp$ a P legkisebb eleme, akkor

$$\perp \leq f(\perp) \leq f(f(\perp)) \leq \ldots \leq f^n(\perp) \leq \ldots .$$

Folytonos függvény iterációja teljes hálón

Állítás

Ha P teljes háló, $f : P \to P$ pedig folytonos függvény, akkor

$$f^* := \bigvee_{n \geq 0} f^n(\bot)$$

az f legkisebb prefixpontja, sőt fixpont is.

Bizonyítás eleje

Teljes hálón ez a szuprémum létezik.
Ha x prefixpont, akkor $f^* \leq x$:

- $\bot \leq x$ (mert $\bot$ a legkisebb elem)
- ha $f^n(\bot) \leq x$, akkor $f^{n+1}(\bot) \leq f(x)$ (mert f monoton), és $f(x) \leq x$ (mert x prefixpont), ezért $f^{n+1}(\bot) \leq x$
- tehát x felső korlátja a $\{f^n(\bot) : n \geq 0\}$ halmaznak
- f^* pedig a legkisebb felső korlátja, tehát $f^* \leq x$.

Folytonos függvény iterációja teljes hálón

Állítás

Ha P teljes háló, $f : P \to P$ pedig folytonos függvény, akkor

$$f^* := \bigvee_{n \geq 0} f^n(\perp)$$

az f legkisebb prefixpontja, sőt fixpont is.

Bizonyítás vége

Az f^* pedig fixpont:

$$f(f^*) = f(\bigvee_{n \geq 0} f^n(\perp)) = \bigvee_{n \geq 0} f^{n+1}(\perp) = \perp \vee \bigvee_{n > 0} f^n(\perp) = f^*$$

Addig tehát megvagyunk, hogy $\mathbf{2}^Z$ teljes háló és hogy ha $T_{\mathcal{P}}$ folytonos, akkor tényleg van legkisebb fixpontja.

Folytonosságőrző műveletek függvényeken

Target tupling

Ha minden $i \in I$-re $f_i : P \to Q$ egy függvény, akkor az f_i-k target tuplingja az $\langle f_i \rangle_{i \in I} : P \to Q^I$ függvény, amire

$$\langle f_i \rangle_{i \in I}(x)(i) := f_i(x).$$

(tehát az f_i függvények eredményeit egy I-vel indexelt ,,vektorba'' tesszük.)

Például

A $T_{\mathcal{P}} : \mathbf{2}^Z \to \mathbf{2}^Z$ függvény a

$$T_{\mathcal{P},q}(u) := \bigvee_{p_1 \wedge \ldots \wedge p_n \to q \in \mathcal{P}} u(p_1) \wedge \ldots \wedge u(p_n)$$

függvények (ezek $\mathbf{2}^Z \to \mathbf{2}$ függvények, minden $q \in Z$-re van egy függvény) target tuplingja.

Állítás

Folytonos függvények target tuplingja is folytonos.

Bizonyítás

- Legyenek $f_i : P \to Q$ folytonos függvények és $X \subseteq P$ egy lineárisan rendezett halmaz P-ben, aminek van szuprémuma, $x^* := \bigvee X$. Jelölje f az $\langle f_i \rangle_{i \in I} : P \to Q^I$ függvényt.
- Meg kell mutatnunk, hogy $f(x^*) = \bigvee_{x \in X} f(x)$.
- Ez azt jelenti, hogy minden i-re $f(x^*)(i) = \left(\bigvee_{x \in X} f(x)\right)(i)$.
- A jobb oldalon tudjuk, hogy a szuprémumot pontonként kell venni:

$$\left(\bigvee_{x \in X} f(x)\right)(i) = \bigvee_{x \in X} f(x)(i) = \bigvee_{x \in X} f_i(x).$$

- Ami pont $f_i(\bigvee_{x \in X} x) = f_i(\bigvee X)$, mert f_i folytonos.
- Ami $f(x^*)(i)$ az f definíciója szerint.

Folytonos függvények szuprémuma is folytonos

Állítás

Ha Q teljes háló és $f_i : P \to Q$ folytonos függvények, akkor $f := \bigvee f_i$ is folytonos.

Bizonyítás

Ha Q teljes háló, akkor P^Q is az, tehát f létezik. Legyen $X \subseteq P$ lineárisan rendezett halmaz, melyre $x^* = \bigvee X$ létezik. Meg kell mutatnunk, hogy $f(x^*) = \bigvee_{x \in X} f(x)$.
Kiírjuk a definíciókat:

$$f(x^*) = \bigvee_{i \in I} f_i(x^*) = \bigvee_{i \in I} \bigvee_{x \in X} f_i(x) = \bigvee_{x \in X} \bigvee_{i \in I} f_i(x) = \bigvee_{x \in X} f(x).$$

Mivel a $T_{\mathcal{P},q}$ függvények $u \mapsto u(p_1) \wedge \ldots \wedge u(p_n)$ függvények kompozíciói, elég ez utóbbiakról belátnunk most már, hogy folytonosak.

Projekciók

Ha P poset, I halmaz, $i \in I$ index, akkor $\pi_i : P^I \to P$ az i. koordinátára való projekció:

$$\pi_i(u) := u(i).$$

Állítás

A projekciók folytonosak.

Bizonyítás

Legyen $U \subseteq P^I$ lineárisan rendezett halmaz, amire $u^* := \bigvee U$ létezik.
Be kell lássuk, hogy $\pi_i(u^*) = \bigvee_{u \in U} u(i)$.
Ez igaz, hiszen

$$\pi_i(u^*) = u^*(i) = \left(\bigvee U\right)(i) = \bigvee_{u \in U} u(i),$$

mert P^I-ben a szuprémumot koordinátánként kell vennünk.

Véges éselés

Eddig az megvan, hogy $u \mapsto u(p)$ folytonos minden $p \in Z$-re, az kell, hogy $u \mapsto u(p_1) \wedge \ldots \wedge u(p_n)$ is folytonos minden $p_1, \ldots, p_n \in Z$-re.

Állítás

Az $\wedge_n : \mathbf{2}^n \to \mathbf{2}$ függvény folytonos.

Bizonyítás

Legyen $X \subseteq \mathbf{2}^n$ lineárisan rendezett halmaz, melyre $x^* = \bigvee X$ létezik. Meg kell mutassuk, hogy $\wedge_n(x^*) = \bigvee_{x \in X} \wedge_n(x)$.
Mivel $\mathbf{2}^n$ véges, a lineárisan rendezett $X = \{x_1, \ldots, x_k\}$ kell legyen úgy, hogy $x_1 \leq x_2 \leq \ldots \leq x_k$.
Akkor $x^* = x_k$ és $\wedge_n(x_k)$ akkor 1, ha x_k-ban minden koordináta 1.
A $\bigvee_{x \in X} \wedge_n(x)$ pedig akkor 1, ha van a $\wedge_n(x)$-ek közt 1, ami pont akkor igaz, ha van olyan $x \in X$, melyben minden koordináta 1, ami pedig megint csak azt jelenti, hogy a köztük legnagyobb x_k-ban minden koordináta 1.

Kompozíció

Állítás

Folytonos $f : P \to Q$ és $g : Q \to R$ függvények $g \circ f : P \to R$ kompozíciója folytonos.

Bizonyítás

Legyen $X \subseteq P$ a P-nek egy lineárisan rendezett részhalmaza. Mivel f monoton is, ezért ha $x \leq y$, akkor $f(x) \leq f(y)$. Tehát az $f(X)$ halmaz is lineárisan rendezett Q-ban.
Mivel f folytonos, így $f(\bigvee X) = \bigvee_{x \in X} f(x)$. Tehát a jobb oldalon egy lineárisan rendezett halmaz áll Q-ban, aminek van szuprémuma, erre alkalmazva g folytonosságát kapjuk, hogy
$g(\bigvee_{x \in X} f(x)) = \bigvee_{x \in X}(g(f(x)))$, és pont ezt akartuk.

Összegezve

Állítás

A $T_{\mathcal{P}}$ függvény folytonos.

Bizonyítás

$T_{\mathcal{P}}$-t úgy kapjuk, hogy veszünk projekciókat, ezeknek a target tuplingját, az eredményen alkalmazunk véges éselést, ilyen függvényeknek vesszük a szuprémumát, és az eredményeknek a target tuplingját, minden alapfüggvény folytonos és minden művelet őrzi a folytonosságot.

Tehát azt kaptuk, hogy

A $\mathcal{P}$ logikai program egyetlen ,,jó'' szemantikája pontosan a $T_{\mathcal{P}}$ függvény legkisebb (pre)fixpontja.
Ez pontosan az az értékadás, melyet a Horn-algoritmus (esetleg végtelen) iterálásával kapunk.

(Hiszen az értékadások $\mathbf{2}^{Z}$ posetjének legkisebb eleme az épp a konstans 0 értékadás, melyből a Horn-algoritmus is kiindul, és melyre folytatjuk az $\perp \leq T_{\mathcal{P}}(\perp) \leq T_{\mathcal{P}}(T_{\mathcal{P}}(\perp)) \leq \ldots$ iterációt.)

Modellek, alátámasztott modellek

A $\mathcal{P}$ program modelljei közül (amik pont a $T_\mathcal{P}$ függvény prefixpontjai) ...

- a $T_\mathcal{P}$ függvény fixpontjait alátámasztott (supported) modelljeinek hívjuk,
- a legkisebb fixpontját pedig a kanonikus szemantikának.

Az ,,alátámasztott'' modellekben minden igaz változó ,,okkal'' igaz: ha $u(q) = 1$, akkor van is olyan klóz, melynek q a feje és u melletti törzse szintén 1.

Általános logikai programok

Lehet negálni a törzsben

Általános logikai program: $\ell_1 \wedge \ell_2 \wedge \ldots \ell_n \to p$ alakú klózok (esetleg végtelen) halmaza, ahol az ℓ_i-k literálok (változók vagy negáltjuk), p pedig változó.

Páros-páratlan példa

$$\to \mathrm{even}(0) \qquad \neg\mathrm{even}(x) \to \mathrm{even}(\mathrm{s}(x))$$

Herbrand kiterjesztése

$$\to p_0 \qquad \neg p_0 \to p_1 \qquad \neg p_1 \to p_2 \qquad \neg p_2 \to p_3 \qquad \neg p_3 \to p_4$$

Szemantikájuk

Ami marad

Továbbra is van több modell.
Továbbra is modell a konstans igaz értékadás.
Továbbra is egy modellt akarunk választani.
Továbbra is nézhetjük a $T_{\mathcal{P}}$ függvényt:

$$T_{\mathcal{P}}(u)(r) := \bigvee_{p_1\wedge\ldots\wedge p_n\wedge\neg q_1\wedge\ldots\wedge\neg q_k\to r\in\mathcal{P}} u(p_1)\wedge\ldots\wedge u(p_n)\wedge\neg u(q_1)\wedge\ldots\wedge\neg u(q_k)$$

Továbbra is $T_{\mathcal{P}}$ prefixpontjai a $\mathcal{P}$ modelljei.

Ami változik...

A $T_{\mathcal{P}}$ függvény még csak nem is mindig monoton, nemhogy folytonos:

$$\neg p \to p$$

nincs fixpontja, nincs alátámasztott modellje!

Intervallumok

A problémát úgy hidaljuk át, hogy konkrét igazságértékek helyett igazságérték-intervallumokkal fogunk számolni.

$P \times P$

Ha P egy poset, akkor a $P \times P$ halmazt felfoghatjuk úgy, mint az intervallumok egy halmazát: az (x, y) intervallumba azok a z elemek tartoznak, melyekre $x \leq z \leq y$.
(Ha $x \not\leq y$, akkor az intervallum üres, avagy inkonzisztens. Ha $x \leq y$, akkor pedig konzisztens.)

Rendezések $P \times P$-n

Két rendezést definiálunk: a $\leq_t$ „igazságérték-rendezést" és a $\leq_p$ „precíziós rendezést":

$$(x, y) \leq_t (x', y') \Leftrightarrow x \leq x',\ y \leq y' \quad (\text{„igazabb"})$$
$$(x, y) \leq_p (x', y') \Leftrightarrow x \leq x',\ y' \leq y \quad (\text{„precízebb"})$$

Infimum, szuprémum

Jelölések

A $\bigvee$, $\bigwedge$ jeleket a $\leq_t$ szerinti, a $\oplus$, $\otimes$ jeleket pedig a $\leq_p$ szerinti szuprémumra ill. infimumra használjuk.

Állítás

Ha P teljes háló, akkor $(P \times P, \leq_t)$ is az és $(P \times P, \leq_p)$ is az.

A négyértékű logika

Ha a posetünk $L = \mathbf{2}$, akkor L^2 elemei:

- $(0, 0)$, a f, ,,hamis" elem;
- $(1, 1)$, a t, ,,igaz" elem;
- $(0, 1)$, a $\perp$, ,,unknown" elem;
- $(1, 0)$, a $\top$, ,,inkonzisztens" elem.

És f $<_t$ $\top, \perp$ $<_t$ t, valamint $\perp$ $<_p$ t, f $<_p$ $\top$.

Negálás

Legyen az intervallumokon a negálás a következő: $\neg(x, y) := (\neg y, \neg x)$.

Ez azért „jó” negálásnak, mert pl. $\neg f = \neg(0, 0) = (\neg 0, \neg 0) = (1, 1) = t$, hasonlóan $\neg t = f$ (tehát kiterjeszti a „hagyományos” negálást), $\neg\bot = \bot$ (unknown értékének a negáltjáról se tudunk semmit) és $\neg\top = \top$ (inkonzisztens érték inkonzisztens marad).

Állítás

A negálás $\leq_p$-monoton.

vagyis ha $(x, y) \leq_p (x', y')$, akkor $\neg(x', y') \leq_p \neg(x, y)$.

Bizonyítás

$$\begin{aligned}(x, y) \leq_p (x', y') &\Rightarrow x \leq x', y' \leq y \\ &\Rightarrow \neg x' \leq \neg x, \neg y \leq \neg y' \\ &\Rightarrow \neg(x, y) \leq_p (\neg x', y').\end{aligned}$$

A $\Phi_{\mathcal{P}}$ függvény

Hasonlít $T_{\mathcal{P}}$-hez, csak négyértékű

Ha $u \in (\mathbf{2} \times \mathbf{2})^Z$ egy értékadás (minden változó kap egy intervallumot értéknek), akkor vizsgálhatjuk a

$$\Phi_{\mathcal{P}}(w)(r) := \bigvee_{p_1 \wedge \ldots \wedge p_n \wedge \neg q_1 \wedge \ldots \wedge \neg q_k \to r \in \mathcal{P}} w(p_1) \wedge \ldots \wedge w(p_n) \wedge \neg w(q_1) \wedge \ldots \wedge w(q_k)$$

függvényt.

,,minden r változóra értékeljük ki az r fejű klózok törzsét és az igazságérték szerinti szuprémumra állítsuk be r új értékét.''
A törzsek kiértékelése közben az éselés is az igazságérték szerinti infimum, a negálás pedig az intervallumokra az előbb bevezetett negálás.

A $\Phi_\mathcal{P}$ függvény $\Psi_\mathcal{P}$ alakja

Átformalizálás

Matematikailag kezelhetőbb lesz a $\Phi_\mathcal{P}$ függvény, ha nem $(\mathbf{2} \times \mathbf{2})^Z$-t, hanem $\mathbf{2}^Z \times \mathbf{2}^Z$-t képzi önmagába.

A különbség

Tehát $\Phi_\mathcal{P}$ két „hagyományos” $u, v \in \mathbf{2}^Z$-beli értékadást kap: az elsőben az intervallumok „bal” végpontját, a másodikban a „jobb” végpontokat.

A bal végpontokat kiszámító függvény: $f_\mathcal{P}$

$$f_\mathcal{P}(u,v)(r) := \bigvee_{p_1 \wedge \ldots \wedge p_n \wedge \neg q_1 \wedge \ldots \wedge \neg q_k \to r \in \mathcal{P}} u(p_1) \wedge \ldots \wedge u(p_n) \wedge \neg v(q_1) \wedge \ldots \wedge \neg v(q_k).$$

A $\Phi_{\mathcal{P}}$ függvény $\Psi_{\mathcal{P}}$ alakja

A bal végpontokat kiszámító függvény: $f_{\mathcal{P}}$

$$f_{\mathcal{P}}(u,v)(r) := \bigvee_{p_1\wedge\ldots\wedge p_n\wedge\neg q_1\wedge\ldots\wedge\neg q_k\to r\in\mathcal{P}} u(p_1)\wedge\ldots\wedge u(p_n)\wedge\neg v(q_1)\wedge\ldots\wedge\neg v(q_k).$$

A jobb végpontokat kiszámító függvény: $g_{\mathcal{P}}$

$$g_{\mathcal{P}}(u,v)(r) := \bigvee_{p_1\wedge\ldots\wedge p_n\wedge\neg q_1\wedge\ldots\wedge\neg q_k\to r\in\mathcal{P}} v(p_1)\wedge\ldots\wedge v(p_n)\wedge\neg u(q_1)\wedge\ldots\wedge\neg u(q_k).$$

$$\Psi_{\mathcal{P}} := \langle f_{\mathcal{P}}, g_{\mathcal{P}}\rangle.$$

Vegyük észre: $f(u,v) = g(v,u)$!

Szimmetrikus és $\leq_p$-monoton függvények

Az $f = \langle f_1, f_2 \rangle$ függvény szimmetrikus, ha $f_1(x, y) = f_2(y, x)$.

Például a $\Psi_{\mathcal{P}}$ függvény szimmetrikus.

Állítás

Egy $f = \langle f_1, f_2 \rangle : L_1^2 \to L_2^2$ szimmetrikus függvény pontosan akkor $\leq_p$-monoton, ha f_1 is $\leq_p$-monoton.

Bizonyítás

Ha f szimmetrikus és $(x, y) \leq_p (x', y')$, akkor

$$\begin{aligned} f(x,y) \leq_p f(x',y') \quad &\Leftrightarrow \quad f_1(x,y) \leq f_1(x',y') \ \wedge \ f_2(x',y') \leq f_2(x,y) \\ &\Leftrightarrow \quad f_1(x,y) \leq f_1(x',y') \ \wedge \ f_1(y',x') \leq f_1(y,x), \end{aligned}$$

tehát ha f $\leq_p$-monoton, akkor f_1 is, és ha f_1 $\leq_p$-monodon, akkor $(x, y) \leq_p (x', y')$ maga után vonja az utolsó állítást is (mert akkor $(y', x') \leq_p (y, x)$ is igaz), így akkor f is $\leq_p$-monoton lesz.

A célunk most

- Be akarjuk látni azt, hogy a $\Psi_{\mathcal{P}}$ függvénynek is van legkisebb (pre)fixpontja.
- Ehhez először megmutatjuk, hogy $\leq_p$-monoton.
- Aztán azt mutatjuk meg, hogy teljes hálón monoton függvénynek mindig van legkisebb (pre)fixpontja (ami megint csak fixpont lesz).

Ez a legkisebb fixpont lesz majd az általános $\mathcal{P}$ program Kripke-Kleene szemantikája.

Monotonitás

Projekciók

Tetszőleges $z \in Z$-re a pozitív projekció $\pi_z^+(u, v) = u(z)$, a negatív projekció $\pi_z^-(u, v) = \neg v(z)$.

Állítás

A pozitív / negatív projekciók $\leq_p$-monotonok.

Bizonyítás

Legyen $(u, v) \leq_p (u', v')$, azaz $u \leq u'$ és $v' \leq v$. Ekkor:

- $\pi_z^+(u, v) = u(z) \leq u'(z) = \pi_z^+(u', v')$ (mert $u \leq u'$) és
- $\pi_z^-(u, v) = \neg v(z) \leq \neg v'(z) = \pi_z^-(u', v')$ (mert $v' \leq v$, így $v'(z) \leq v(z)$, tehát $\neg v(z) \leq \neg v'(z)$.

Monotonitás: infimum, szuprémum

Állítás

Ha $f_i : P \to Q$ monoton függvények, $i \in I$, akkor $\bigvee f_i$ és $\bigwedge f_i$ (ha léteznek) is monotonok.

Bizonyítás

Legyen $x, y \in P$, $x \leq y$. Akkor minden $i \in I$-re $f_i(x) \leq f_i(y)$ (mert az f_i-k monotonok). Ezért $X = \{f_i(x) : i \in I\}$ minden elemének van $Y = \{f_i(y) : i \in I\}$-beli felső korlátja, ezért
$(\bigvee f_i)(x) = \bigvee X \leq \bigvee Y = (\bigvee f_i)(y)$ és
$(\bigwedge f_i)(x) = \bigwedge X \leq \bigwedge Y = (\bigwedge f_i)(y)$.

Monotonitás: target tupling

Állítás

Ha minden $i \in I$-re $f_i : P \to Q$ monoton, akkor target tuplingjuk, $f = \langle f_i \rangle_{i \in I} : P \to Q^I$ is monoton.

Bizonyítás

Legyen $x, y \in P$, $x \leq y$. Be kell lássuk, hogy $f(x) \leq f(y)$.
Mivel $f(x), f(y)$ a Q^I poset elemei, ez annyit tesz, hogy minden $i \in I$-re $f(x)(i) \leq f(y)(i)$.
De a tupling def szerint $f(x)(i) = f_i(x)$ és $f(y)(i) = f_i(y)$, azt pedig, hogy $f_i(x) \leq f_i(y)$, tudjuk, mert f_i monoton.

Következmény

Az f_P függvény (és így Ψ_P is) $\leq_p$-monoton.

Monoton függvények fixpontjai: példa

Példa f

Vegyük a következő $f : P \to P$ függvényt, ahol $P = \mathbb{R}_0 \cup \{\infty\}$:
$f(n-\alpha) = n - \frac{\alpha}{2}$, ha n egész és $0 < \alpha \leq 1$, és $f(\infty) = \infty$.
Pl. $f(0) = 0.5$, $f(0.5) = 0.75$, $f(0.75) = 0.875$, $f(1) = 1.5$,
$f(42.5) = 42.75$.

Iteráció

$x_0 = 0$, $x_1 = 0.5$, $x_2 = 0.75$, $x_3 = 0.875$, $x_4 = 0.9375, \ldots$
(szuprémum) $x_\omega = 1$
(tovább) $x_{\omega+1} = 1.5$, $x_{\omega+2} = 1.75, \ldots$
(szuprémum) $x_{\omega\times 2} = 2$
$\ldots$
(végtelen sok szuprémum után) $x_{\omega\times\omega} = \infty$
és ez a legkisebb fixpont.

Rendszámok

Indexelés

Az előző sorozatot rendszámokkal indexeltük. Amit a rendszámokról tudni érdemes:

- a 0 egy rendszám;
- a rendszámokon van egy teljes rendezés, 0 a legkisebb rendszám;
- minden α rendszámnál van egy eggyel nagyobb, $\alpha + 1$, köztük nincs másik, az $\alpha + 1$ alakú rendszámok a rákövetkező rendszámok;
- rendszámok tetszőleges X halmazának van szuprémuma, az $\alpha = \bigvee_{\beta<\alpha} \beta$ alakú rendszámok a limesz rendszámok;
- tetszőleges α rendszámra az α-nál kisebb rendszámok halmazt alkotnak;
- rendszámokon lehet jólmegalapozott indukciót csinálni.

Jólmegalapozott indukció

Amit a legutolsó pont jelent: ha egy P tulajdonságról belátjuk, hogy

- P igaz a 0-ra;
- ha P igaz α-ra, akkor P igaz $\alpha + 1$-re is;
- ha $\alpha = \bigvee_{\beta<\alpha} \beta$ és P igaz minden $\beta < \alpha$-ra, akkor P igaz α-ra is;

akkor P igaz minden rendszámra.

Kripke-Kleene iteráció

Egy rendszámokkal indexelt sorozat

Legyen P teljes háló és $f : P \to P$ monoton függvény. Minden α rendszámhoz definiáljuk az $x_\alpha \in P$ elemet a következőképp:

- ha $\alpha = 0$, akkor $x_\alpha = \bot$.
- ha $\alpha = \beta + 1$ rákövetkező rendszám, akkor $x_\alpha = f(x_\beta)$.
- ha $\alpha = \bigvee_{\beta<\alpha} \beta$ limesz rendszám, akkor $x_\alpha = \bigvee_{\beta<\alpha} x_\beta$.

Állítás

Minden x_α az f-nek egy posztfixpontja.

Bizonyítás

- $x_0 = \bot \leq f(\bot)$, mert $\bot$ a P legkisebb eleme.
- Ha $x \leq f(x)$, akkor $f(x) \leq f(f(x))$, mert f monoton. Tehát ekkor $f(x)$ is posztfixpont. Így ha x_α posztfixpont, akkor $f(x_\alpha) = x_{\alpha+1}$ is az.

Kripke-Kleene iteráció

Bizonyítás tovább

Legyen X posztfixpontok tetszőleges halmaza. Akkor $x^* = \bigvee X$ is posztfixpont:

- Minden $x \in X$-re $x \leq x^*$, mert x^* az X-nek egy felső korlátja.
- Az f monotonitása miatt tehát minden $x \in X$-re $f(x) \leq f(x^*)$.
- Mivel X-ben posztfixpontok vannak, így minden $x \in X$-re $x \leq f(x)$, tehát $x \leq f(x^*)$.
- Tehát $f(x^*)$ az X-nek egy felső korlátja.
- x^* pedig az X-nek a legkisebb felső korlátja, így $x^* \leq f(x^*)$, tehát x^* is posztfixpont.

Tehát ha α limesz rendszám és minden $\beta < \alpha$-ra x_β posztfixpont, akkor $x_\alpha = \bigvee_{\beta<\alpha} x_\beta$ is posztfixpont.

Kripke-Kleene iteráció

Állítás

Legyen X az összes x_α alakban előálló elem halmaza.
Akkor X-nek van legnagyobb eleme, ami egy fixpont.

Bizonyítás

Legyen minden $x \in X$-re α_x egy olyan rednszám, melyre $x = x_{\alpha_x}$. Akkor az $\{\alpha_x : x \in X\}$ rendszám-halmaznak van szuprémuma, legyen ez α.
Legyen α^* az $\{\alpha, \alpha + 1, \alpha + 2, \dots\}$ rendszám-halmaz szuprémuma.
Ekkor α^* limesz rendszám és nagyobb, mint bármelyik α_x.
Így $x^* = x_{\alpha^*} = \bigvee_{\beta<\alpha^*} x_\beta = \bigvee X$, mert minden X-beli elem előáll x_β alakban egy $\beta < \alpha^*$ rendszámra és mert minden x_β alakú elem X-beli.
De akkor $x_{\alpha^*+1} = f(x^*)$ is X-beli (tehát posztfixpont is) és $f(x^*) \leq x^*$ (mert x^* az X-nek egy felső korlátja), tehát $f(x^*) = x^*$.

Kripke-Kleene iteráció

Állítás

X legnagyobb eleme az f legkisebb (pre)fixpontja.

Bizonyítás

Azt már láttuk az előbb, hogy ez az $x^* = \bigvee X$ elem létezik és X-beli, továbbá hogy fixpont. Megmutatjuk, hogy tetszőleges y prefixpontra $X \leq y$.
(Ebből kapjuk, hogy $\bigvee X \leq y$, vagyis y a legkisebb prefixpont.)
Jólmegalapozott indukcióval belátjuk, hogy minden $x_\alpha \leq y$:

- Ha $\alpha = 0$, akkor $x_\alpha = \bot \leq y$, mert $\bot$ a legkisebb elem.
- Ha $\alpha = \beta + 1$ és $x_\beta \leq y$, akkor f monotonitása miatt $x_\alpha = f(x_\beta) \leq f(y)$, és $f(y) \leq y$, mert y prefixpont. Így $x_\alpha \leq y$.
- Ha $\alpha = \bigvee_{\beta<\alpha} \beta$, és minden $\beta < \alpha$-ra $x_\beta \leq y$, akkor $x_\alpha = \bigvee_{\beta<\alpha} x_\beta$ az $\{x_\beta : \beta < \alpha\}$ halmaznak a legkisebb felső korlátja, y pedig egy felső korlátja, tehát $x_\alpha \leq y$.

Kripke-Kleene iteráció

Tétel

Beláttuk tehát, hogy minden $f : P \to P$ monoton függvénynek a P teljes hálón létezik legkisebb (pre)fixpontja, mely előáll a Kripke-Kleene iterációval.

A Kripke-Kleene szemantika

Így egy $\mathcal{P}$ általános logikai program Kripke-Kleene szemantikáját definiálhatjuk mint a $\Psi_{\mathcal{P}}$ függvény $\leq_p$-legkisebb (pre)fixpontját. Jelölje ezt $\kappa(\mathcal{P})$.

A Kripke-Kleene szemantika jó tulajdonságai

Approximációs függvények

Az $f : P^2 \to P^2$ függvényt approximációs függvénynek nevezzük, ha f szimmetrikus és $\leq_p$-monoton.

Például $\Psi_{\mathcal{P}}$ ilyen.

Állítás

Approximációs függvény Kripke-Kleene fixpontja mindig konzisztens.

Konzisztencia

Bizonyítás

Először belátjuk, hogy ha $\beta < \alpha$, akkor $x_\beta \leq x_\alpha$. Ezt α szerinti jólmegalapozott indukcióval tesszük:

- Ha $\alpha = 0$, akkor nincs nála kisebb rendszám és az állítás igaz.
- Ha $\alpha = \beta + 1$, akkor $x_\beta \leq f(x_\beta) = x_\alpha$, mert x_β posztfixpont.
- Ha $\alpha = \bigvee_{\beta<\alpha}$, akkor $x_\alpha = \bigvee_{\beta<\alpha} x_\beta$, tehát $x_\beta \leq x_\alpha$ (mert x_α az x_β-k felső korlátja).

Most belátjuk, hogy minden x_α konzisztens, ha $f : P^2 \to P^2$ approximációs függvény, α szerinti jólmegalapozott indukcióval:

- ha $\alpha = 0$, akkor $x_\alpha = (\bot, \top)$ (ez a $\leq_p$-legkisebb elem), ami konzisztens, mert $\bot \leq \top$.
- ha $\alpha = \beta + 1$, mondjuk $x_\beta = (x, y)$, ahol indukció szerint $x \leq y$, akkor $x_\alpha = f(x_\beta) = (f_1(x, y), f_2(x, y)) = (f_1(x, y), f_1(y, x))$ és $f_1(x, y) \leq f_1(y, x)$, mert $(x, y) \leq_p (y, x)$ és $f_1 \leq_p$-monoton.

Konzisztencia

Bizonyítás, tovább

Végül, ha $\alpha = \bigvee_{\beta<\alpha} \beta$, akkor $x_\alpha = \bigoplus_{\beta<\alpha} x_\beta$ (mert ha f egy $\leq_p$-monoton függvény, akkor $\leq_p$ szerinti szuprémumát kell vegyük).
Legyen minden β-ra $x_\beta = (u_\beta, v_\beta)$. Indukció szerint $u_\beta \leq v_\beta$ és az előzőből tudjuk, hogy ha $\beta \leq \gamma$, akkor $(u_\beta, v_\beta) \leq_p (u_\gamma, v_\gamma)$, azaz $u_\beta \leq u_\gamma$ és $v_\gamma \leq v_\beta$.
Ekkor $\bigoplus_{\beta<\alpha} x_\beta = \left(\bigvee_{\beta<\alpha} u_\beta, \bigwedge_{\beta<\alpha} v_\beta\right)$.
Legyen $U = \{u_\beta : \beta < \alpha\}$ és $V = \{v_\beta : \beta < \alpha\}$. Megmutatjuk, hogy $U \leq V$, ebből következik, hogy $\bigvee U \leq \bigwedge V$, tehát hogy x_α konzisztens.
Legyen $u_\beta \in U$ és $v_\gamma \in V$. Két eset lehetséges: $\beta \leq \gamma$ vagy $\gamma \leq \beta$.

- Ha $\beta \leq \gamma$, akkor $u_\beta \leq u_\gamma \leq v_\gamma$.
- Ha $\gamma \leq \beta$, akkor $u_\beta \leq v_\beta \leq v_\gamma$.

Tehát $U \leq V$ és így x_α konzisztens.

A Kripke-Kleene szemantika rossz tulajdonságai

A Kripke-Kleene szemantika

- nem minimalizálja az igazságértéket;
- negációmentes programokon nem ugyanaz, mint a kanonikus szemantika.

A célunk most

- Definiáljuk approximációs függvények stabilizációs függvényeit.
- Megmutatjuk, hogy a stabilizációs függvény is approximációs függvény. (Tehát pl. van fixpontja, sőt $\leq_p$-legkisebb fixpontja is.)
- Megmutatjuk, hogy a stabilizációs függvény minden fixpontja az eredeti approximációs függvény $\leq_t$-minimális fixpontja is.
- Így általános logikai programok ún. jólmegalapozott szemantikáját definiálhatjuk mint a $\Psi_{\mathcal{P}}$ függvény stabilizációs függvényének $\leq_p$-legkisebb fixpontját.
- Az így kapott szemantika minimalizálja az igazságértéket és negációmentes programokon ugyanaz lesz, mint a kanonikus.

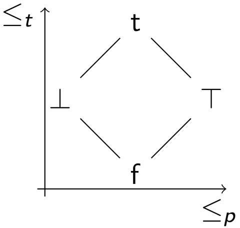
Recap: Kripke-Kleene szemantika, példa

Vegyük a következő $\mathcal{P}$ logikai programot:

$$\begin{array}{rcl} & \rightarrow & p \\ p & \rightarrow & q \\ r \wedge s & \rightarrow & q \\ p \wedge q & \rightarrow & r \\ s & \rightarrow & t \end{array}$$

Erre $\Phi_{\mathcal{P}}$ iterációja:

Z	szabály	0	1	2	3	4
p	$\bigvee \bigwedge \emptyset = \mathrm{t}$	$\bot$	t	t	t	t
q	$p \vee (r \wedge s)$	$\bot$	$\bot$	t	t	t
r	$p \wedge q$	$\bot$	$\bot$	$\bot$	t	t
s	$\bigvee \emptyset = \mathrm{f}$	$\bot$	f	f	f	f
t	s	$\bot$	$\bot$	$\bot$	f	f



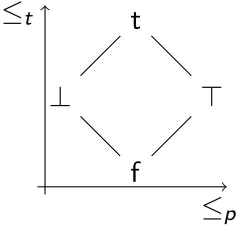
Recap: Kripke-Kleene szemantika, példa

Vegyük a következő $\mathcal{P}$ logikai programot:

$$\begin{array}{rcl} & \rightarrow & p \\ p & \rightarrow & q \\ r \wedge s & \rightarrow & q \\ p \wedge q & \rightarrow & r \\ s & \rightarrow & t \\ s & \rightarrow & s \end{array}$$

Erre $\Phi_{\mathcal{P}}$ iterációja:

Z	szabály	0	1	2	3	4
p	$\bigvee \bigwedge \emptyset = \mathrm{t}$	$\perp$	t	t	t	t
q	$p \vee (r \wedge s)$	$\perp$	$\perp$	t	t	t
r	$p \wedge q$	$\perp$	$\perp$	$\perp$	t	t
s	s	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$
t	s	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$



Erre a kanonikus szemantika $s = t = \mathrm{f}$!

$\mu x.f_1(x, y)$

Ha $f : P^2 \to P$ monoton függvény, akkor tetszőleges $y \in P$-ra a $\lambda x.f(x, y)$ függvény is az.
(A $\lambda x.f(x, y)$ jelölés az $x \mapsto f(x, y)$ függvényt jelenti, ami egy $P \to P$ függvény).

Hiszen ha $x \leq x'$, akkor $f(x, y) \leq f(x', y)$.

Mivel $\lambda x.f(x, y)$ egy $P \to P$ monoton függvény, van legkisebb fixpontja.
Ezt $\mu x.f(x, y)$ jelöli.

Stabilizációs függvény

Ha $f = \langle f_1, f_2 \rangle : P^2 \to P^2$ approximációs függvény (=szimmetrikus és $\leq_p$-monoton), akkor stabilizációs függvénye az $s(x, y) = (s_1(y), s_1(x))$, $s_1(z) = \mu x.f_1(x, z)$ függvény.

$\mu x.f_1(x,y)$

Mit „jelent” $\mu x.f_1(x,y)$ pl. $\Psi_{\mathcal{P}}$ esetén?

- Az f_1 függvény megkapta az x, y intervallumvégpontokat: x a bal, y a jobb végpontok vektora.
- Ebből kiszámolta az új intervallum-balvégpontokat. (f_2 pedig a jobbakat).
- Akkor $s_1(y)$: rögzítjük a jobb végpontokat y-ra, kiindulunk a $\perp$ balvégpontokból (mindenki 0), $x_1 = f_1(\perp, y)$ a bal végpontok új értéke, $x_2 = f_1(x_1, y)$,..., iteráljuk f_1-et mindig ugyanazokkal a jobb végpontokkal, csak a bal végpontokat updateljük.
- A legkisebb fixpont az eredmény.

Az $s(x,y) = (s_1(y), s_1(x))$ képletben a második argumentum $s_1(x)$, ez $\mu y.f_1(y,x) = \mu y.f_2(x,y)$, ugyanez szimmetrikusan: a bal végpontokat rögzítjük x-re és csak a jobbakra számolunk legkisebb fixpontot.

A stabilizációs függvény jobb

Állítás

Ha s az f stabilizációs függvénye, akkor s is approximációs függvény.

Bizonyítás

- s szimmetrikus, hiszen $s(x, y) = (s_1(y), s_1(x))$, $s(y, x) = (s_1(x), s_1(y))$: az argumentumok cseréje megcseréli az output koordinátáit.
- s $\leq_p$-monoton: ha $(x, y) \leq_p (x', y')$, akkor $x \leq x'$ és $y' \leq y$. Elég belátnunk, hogy s_1 antimonoton: ha $x \leq x'$, akkor $s_1(x') \leq s_1(x)$. (Ekkor lesz az $(x, y) \mapsto s_1(y)$ függvény $\leq_p$-monoton.) Legyen $y = s_1(x)$. Akkor $y = f_1(y, x)$. Ha $x \leq x'$, akkor $(y, x') \leq_p (y, x)$, f_1 $\leq_p$-monotonitása miatt akkor $f_1(y, x') \leq f_1(y, x) = y$. Tehát $y = s_1(x)$ a $\lambda y.f_1(y, x')$ függvénynek egy prefixpontja. $s_1(x')$ pedig a legkisebb prefixpontja, tehát $s_1(x') \leq s_1(x)$.

A stabilizációs függvény jobb

Állítás

Ha s az f stabilizációs függvénye, akkor s minden fixpontja az f-nek egy $\leq_t$-minimális fixpontja.

Bizonyítás

Legyen $s(x, y) = (x, y)$.

- Fixpont: akkor $x = s_1(y)$ és $y = s_1(x)$. Tehát $x = f_1(x, y)$ és $y = f_1(y, x) = f_2(x, y)$, tehát $(x, y) = f(x, y)$ az f-nek is fixpontja.
- $\leq_t$-minimális: Legyen $(x', y') \leq_t (x, y)$ szintén fixpontja f-nek.
  - Akkor $f_1(x', y') = x'$ és $f_1(y', x') = y'$.
  - Mivel $x' \leq x$ és $y' \leq y$, így $(x', y) \leq_p (x', y')$.
  - Így $f_1(x', y) \leq f_1(x', y') = x'$, tehát x' a $\lambda x.f_1(x, y)$-nak egy prefixpontja.
  - Az $x = s_1(y)$ pedig a legkisebb prefixpontja $\Rightarrow x \leq x'$, ezért $x = x'$.
  - Hasonlóan $y = y'$ is, tehát $(x, y) = (x', y')$, így (x, y) egy $\leq_t$-minimális fixpont.

A jólmegalapozott szemantika

Definíció

A $\mathcal{P}$ általános logikai program jólmegalapozott szemantikája a $\Psi_{\mathcal{P}}$ függvény stabilizációs függvényének a $\leq_p$-legkisebb fixpontja (azaz a Kripke-Kleene fixpontja).

Állítás

A jólmegalapozott szemantika is mindig konzisztens, $\leq_t$-minimális és negációmentes programokra ugyanaz, mint a kanonikus szemantika.

Ugyanaz, mint a kanonikus

A $\Psi_{\mathcal{P}}$ függvényben $f_{\mathcal{P}}(x, y) = T_{\mathcal{P}}(x)$, ha $\mathcal{P}$ negációmentes.
Akkor az $s_1(y)$ függvény $T_{\mathcal{P}}$ legkisebb fixpontját adja vissza, ami maga a kanonikus szemantika.

Logikai programok szemantikája, összefoglalás

- Logikai program: $p_1 \wedge \ldots \wedge p_n \rightarrow q$ alakú implikációk $\mathcal{P}$ halmaza.
- $T_{\mathcal{P}}$: a q változó új értéke a q fejű klózok törzseinek régi értékeinek szuprémuma.
- $T_{\mathcal{P}}$ prefixpontjai: $\mathcal{P}$ modelljei.
- A kanonikus szemantika: a legkisebb (pre)fixpont.
- Általános logikai program: $p_1 \wedge \ldots \wedge p_n \wedge \neg q_1 \wedge \ldots \wedge \neg q_k \rightarrow r$ alakú klózok $\mathcal{P}$ halmaza.
- Négyértékű logika: $\perp$, t, f és $\top$, mint intervallumok.
- $T_{\mathcal{P}}$ megfelelője ebben az esetben: $\Phi_{\mathcal{P}}$.
- $\Phi_{\mathcal{P}}$-nek egy másik formája: $\Psi_{\mathcal{P}}$, aki $\leq_p$-monoton.
- Kripke-Kleene szemantika: $\Phi_{\mathcal{P}}$ legkisebb fixpontja $\leq_p$ szerint.
- Stabilizációs függvény: egy lépésen belül is fixpontiterálunk.
- Jólmegalapozott szemantika: $\Phi_{\mathcal{P}}$ legkisebb stabil fixpontja.
- Ez minimalizálja az igazságértékeket és kiterjeszti a kanonikust.

Funkcionális programozási nyelvek szemantikája

Funkcionális nyelvek

- Vannak elemi adattípusok
- és ha A és B már típus, akkor az $A \to B$ függvények is egy osztályt alkotnak
- a nyelv támogatja olyan függvények írását, melyek valamilyen típusú függvényt várnak argumentumként és szintén (esetleg másmilyen típusú) függvényt is adhatnak vissza

Scala példa

Példa

Változó

Változó típusának deklarálása

Visszatérési érték típusa

Függvény alkalmazása

def iterate $(f : \mathrm{Int} \to \mathrm{Int}) : \mathrm{Int} \to \mathrm{Int}$ {

$n \Rightarrow$ if($n == 0$) $f(1)$ else $f($ iterate $(f)(n-1))$

}

Függvény-absztrakció

Rekurzió

if $-$ else

Built-in: $0,\ 1,\ x \mapsto x - 1$

λ-kalkulus: Típusok

- nat az egyetlen alaptípus (szándék: objektumai a természetes számok)
- ha σ és τ típusok, akkor $(\sigma \to \tau)$ is típus (szándék: objektumai olyan egyváltozós függvények, melyek σ típusú inputot várnak és τ típusú outputot adnak vissza)

Példák

- nat $\to$ nat egy típus (ilyen típusú lehet pl. az $n \mapsto n+1$ vagy az $n \mapsto 2n$ függvény)
- nat $\to$ (nat $\to$ nat) egy típus (input: egy szám; output: egy szám$\to$szám függvény. Ilyen lehet pl. az $n \mapsto (m \mapsto n+m)$ függvény: ha az input az n szám, az output az ,,adjunk hozzá az inputhoz n-t'' függvény lesz)
- (nat $\to$ nat) $\to$ (nat $\to$ nat) egy típus (input: egy szám$\to$szám függvény, output: egy szám$\to$ szám függvény. Ilyen pl. az $f \mapsto (n \mapsto 2f(n))$ függvény: ha az input az f függvény, az output egy olyan f' függvény, ami minden outputra pont kétszer annyit ad, mint az f)

λ-kalkulus: változódeklarációk – környezetek

Context, környezet

egy $\Gamma \;=\; x_1 : \sigma_1, x_2 : \sigma_2, \ldots, x_n : \sigma_n$ sorozat, az x_i-k különböznek

kb. „x_1 egy σ_1 típusú, x_2 egy σ_2 típusú stb. változó"

Példa

Az iterate függvényünk belsejében (pl. az $f(1)$ résznél) a környezet

$$\Gamma \;=\; n : \mathsf{nat},\;\; f : \mathsf{nat} \to \mathsf{nat},\;\; \mathsf{iterate} : (\mathsf{nat} \to \mathsf{nat}) \to (\mathsf{nat} \to \mathsf{nat})$$

λ-kalkulus: termek

λ-term

Egy $\Gamma \vdash M : \sigma$ alakú hármas, ahol

- Γ egy környezet,
- σ egy típus (a ,,visszatérési értéké"),
- M egy ún. ,,nyers term" (tkp. maga a term ,,kódja")

A valid termeket építési szabályok alkalmazásával képezzük.

Konstans

A 0 kifejezés (nyers term) minden környezetben egy nat típusú term:

$$\frac{}{\Gamma \ \vdash \ 0 \ : \ \mathrm{nat}}$$

Built-in

Ha egy környezetben M egy nat típusú term, akkor succ(M) és pred(M) is nat típusú termek (ugyanabban a környezetben):

$$\frac{\Gamma \ \vdash \ M \ : \ \mathrm{nat}}{\Gamma \ \vdash \ \mathrm{succ}(M) \ : \mathrm{nat}} \qquad \frac{\Gamma \ \vdash \ M \ : \ \mathrm{nat}}{\Gamma \ \vdash \ \mathrm{pred}(M) \ : \mathrm{nat}}$$

Példák

Ha Γ az előbbi környezet, akkor

$$\Gamma \vdash \ 0 \ : \ \mathrm{nat}$$

$$\Gamma \vdash \ \mathrm{succ}(0) \ : \ \mathrm{nat}$$

Változók

Ha a környezetben szerepel $x : \sigma$, akkor x egy kifejezés, aminek típusa σ:

$$\frac{}{\Gamma_1, x : \sigma, \Gamma_2 \ \vdash \ x \ : \ \sigma}$$

Példák

Ha Γ az előbbi környezet, akkor

$$\begin{aligned}
\Gamma &\vdash n : \mathsf{nat} \\
\Gamma &\vdash f : \mathsf{nat} \to \mathsf{nat} \\
\Gamma &\vdash \mathsf{iterate} : (\mathsf{nat} \to \mathsf{nat}) \to (\mathsf{nat} \to \mathsf{nat}) \\
\Gamma &\vdash \mathsf{pred}(n) : \mathsf{nat}
\end{aligned}$$

Függvény-alkalmazás (application)

Ha Γ-ban M típusa $\sigma \to \tau$, N típusa pedig σ, akkor $M(N)$ egy kifejezés, aminek típusa τ:

$$\frac{\Gamma \vdash M : \sigma \to \tau, \quad \Gamma \vdash N : \sigma}{\Gamma \vdash M(N) : \tau}$$

Példák

Ha Γ az előbbi környezet, akkor

$$\begin{aligned}
\Gamma &\vdash f(\mathrm{succ}(0)) : \mathrm{nat} \\
\Gamma &\vdash \mathrm{iterate}(f) : \mathrm{nat} \to \mathrm{nat} \\
\Gamma &\vdash (\mathrm{iterate}(f))(\mathrm{pred}(n)) : \mathrm{nat} \\
\Gamma &\vdash f\big((\mathrm{iterate}(f))(\mathrm{pred}(n))\big) : \mathrm{nat}
\end{aligned}$$

Feltételes elágazás (conditional branching, ifzero)

Ha Γ-ban M_1, M_2 és M_3 típusa nat, akkor ifzero(M_1, M_2, M_3) típusa is nat:

$$\frac{\Gamma \vdash M_1 : \mathrm{nat}, \quad \Gamma \vdash M_2 : \mathrm{nat}, \quad \Gamma \vdash M_3 : \mathrm{nat}}{\Gamma \ \vdash \ \mathrm{ifzero}(M_1, M_2, M_3) \ : \ \mathrm{nat}}$$

Példa

$$\Gamma \vdash \mathrm{ifzero}\Big(n, f(\mathrm{succ}(0)), f\big((\mathrm{iterate}(f))(\mathrm{pred}(n))\big)\Big) \ : \ \mathrm{nat})$$

λ-absztrakció (függvényabsztrakció)

Ha a $\Gamma = \Gamma_1, x : \sigma, \Gamma_2$ környezetben M típusa τ, akkor a Γ_1, Γ_2 környezetben $\lambda x : \sigma.(M)$ típusa $\sigma \to \tau$:

$$\frac{\Gamma_1, x : \sigma, \Gamma_2 \;\vdash\; M \;:\; \tau}{\Gamma_1, \Gamma_2 \;\vdash\; \lambda x : \sigma.(M) \;:\; \sigma \to \tau}$$

Tkp. egy eddigi ,,globális'' változót formális paraméterré alakítunk.

Példa

$$f : \mathrm{nat} \to \mathrm{nat}, \mathrm{iterate} : (\mathrm{nat} \to \mathrm{nat}) \to (\mathrm{nat} \to \mathrm{nat})$$

$$\vdash \lambda n : \mathrm{nat}.\mathrm{ifzero}\Big(n, f(\mathrm{succ}(0)), f\big((\mathrm{iterate}(f))(\mathrm{pred}(n))\big)\Big) \;:\; \mathrm{nat} \to \mathrm{nat}$$

$$\mathrm{iterate} : (\mathrm{nat} \to \mathrm{nat}) \to (\mathrm{nat} \to \mathrm{nat})$$

$$\vdash \lambda f : \mathrm{nat} \to \mathrm{nat}.\lambda n : \mathrm{nat}.\mathrm{ifzero}\Big(n, f(\mathrm{succ}(0)), f\big((\mathrm{iterate}(f))(\mathrm{pred}(n))\big)\Big)$$

$$: \;(\mathrm{nat} \to \mathrm{nat}) \to (\mathrm{nat} \to \mathrm{nat})$$

Rekurzió (fixpont)

Ha a Γ környezetben M típusa $\sigma \rightarrow \sigma$, akkor $Y_\sigma(M)$ típusa σ:

$$\frac{\Gamma \vdash M : \sigma \rightarrow \sigma}{\Gamma \vdash Y_\sigma(M) : \sigma}$$

Ezt a konstrukciót rekurzív függvényhívások modellezésére fogjuk használni (mivel λ-kalkulusban a termeket nem ,,nevezzük el'', így másképp kell megoldani a rekurzív hívásokat), hamarosan látni fogjuk, hogyan.

Példa: Az iterate függvénnyel (majdnem) ekvivalens λ-term

$$\vdash Y_{(\mathrm{nat}\rightarrow\mathrm{nat})\rightarrow(\mathrm{nat}\rightarrow\mathrm{nat})}\Big($$
$$\lambda i : (\mathrm{nat} \rightarrow \mathrm{nat}) \rightarrow (\mathrm{nat} \rightarrow \mathrm{nat}).\lambda f : \mathrm{nat} \rightarrow \mathrm{nat}.\lambda n : \mathrm{nat}.$$
$$\mathrm{ifzero}\Big(n, f(\mathrm{succ}(0)), f\big((i(f))(\mathrm{pred}(n))\big)\Big)\Big)$$
$$: (\mathrm{nat} \rightarrow \mathrm{nat}) \rightarrow (\mathrm{nat} \rightarrow \mathrm{nat}).$$

Célunk

- Először megadunk egy műveleti szemantikát, ami nyers termeknek egy átírási szabályrendszere lesz; ez hasonló lesz nagyon a funkcionális programok ,,futtatásának'' módjához, lépésenként átírva a termeket egymásba, majd megállva egy végeredménnyel (vagy végtelen ciklusba esve).
- Ezután megadjuk termeknek egy denotációs szemantikát is, ami pedig egy termhez egy (folytonos) függvényt rendel majd; ez ahhoz hasonló, mikor egy függvényről azt mondjuk, hogy ,,ez a négyzetreemelés függvény'', ,,ez a faktoriális'' stb.
- Ezután belátjuk, hogy a két szemantika ekvivalens (azaz ők ketten valójában funkcionális programozási nyelveknek egy szemantikájának két vetülete, a ,,hogyan'' és a ,,mit'' nézete ugyanannak a viselkedésnek).

Műveleti szemantika

Ezt a szemantikát nyers termekre definiáljuk: $M \triangleright N$ jelöli azt, hogy az M termet egy lépésben átírjuk az N termre.

- $M \triangleright^* N$: nulla, egy vagy több lépésben.
- $M \Downarrow N$: $M \triangleright^* N$ és N már nem írható át.
- Azokat a nyers termeket, melyeket nem tudjuk átírni, (szintaktikus) értéknek (value) nevezzük.
- Ha $M \Downarrow V$, akkor azt mondjuk, hogy az M értéke V.
- Ha M-nek nincs értéke, annak jele $M \nearrow$ lesz.

Nyers term

$$M \to 0 \mid x \mid \mathrm{pred}(M) \mid \mathrm{succ}(M) \mid M(M) \mid \mathrm{ifzero}(M, M, M) \mid \lambda x : \sigma.M \mid Y_\sigma(M)$$

Konstans, változó, λ-absztrakció

Ezek mind értékek: 0, x és a $\lambda x : \sigma . M$ alakú nyers termek.

Jelölje $\underline{n}$ a $\mathrm{succ}^n 0$ nyers termet. Ezek lesznek a számok.

Built-inek

Ha a termünk $\mathrm{succ}(M)$ és belseje nem érték, akkor átírjuk (redukáljuk) a belsejét:

$$\frac{M \triangleright N}{\mathrm{succ}(M) \triangleright \mathrm{succ}(N)}$$

Ha a termünk $\mathrm{pred}(M)$ és belseje...

- 0, akkor átírjuk 0-ra az egészet: $\mathrm{pred}(0) \triangleright 0$
- pozitív szám, akkor eggyel csökkentjük: $\mathrm{pred}(\underline{n+1}) \triangleright \underline{n}$
- nem érték, akkor a belsejét redukáljuk:

$$\frac{M \triangleright N}{\mathrm{pred}(M) \triangleright \mathrm{pred}(N)}$$

Alkalmazás

Ha a termünk $M(N)$ alakú, akkor...

- ha M redukálható, akkor redukáljuk:

$$\frac{M \;\triangleright\; M'}{M(N) \;\triangleright\; M'(N)}$$

- ha $M = \lambda x : \sigma.M'$ alakú, akkor M'-ben az x-ek helyére N-t helyettesítünk (pontosabban ld mindjárt):

$$(\lambda x : \sigma.M)(N) \;\triangleright\; M[x/N]$$

- egyébként nem tudunk redukálni.

Helyettesítés

Mint elsőrendű logikában

Ha M egy nyers term, x egy változó és N szintén egy nyers term, akkor $M[x/N]$ az a nyers term, amit úgy kapunk, hogy M-ben az összes szabad x-et átírjuk N-re úgy, hogy ha egy beírt N-ben így „lekötődne" változó, annak a kötő λ-ját átnevezzük, hogy feloldjuk a névütközést

Formálisan

- $0[x/N] = 0$
- $x[x/N] = N$, és $y[x/N] = y$,ha $x \neq y$
- $\text{pred}(M)[x/N] = \text{pred}(M[x/N])$, $\text{succ}(M)[x/N] = \text{succ}(M[x/N])$
- $\text{ifzero}(M_1, M_2, M_3)[x/N] = \text{ifzero}(M_1[x/N], M_2[x/N], M_3[x/N])$
- $(\lambda x : \sigma.M)(x/N) = \lambda x : \sigma.M$
- $(\lambda y : \sigma.M)[x/N] = \lambda z : \sigma.M[y/z][x/N]$, ha $y \neq x$, ahol z olyan változó, mely nem fordul elő sehol máshol
- $Y_\sigma(M)[x/N] = Y_\sigma(M[x/N])$

Elágazás

Ha a termünk ifzero(M_1, M_2, M_3) alakú, akkor

- Ha $M_1 = 0$, akkor átírjuk az egészet M_2-re: ifzero$(0, M_2, M_3) \ \triangleright\ M_2$
- Ha M_1 egy pozitív szám, akkor átírjuk az egészet M_3-ra: ifzero$(\underline{n+1}, M_2, M_3) \triangleright M_3$
- Ha M_1 redukálható, akkor redukáljuk:

$$\frac{M_1 \ \triangleright\ N_1}{\text{ifzero}(M_1, M_2, M_3) \ \triangleright\ \text{ifzero}(N_1, M_2, M_3)}$$

- egyébként nem tudunk redukálni.

Rekurzió

Ha a termünk $Y_\sigma(M)$ alakú, akkor redukáljuk $M(Y_\sigma(M))$-re:

$$Y_\sigma(M) \ \triangleright\ M(Y_\sigma(M))$$

Példa: $2 \times 2 = 4$

Nézzünk egy példát, amiből a rekurzió is világosabb lesz.

Scala

$$\text{def } f(n) \;=\; \text{if}(n = 0)\ 0 \text{ else } 2 + f(n-1);\;\; f(2)$$

Ez a kettővel szorzás függvény.

Nyers λ-term (unárisaknál $f(x)$ helyett $f.x$, típusok elhagyva)

$$\Big(Y.\lambda f.\lambda n.\text{ifzero}\big(n, 0, \text{succ.succ}.f.\text{pred}.n\big)\Big)(\text{succ.succ}.0)$$

Nézzük meg, hogy a redukálási szabályokkal ebből hogy kapunk succ.succ.succ.succ.0-t! (négyet)

Denotációs szemantika

Ez a szemantika egy $\Gamma \vdash M : \sigma$ termhez rendel egy $[[\Gamma \vdash M : \sigma]]$-val jelölt (folytonos) függvényt.

A típusok interpretációs domainek

Először is minden σ típushoz rendelünk egy $[[\sigma]]$ alaphalmazt, domaint (a σ típusú „objektumok" halmazát). Ez egy poset lesz.

- $[[\text{nat}]]$ legyen az $\mathbb{N}_\perp$ poset.
- $[[\sigma \to \tau]]$ legyen a $[[\sigma]] \to [[\tau]]$ folytonos függvények posetje.

A $P \to Q$ folytonos függvények posetjét jelölje innentől $[P \to Q]$.
Tehát $[[\sigma \to \tau]] = \big[[[\sigma]] \to [[\tau]]\big]$.

Ha $\Gamma = x_1 : \sigma_1, \ldots, x_n : \sigma_n$ környezet, akkor legyen $[[\Gamma]] = [[\sigma]] \times \ldots \times [[\sigma]]$.

A $[[\Gamma \vdash M : \sigma]]$ függvények $[[\Gamma]] \to [[\sigma]]$ függvények lesznek.

Teljes részbenrendezett halmazok, CPOk

Az $\mathbb{N}_\perp$ poset nem teljes háló.

De szuprémumokkal kell dolgoznunk. Egy gyengébb struktúra:

Definíció: CPO

A P poset CPO, ha minden lineárisan rendezett részhalmazának van szuprémuma.

Lineárisan rendezett az X halmaz, ha bármelyik két eleme összehasonlítható.

Például $X_\perp$ minden X-re CPO, így $[[\mathrm{nat}]] = \mathbb{N}_\perp$ is az.

Fixpontokkal akarunk majd számolni. A Tarski-féle fixponttétel szerint ha P CPO és $f : P \to P$ folytonos függvény, akkor van legkisebb fixpontja. Ezért belátjuk, hogy minden domain CPO és minden $[[\ldots]]$ függvény folytonos lesz.

Minden típus domainje CPO

Állítás

Ha P és Q CPO-k, akkor $[P \to Q]$ is az.

Bizonyítás

Legyen $F \subseteq [P \to Q]$ folytonos $P \to Q$ függvények lineárisan rendezett halmaza. Belátjuk, hogy $\bigvee F$ létezik és folytonos.

- Azt tudjuk, hogy $(\bigvee F)(x) = \bigvee_{f \in F} f(x)$ ha létezik, akkor ez a szuprémuma F-nek.
- Mivel $\{f(x) : f \in F\} \subseteq Q$ és Q CPO, így ha belátjuk, hogy $\{f(x) : f \in F\}$ lineárisan rendezett, akkor $\bigvee F$ létezik.
- Legyen $f_1(x), f_2(x) \in \{f(x) : f \in F\}$. Mivel $f_1, f_2 \in F$, és F lineárisan rendezett, így vagy $f_1 \leq f_2$, vagy $f_2 \leq f_1$.
- Ha $f_1 \leq f_2$, akkor (függvény $\leq$ def szerint) $f_1(x) \leq f_2(x)$; ha $f_2 \leq f_1$, akkor $f_2(x) \leq f_1(x)$. Tehát $\bigvee F$ létezik $P \to Q$-ban.

Minden típus domainje CPO

Állítás

Ha P és Q CPO-k, akkor $[P \to Q]$ is az.

Bizonyítás, tovább

Még látnunk kell, hogy $\bigvee F$ folytonos. Legyen $X \subseteq P$ nemüres, lineárisan rendezett halmaz és $x^* = \bigvee X$ a szuprémuma. Akkor

$$\begin{aligned}
(\bigvee F)(x^*) &= \bigvee_{f \in F} f(x^*) \\
&= \bigvee_{f \in F} \bigvee_{x \in X} f(x) \\
&= \bigvee_{x \in X} \bigvee_{f \in F} f(x) \\
&= \bigvee_{x \in X} (\bigvee F)(x).
\end{aligned}$$

A környezetek domainje is CPO

Állítás

Ha P_i, $i \in I$ mind CPOk, akkor $\prod_{i \in I} P_i$ is az.

Bizonyítás

Legyen $U \subseteq \prod_{i \in I} P_i$ lineárisan rendezett. Akkor tetszőleges $i \in I$-re $U(i) = \{u(i) : u \in U\}$ is az, hiszen ha $u \leq v$, akkor $u(i) \leq v(i)$ (mert a szorzat posetben a rendezés pontonkénti).
Tehát minden $i \in I$-re $\bigvee U(i)$ létezik, így a $(\bigvee U)(i) = \bigvee U(i)$ jóldefiniált szuprémuma U-nak.

Konstans, változók

Innentől jelölje Γ az $x_1 : \sigma_1, \ldots, x_n : \sigma_n$ környezetet.

Konstans

Legyen a $\Gamma \vdash 0 : \mathrm{nat}$ term szemantikája a konstans 0 függvény:

$$[[\Gamma \vdash 0 : \mathrm{nat}]](d_1, \ldots, d_n) = 0.$$

Változó

Legyen a $\Gamma \vdash x_i : \sigma_i$ term szemantikája az i. projekció függvény:

$$[[\Gamma \vdash x_i : \sigma_i]](d_1, \ldots, d_n) = d_i.$$

A konstans függvények és a projekciók mindig folytonosak.

[[succ]]

Legyen [[succ]] : [[nat]] $\to$ [[nat]] a következő függvény:

$$[[\text{succ}]](x) = \begin{cases} \bot & \text{ha } x = \bot \\ x+1 & \text{egyébként.} \end{cases}$$

[[nat]] $\to$ [[nat]] függvények folytonossága

Egy f : [[nat]] $\to$ [[nat]] függvény mikor folytonos?

- Ha minden nemüres lineárisan rendezett $X \subseteq \mathbb{N}_\bot$-ra $f(\bigvee X) = \bigvee_{x \in X} f(x)$.
- A feltétel automatikusan teljesül az üres és az egyelemű X-ekre.
- Tehát csak a kételemű, $\{\bot, x\}$ alakú halmazokat kell vizsgálni. Ezeknek szuprémuma x.
- A feltétel: $f(x) = f(\bot) \vee f(x)$, azaz hogy $f(\bot) \leq f(x)$.

Ez [[succ]]ra igaz, tehát folytonos.

$[\![\text{pred}]\!]$

Legyen $[\![\text{pred}]\!] : [\![\text{nat}]\!] \to [\![\text{nat}]\!]$ a következő függvény:

$$[\![\text{pred}]\!](x) = \begin{cases} \perp & \text{ha } x = \perp \\ 0 & \text{ha } x = 0 \\ x - 1 & \text{egyébként.} \end{cases}$$

Ez a $[\![\text{pred}]\!]$ függvény is folytonos, hiszen $\perp$ képe $\perp$.

Ha a termünk $\Gamma \vdash \text{succ}(M) : \text{nat}$ ill. $\Gamma \vdash \text{pred}(M) : \text{nat}$ alakú, akkor szemantikája M szemantikája plusz ill. mínusz egy:

$$[\![\Gamma \vdash \text{succ}(M) : \text{nat}]\!](\vec{d}) = [\![\text{succ}]\!]\Big([\![\Gamma \vdash M : \text{nat}]\!](\vec{d})\Big)$$

$$[\![\Gamma \vdash \text{pred}(M) : \text{nat}]\!](\vec{d}) = [\![\text{pred}]\!]\Big([\![\Gamma \vdash M : \text{nat}]\!](\vec{d})\Big)$$

Vagyis $[\![\Gamma \vdash \text{succ}(M) : \text{nat}]\!] = [\![\text{succ}]\!] \circ [\![\Gamma \vdash M : \text{nat}]\!]$. Folytonosak.

[[ifzero]]

Legyen $[[\text{ifzero}]] : [[\text{nat}]]^3 \to [[\text{nat}]]$ a következő függvény:

$$[[\text{ifzero}]](x, y, z) = \begin{cases} \bot & \text{ha } x = \bot, \\ y & \text{ha } x = 0, \\ z & \text{egyébként.} \end{cases}$$

Ha a termünk $\Gamma \vdash \text{ifzero}(M_1, M_2, M_3) : \text{nat}$ alakú, akkor szemantikája: kiszámoljuk az M_i-ket, erre a három értékre alkalmazzuk az ifzero függvényt:

$$[[\Gamma \vdash \text{ifzero}(M_1, M_2, M_3) : \text{nat}]](\vec{d}) = [[\text{ifzero}]](v_1, v_2, v_3),$$

ahol $v_i = [[\Gamma \vdash M_i : \text{nat}]](\vec{d})$. Így is írhatjuk:

$$\begin{aligned} & [[\Gamma \vdash \text{ifzero}(M_1, M_2, M_3) : \text{nat}]] \\ = \; & [[\text{ifzero}]] \circ \left\langle [[\Gamma \vdash M_1 : \text{nat}]], [[\Gamma \vdash M_2 : \text{nat}]], [[\Gamma \vdash M_3 : \text{nat}]] \right\rangle \end{aligned}$$

[[ifzero]] folytonos

Ahhoz, hogy belássuk, hogy [[ifzero]] is folytonos, ezzel kezdjük:

Definíció

Legyen $f : P_1 \times \ldots \times P_n \to Q$ függvény, P_i és Q CPO-k.
Azt mondjuk, hogy f az i. koordinátán folytonos, $i = 1, \ldots, n$, ha minden $p_1 \in P_1, \ldots, p_{i-1} \in P_{i-1}, p_{i+1} \in P_{i+1}, \ldots, p_n \in P_n$ rögzített értékekre és $X_i \subseteq P_i$ nemüres, lineárisan rendezett halmazra igaz, hogy

$$f(p_1, \ldots, p_{i-1}, \bigvee X_i, p_{i+1}, \ldots, p_n) = \bigvee_{x \in X_i} f(p_1, \ldots, p_{i-1}, x, p_{i+1}, \ldots, p_n).$$

Állítás

A fenti f pontosan akkor folytonos, ha minden $1 \leq i \leq n$ koordinátán folytonos.

Miért lesz ez jó

Ha ez igaz, akkor $f = [[\text{ifzero}]]$ folytonos, mert:

- Az első koordinátán folytonos, ha $f(\perp, y, z) \leq f(x, y, z)$ – azaz $\perp \leq f(x, y, z)$, ami igaz;
- A másodikon folytonos, ha $f(x, \perp, z) \leq f(x, y, z)$ – azaz
  - ha $x = \perp$: $\perp \leq \perp$ – igaz
  - ha $x = 0$: $\perp \leq y$ – igaz
  - ha $x > 0$: $z \leq z$ – igaz
- A harmadikon folytonos, ha $f(x, y, \perp) \leq f(x, y, z)$ – azaz
  - ha $x = \perp$: $\perp \leq \perp$ – igaz
  - ha $x = 0$: $y \leq y$ – igaz
  - ha $x > 0$: $\perp \leq z$ – igaz

Tehát $[[\text{ifzero}]]$ minden koordinátáján folytonos, tehát folytonos.

Bizonyítás

Legyen $f : P_1 \times \ldots \times P_n \to Q$ minden koordinátáján folytonos és $U \subseteq P_1 \times \ldots \times P_n$ lineárisan rendezett, nemüres részhalmaz, és mondjuk írjuk az $u \in U$ elemeket $u = (x_1^u, x_2^u, \ldots, x_n^u)$ alakban.

- Legyen $X_i = \{x_i^u : u \in U\}$ az i. koordinátán előforduló elemek halmaza.
- Tudjuk, hogy X_i lineárisan rendezett (mert ha $u \leq v$, akkor $x_i^u \leq x_i^v$), tehát van szuprémuma (mivel P_i CPO) és

$$\bigvee U = \Big(\bigvee_{u_1 \in U} x_1^{u_1}, \bigvee_{u_2 \in U} x_2^{u_2}, \ldots, \bigvee_{u_n \in U} x_n^{u_n} \Big).$$

Bizonyítás

- A koordinátánkénti folytonosságot alkalmazva n-szer:

$$\begin{aligned}
f(\bigvee U) &= f\Big(\bigvee_{u_1\in U} x_1^{u_1}, \bigvee_{u_2\in U} x_2^{u_2}, \ldots, \bigvee_{u_n\in U} x_n^{u_n}\Big)\\
&= \bigvee_{u_1\in U} f\Big(x_1^{u_1}, \bigvee_{u_2\in U} x_2^{u_2}, \ldots, \bigvee_{u_n\in U} x_n^{u_n}\Big)\\
&= \bigvee_{u_1\in U}\bigvee_{u_2\in U} f\Big(x_1^{u_1}, x_2^{u_2}, \ldots, \bigvee_{u_n\in U} x_n^{u_n}\Big)\\
&= \ldots\\
&= \bigvee_{u_1\in U}\bigvee_{u_2\in U}\ldots\bigvee_{u_n\in U} f\Big(x_1^{u_1}, x_2^{u_2}, \ldots, x_n^{u_n}\Big)\\
&= \bigvee_{u_1,\ldots,u_n\in U} f\Big(x_1^{u_1}, x_2^{u_2}, \ldots, x_n^{u_n}\Big).
\end{aligned}$$

- Erről kellene látnunk, hogy ugyanaz, mint $\bigvee_{u\in U} f\Big(x_1^u, x_2^u, \ldots, x_n^u\Big)$.

Bizonyítás

- Elég belátnunk, hogy minden $(x_1^{u_1}, x_2^{u_2}, \ldots, x_n^{u_n})$ alakú vektornak van $(x_1^u, x_2^u, \ldots, x_n^u)$ alakú felső korlátja.
- Mivel U lineárisan rendezett volt, a véges $\{u_1, \ldots, u_n\}$ részhalmazának van legnagyobb eleme. Legyen ez u.
- Ekkor $x_i^{u_j} \leq x_i^u$ minden i, j-re.
- Tehát $(x_1^{u_1}, \ldots, x_n^{u_n}) \leq (x_1^u, \ldots, x_n^u)$.
- A koordinátánkénti monotonitást alkalmazva pedig $f(x_1^{u_1}, \ldots, x_n^{u_n}) \leq f(x_1^u, \ldots, x_n^u)$.

Eval, alkalmazás

eval

Legyen eval : $([P \times Q] \times P) \to Q$ az $\text{eval}(f, x) = f(x)$ függvény.

Állítás

Az eval függvény folytonos.

Bizonyítás

Koordinátánként:

- Ha $f \in [P \to Q]$ és $X \subseteq P$ lánc, akkor $\text{eval}(f, \vee X) = f(\vee X) = \vee f(x) = \vee \text{eval}(f, x)$.
- Ha $F \subseteq [P \to Q]$ lánc és $x \in P$, akkor $\text{eval}(\vee F, x) = (\vee F)(x) = \vee f(x) = \vee \text{eval}(f, x)$.

$$[[\Gamma \vdash M(N) : \tau]] := \text{eval} \circ \langle [[\Gamma \vdash M : \sigma \to \tau]], [[\Gamma \vdash N : \sigma]] \rangle$$

Curry, λ-absztrakció

Legyen curry : $[(P \times Q) \to R] \to (P \to (Q \to R))$ az a függvény, melyre

$$\mathrm{curry}(f)(p)(q) \;=\; f(p,q).$$

Állítás

curry(f) egy $[P \to [Q \to R]]$ függvény.

Bizonyítás

- Ha $Y \subseteq Q$ lánc, akkor
  $\mathrm{curry}(f)(p)(\vee Y) = f(p, \vee Y) = \vee f(p,y) = \vee \mathrm{curry}(f)(p)(y)$.
- Ha $X \subseteq P$ lánc, akkor $\mathrm{curry}(f)(\vee X) = \vee \mathrm{curry}(f)(x)$, mert minden $y \in Q$-ra
  $\mathrm{curry}(f)(\vee X)(y) = f(\vee X, y) = \vee f(x,y) = \vee \mathrm{curry}(f)(x)(y)$.

$$[[\Gamma \vdash \lambda x : \sigma . M : \sigma \to \tau]] \;:=\; \mathrm{curry}([[\Gamma, x : \sigma \vdash M : \tau]]).$$

lfp

Ha $f : [P \to [Q \to Q]]$ függvény, akkor legyen $\mathrm{lfp}(f)$ az a $P \to Q$ függvény, melyre

$$\mathrm{lfp}(f)(p) \text{ az } f(p) : Q \to Q \text{ folytonos függvény legkisebb fixpontja.}$$

Állítás

Ekkor $\mathrm{lfp}(f)$ egy $[P \to Q]$ függvény.

Bizonyítás

Azt kell belássuk, hogy ha $X \subseteq P$ nemüres lánc, akkor $\mathrm{lfp}(f)(\vee X) = \vee \mathrm{lfp}(f)(x)$.

- Tudjuk, hogy $\mathrm{lfp}(f)(p) = \bigvee_{n \geq 0} (f(p))^n(\perp)$.

Bizonyítás

- Tehát a jobb oldal: $\bigvee_{x\in X}\bigvee_{n\geq 0}(f(x))^n(\perp) = \bigvee_{n\geq 0}\bigvee_{x\in X}(f(x))^n(\perp)$.
- A bal oldal: $\bigvee_{n\geq 0}(f(\vee X)^n)(\perp)$.
- Elég azt belátnunk, hogy minden n-re

$$\bigvee_{x\in X}(f(x))^n(\perp) \;=\; f(\vee X)^n(\perp).$$

- A jobb oldal:

$$\begin{aligned} f(\vee X)^n(\perp) &= f(\vee X)f(\vee X)f(\vee X)\dots f(\vee X)(\perp) \\ &= \bigvee_{x_1\in X}\bigvee_{x_2\in X}\dots\bigvee_{x_n\in X} f(x_1)f(x_2)\dots f(x_n)(\perp). \end{aligned}$$

- Megint elég megmutatnunk, hogy minden $f(x_1)f(x_2)\dots f(x_n)(\perp)$ alakú elemnek van $f(x)^n(\perp)$ alakú felső korlátja.

Bizonyítás

- Mivel X lánc, így $\{x_1, \ldots, x_n\}$ egy véges lánc, van legnagyobb eleme, mondjuk x.
- Monotonitás miatt akkor $f(x_i) \leq f(x)$ minden i-re.
- Ez a pontonkénti rendezés definícióia miatt azt jelenti, hogy $f(x_i)(y) \leq f(x)(y)$ minden i-re és y-ra.
- Mivel az $f(x)$ függvények is monotonok, ez azt is jelenti, hogy $f(x_i)(y) \leq f(x)(y')$ minden i-re és $y \leq y'$-re.
- Akkor:

$$
\begin{aligned}
\perp &\leq \perp \\
f(x_n)(\perp) &\leq f(x)(\perp) \\
f(x_{n-1})f(x_n)(\perp) &\leq f(x)^2(\perp) \\
&\cdots \\
f(x_1)f(x_2)\ldots f(x_n)(\perp) &\leq f(x)^n(\perp)
\end{aligned}
$$

és kész vagyunk.

A rekurzió operátor

$$[\![\Gamma \vdash Y_\sigma(M) : \sigma]\!] = \mathsf{lfp}([\![\Gamma \vdash M : \sigma \to \sigma]\!]).$$

Ekvivalencia

A célunk megmutatni, hogy a műveleti szemantika és a denotációs szemantika megegyezik, tehát azt, hogy

$$[\![\vdash M : \mathsf{nat}]\!] = n \;\Leftrightarrow\; M \Downarrow \underline{n}.$$

Átírás során nem változik $[[\_]]$

Állítás

Ha $M \rhd N$, akkor $[[\Gamma \vdash M : \sigma]] = [[\Gamma \vdash N : \sigma]]$.

Bizonyítás

Az M felépítése szerinti indukcióval.

- Ha $M = 0$, $M = x_i$ vagy $M = \lambda x : \tau.M'$: nem írjuk át, ilyen eset nincs
- Ha $M = \mathsf{f}(M')$, ahol $\mathsf{f} \in \{\mathsf{pred}, \mathsf{succ}\}$ és $M' \rhd N'$, akkor $N = \mathsf{f}(N')$ és

$$\begin{aligned} [[\Gamma \vdash M : \mathsf{nat}]] &= [[\Gamma \vdash \mathsf{f}(M') : \mathsf{nat}]] \\ &= [[\mathsf{f}]] \circ [[\Gamma \vdash M' : \mathsf{nat}]] \\ &= [[\mathsf{f}]] \circ [[\Gamma \vdash N' : \mathsf{nat}]] \\ &= [[\Gamma \vdash \mathsf{f}(N') : \mathsf{nat}]] \\ &= [[\Gamma \vdash N : \mathsf{nat}]]. \end{aligned}$$

Bizonyítás

- Ha $M = \mathrm{pred}(0)$, akkor $N = 0$ és

$$0 = [[\Gamma \vdash 0 : \mathrm{nat}]] = [[\mathrm{pred}]] \circ [[\Gamma \vdash 0 : \mathrm{nat}]] = [[\Gamma \vdash \mathrm{pred}(0)]],$$

  mert $[[\mathrm{pred}]](0) = 0$.
- Ha $M = \mathrm{pred}(\underline{n+1})$, akkor $N = \underline{n}$ és

$$[[\Gamma \vdash \underline{n} : \mathrm{nat}]] = n = [[\mathrm{pred}]](n+1) = [[\Gamma \vdash \mathrm{pred}(\underline{n+1})]].$$

- Ha $M = \mathrm{ifzero}(M_1, M_2, M_3)$ és $M_1 \triangleright M_1'$, akkor $N = \mathrm{ifzero}(M_1', M_2, M_3)$ és

$$\begin{aligned} & [[\Gamma \vdash M : \mathrm{nat}]] \\ = \ & [[\mathrm{ifzero}]] \circ \langle [[\Gamma \vdash M_1 : \mathrm{nat}]], [[\Gamma \vdash M_2 : \mathrm{nat}]], [[\Gamma \vdash M_3 : \mathrm{nat}]] \rangle \\ = \ & [[\mathrm{ifzero}]] \circ \langle [[\Gamma \vdash M_1' : \mathrm{nat}]], [[\Gamma \vdash M_2 : \mathrm{nat}]], [[\Gamma \vdash M_3 : \mathrm{nat}]] \rangle \\ = \ & [[\Gamma \vdash N : \mathrm{nat}]]. \end{aligned}$$

Bizonyítás

- Ha $M = \text{ifzero}(0, M_2, M_3)$, akkor $N = M_2$ és

$$\begin{aligned} & [[\Gamma \vdash M : \text{nat}]] \\ = \quad & [[\text{ifzero}]] \circ \langle 0, [[\Gamma \vdash M_2 : \text{nat}]], [[\Gamma \vdash M_3 : \text{nat}]] \rangle \\ = \quad & [[\Gamma \vdash M_2]], \end{aligned}$$

  mert $[[\text{ifzero}]](0, y, z) = y$.

- Ha $M = \text{ifzero}(\underline{n+1}, M_2, M_3)$, akkor $N = M_3$ és

$$\begin{aligned} & [[\Gamma \vdash M : \text{nat}]] \\ = \quad & [[\text{ifzero}]] \circ \langle n+1, [[\Gamma \vdash M_2 : \text{nat}]], [[\Gamma \vdash M_3 : \text{nat}]] \rangle \\ = \quad & [[\Gamma \vdash M_3]], \end{aligned}$$

  mert $[[\text{ifzero}]](n+1, y, z) = z$.

Bizonyítás

- Ha $M = M_1(M_2)$ és $M_1 \triangleright M_1'$, akkor $N = M_1'(M_2)$ és

$$\begin{aligned} & [[\Gamma \vdash M : \tau]] \\ = \;& \mathrm{eval} \circ \langle [[\Gamma \vdash M_1 : \sigma \to \tau]], [[\Gamma \vdash M_2 : \sigma]] \rangle \\ = \;& \mathrm{eval} \circ \langle [[\Gamma \vdash M_1' : \sigma \to \tau]], [[\Gamma \vdash M_2 : \sigma]] \rangle \\ = \;& [[\Gamma \vdash N : \tau]]. \end{aligned}$$

- Ha $M = Y_\sigma(M')$, akkor $N = M'(Y_\sigma(M'))$. Ekkor tetszőleges $\vec{d} \in [[\Gamma]]$-ra

$$x := [[\Gamma \vdash Y_\sigma(M') : \sigma]](\vec{d})$$

az $f := [[\Gamma \vdash M' : \sigma \to \sigma]](\vec{d})$ függvény legkisebb fixpontja, vagyis:

$$\begin{aligned} & [[\Gamma \vdash Y_\sigma(M') : \sigma]](\vec{d}) \\ = \;& x = f(x) = \\ = \;& \mathrm{eval}([[\Gamma \vdash M' : \sigma \to \sigma]](\vec{d}), [[\Gamma \vdash Y_\sigma(M') : \sigma]](\vec{d})) \\ = \;& [[\Gamma \vdash M'(Y_\sigma(M')) : \sigma]](\vec{d}). \end{aligned}$$

Bizonyítás

Az utolsó eset:

- Ha $M = (\lambda x : \sigma M')(N')$, akkor $N = M'[x/N']$

bizonyítását átugorjuk.

Egyébként ennek a lemmának a következménye:

$$[[\Gamma \vdash M : \sigma]] \circ \left\langle [[\Delta \vdash N_1 : \sigma_1]], \ldots, [[\Delta \vdash N_n : \sigma_n]] \right\rangle = [[\Delta \vdash M[\vec{x}/\vec{N}] : \sigma]].$$

Melyet szintén M felépítése szerinti indukcióval bizonyíthatunk be.

Tehát ha $M \Downarrow \underline{n}$, akkor $[[\Gamma \vdash M : \mathrm{nat}]] = [[\Gamma \vdash \underline{n} : \mathrm{nat}]] = n$.

A másik irány

Cél:

Ha $[\![\vdash M : \mathrm{nat}]\!] = n$, akkor $M \Downarrow \underline{n}$.

Egy $\leq$ reláció

Definiálunk típus szerinti rekurzióval egy $\leq$ relációt $[\![\sigma]\!]$ és a $\vdash M : \sigma$ termek közt.

- Ha $\sigma = \mathrm{nat}$, akkor
  - $\bot \;\leq\; \vdash M : \mathrm{nat}$ mindig;
  - $n \;\leq\; \vdash M : \mathrm{nat}$, ha $M \Downarrow \underline{n}$.
- Ha $\sigma = \sigma_1 \to \sigma_2$, akkor $f \;\leq\; \vdash M : \sigma$ pont akkor álljon fenn, ha minden $x \;\leq\; \vdash N : \sigma_1$ esetén $f(x) \;\leq\; \vdash M(N) : \sigma_2$.

Ha $f : [\![\Gamma]\!] \to [\![\sigma]\!]$ és $\Gamma \vdash M : \sigma$, akkor pedig legyen $f \;\leq\; \Gamma \vdash M : \sigma$, ha minden $d_i \;\leq\; \vdash N_i : \sigma_i$ esetben
$f(d_1, \ldots, d_n) \;\leq\; \vdash M[x_1/N_1, \ldots, x_n/N_n]$.

A másik irány

Cél:

$$[[\Gamma \vdash M : \sigma]] \;\leq\; \Gamma \vdash M : \sigma.$$

Amiért ez elég

Akkor $[[\vdash M : \text{nat}]] \;\leq\; \vdash M : \text{nat}$ miatt ha $[[\vdash M : \text{nat}]] = n$, akkor $M \Downarrow \underline{n}$ tényleg fenn kell álljon.

Ezt is M felépítése szerinti indukcióval lehet igazolni, itt a rekurzió operátor kezelése a bonyolult.

Bizonyítás

Belátjuk, hogy $[[\Gamma \vdash M : \sigma]](\vec{d}) \;\leq\; M[\vec{x}/\vec{N}]$, ha minden i-re $d_i \leq N_i$.

- $[[\Gamma \vdash 0 : \mathrm{nat}]](\vec{d}) = 0$, $0[\vec{x}/\vec{N}] = 0$ és $0 \Downarrow 0$, ez így OK.
- $[[\Gamma \vdash \mathrm{succ}(M) : \mathrm{nat}]](\vec{d}) = [[\mathrm{succ}]]([[\Gamma \vdash M : \mathrm{nat}]](\vec{d}))$.
  - Ha $[[\Gamma \vdash M : \mathrm{nat}]](\vec{d}) = \bot$, akkor $[[\mathrm{succ}]](\bot) = \bot$ miatt az eredmény is $\bot$, ami OK, mert $\bot \;\leq\; \Gamma \vdash \mathrm{succ}(M) : \mathrm{nat}$.
  - Ha $[[\Gamma \vdash M : \mathrm{nat}]](\vec{d}) = n \in \mathbb{N}$, akkor az indukciós feltevés miatt $M[\vec{x}/\vec{N}] \Downarrow \underline{n}$. Ekkor pedig $[[\Gamma \vdash \mathrm{succ}(M) : \mathrm{nat}]](\vec{d}) = n+1$ és $\mathrm{succ}(M)[\vec{x}/\vec{N}] \Downarrow \underline{n+1}$, OK.
- $[[\Gamma \vdash \mathrm{pred}(M) : \mathrm{nat}]](\vec{d}) = [[\mathrm{pred}]]([[\Gamma \vdash M : \mathrm{nat}]](\vec{d}))$.
  - Ha a belső eredmény $\bot$, akkor a külső is, ami OK.
  - Ha a belső eredmény 0, akkor a külső is. Másrészt akkor az indukciós feltevés szerint $M[\vec{x}/\vec{N}] \Downarrow 0$, tehát $\mathrm{pred}(M)[\vec{x}/\vec{N}] \triangleright^* \mathrm{pred}(0) \triangleright 0$.
  - Ha a belső eredmény $n+1$, akkor a külső n. Ekkor pedig az indukciós feltevés szerint $M[\vec{x}/\vec{N}] \Downarrow \underline{n+1}$ és ekkor $\mathrm{pred}(M)[\vec{x}/\vec{N}] \Downarrow \underline{n}$.

Bizonyítás

- $[[\Gamma \vdash x_i : \sigma_i]](\vec{d}) = d_i$ és $x_i[\vec{x}/\vec{N}] = N_i$, és abból indultunk ki, hogy $d_i \leq N_i$ minden i-re, OK.
- Az $[[\Gamma \vdash M(K) : \sigma]](\vec{d})$ eset:
  - Indukció szerint $[[\Gamma \vdash K : \tau]](\vec{d}) \ \leq \ K[\vec{x}/\vec{N}]$.
  - Továbbá, $[[\Gamma \vdash M : \tau \to \sigma]](\vec{d}) \ \leq \ M[\vec{x}/\vec{N}]$.
  - Ez utóbbi mivel $\tau \to \sigma$ függvény típus, azt jelenti, hogy minden d értékre és $\vdash T : \tau$ termre $[[\Gamma \vdash M : \tau \to \sigma]](\vec{d})(d) \leq M[\vec{x}/\vec{N}](T)$.
  - Speciálisan $d = [[\Gamma \vdash K : \tau]](\vec{d})$, $T = K[\vec{x}/\vec{N}]$-re:

$$\begin{array}{cl} & [[\Gamma \vdash M(K) : \sigma]](\vec{d}) \\ = & [[\Gamma \vdash M : \tau \to \sigma]](\vec{d})([[\Gamma \vdash K : \tau]](\vec{d})) \\ \leq & M[\vec{x}/\vec{N}](K[\vec{x}/\vec{N}]) \\ = & M(K)[\vec{x}/\vec{N}]. \end{array}$$

Bizonyítás

- Az $[[\Gamma \vdash \lambda x : \sigma.M : \sigma \to \tau]](\vec{d})$ eset:
  - Indukció szerint $[[\Gamma, x : \sigma \vdash M : \tau]] \ \leq \ \Gamma \vdash M : \tau$.
  - Mivel $\sigma \to \tau$ függvény típus, a $\leq$ reláció akkor áll fenn, ha minden $d \ \leq \ \ \vdash K : \sigma$-ra

$$[[\Gamma \vdash \lambda x : \sigma.M : \sigma \to \tau]](\vec{d})(d) \leq (\lambda x : \sigma.M)[\vec{x}/\vec{N}](K).$$

  - Azaz a curry definíciója szerint ha

$$[[\Gamma, x : \sigma \vdash M : \tau]](\vec{d}, d) \leq (\lambda x : \sigma.M)[\vec{x}/\vec{N}](K).$$

  - Tudjuk, hogy $(\lambda x : \sigma.M)[\vec{x}/\vec{N}](K) \triangleright M[\vec{x}/\vec{N}, x/K]$ és hogy indukció szerint

$$[[\Gamma, x : \sigma \vdash M : \tau]](\vec{d}, d) \leq M[\vec{x}/\vec{N}, x/K].$$

A következő lemma hasznos lesz ennek az esetnek (és a rekurzióénak) a befejezéséhez.

Lemma

Ha $f \leq \Gamma \vdash K : \sigma$ és $M \triangleright K$, akkor $f \leq \Gamma \vdash M : \sigma$.

Bizonyítás

A σ felépítése szerinti indukciót alkalmazunk. Legyen $\vec{d} \leq \vec{N}$.

- Ha $\sigma = \mathrm{nat}$:
  - Ha $f(\vec{d}) = \perp$, akkor OK, mert $\perp$ relációban áll minden termmel.
  - Ha $f(\vec{d}) = n \in \mathbb{N}$, akkor $f \leq \Gamma \vdash K : \mathrm{nat}$ miatt $K[\vec{x}/\vec{N}] \Downarrow \underline{n}$, tehát $M \triangleright K$ miatt $M[\vec{x}/\vec{N}] \Downarrow \underline{n}$ is igaz.
- Ha $\sigma = \tau_1 \to \tau_2$, akkor legyen $d \leq \Gamma \vdash N : \tau_1$.
  - Be kell látnunk, hogy $f(\vec{d})(d) \leq M[\vec{x}/\vec{N}](N)$.
  - De ekkor $M[\vec{x}/\vec{N}](N) \triangleright K[\vec{x}/\vec{N}](N)$.
  - Indukció szerint tehát valóban, $f(\vec{d})(d) \leq M[\vec{x}/\vec{N}](N)$.

Bizonyítás

- Az utolsó eset: $[[\Gamma \vdash Y_\sigma.M : \sigma]](\vec{d})$.
- Ekkor $x = [[\Gamma \vdash Y_\sigma.M : \sigma]](\vec{d})$ az $f = [[\Gamma \vdash M : \sigma \to \sigma]](\vec{d})$ függvény legkisebb fixpontja.
- Tehát $x = \bigvee_{n\geq 0} f^n(\perp)$.
- Ha $d \ \leq \ \Gamma \vdash Y_\sigma.M : \sigma$, akkor $f(d)$ is, mert:
  - Indukció szerint $f \ \leq \ \Gamma \vdash M[\vec{x}/\vec{N}] : \sigma \to \sigma$
  - Mivel $\sigma \to \sigma$ függvény típus, alkalmazhatjuk $d \ \leq \ \Gamma \vdash Y_\sigma.M : \sigma$-t és kapjuk:

    $$f(d) \ \leq \ \Gamma \vdash M[\vec{x}/\vec{N}](Y_\sigma.M[\vec{x}/\vec{N}]) \ = \ M(Y_\sigma.M)[\vec{x}/\vec{N}]$$

  - Mivel pedig $Y_\sigma.M \triangleright M(Y_\sigma.M)$, az előző lemmából

    $$f(d) \ \leq \ \Gamma \vdash (Y_\sigma.M)[\vec{x}/\vec{N}].$$

Ha belátjuk, hogy $\perp \ \leq \ \Gamma \vdash M : \sigma$ és ha $D \ \leq \ \Gamma \vdash M : \sigma$ a D nemüres láncra, akkor $\vee D \ \leq \ \Gamma \vdash M : \sigma$ is igaz, kész vagyunk.

Lemma

$$\perp \;\leq\; \Gamma \vdash M : \sigma.$$

Bizonyítás

A σ típus felépítése szerinti indukciót alkalmazunk.

- $\sigma = \text{nat}$: a $\leq$ definíciója szerint így van.
- $\sigma = \tau_1 \to \tau_2$: Ennek a típusnak a $\perp_\sigma$ legkisebb eleme az a függvény, melyre $\perp_\sigma(x) = \perp_{\tau_2}$ minden $x \in [[\tau_1]]$-re.
  Indukció szerint tehát $\perp_\sigma(x) \leq \Gamma \vdash M(N)$ minden $\vdash N : \tau_1$ termre.
  Tehát $\perp_\sigma \;\leq\; \Gamma \vdash M$.

Lemma

Ha $D \subseteq [[\sigma]]$ nemüres lánc, és minden $d \in D$-re $d \ \leq \ \Gamma \vdash M : \sigma$, akkor $\vee D \ \leq \ \Gamma \vdash M : \sigma$.

Bizonyítás

A σ típus felépítése szerinti indukciót alkalmazunk.

- $\sigma =$ nat: $(\vee D)(\vec{d}) = \vee_{d \in D} d(\vec{d})$ egy véges lánc szuprémuma, tehát az egyik eleme, melyre az állítás a feltevés szerint teljesül.
- $\sigma = \tau_1 \rightarrow \tau_2$: legyen $x \ \leq \ \vdash K : \tau_1$. Akkor

  $$(\vee D)(\vec{d})(x) = \vee_{d \in D}(d(\vec{d})(x)),$$

  ami egy véges lánc szuprémuma $[[\tau_2]]$-ben. Indukció szerint tehát

  $$\vee_{d \in D}(d(\vec{d})(x)) \ \leq \ \Gamma \vdash M[\vec{x}/\vec{N}](K),$$

  tehát $\vee D \ \leq \ \Gamma \vdash M : \sigma$.

Ezzel a két szemantika ekvivalenciájának mindkét irányát befejeztük.