... vannak a tárgyban dolgok az ítéletkalkulusról, és aztán...

Az elsőrendű logika szintaxisa és szemantikája

Ítéletkalkulusban csak bitekről (igazságértékekről) beszéltünk, a változók igazságértékeket vehettek fel értékül (és csak kettőt: 0 vagy 1), ezeket lehetett összekötni a logikai konnektívákkal ($\wedge$, $\vee$, $\neg$, $\leftrightarrow$, $\rightarrow$).

Ezzel szemben elsőrendű logikában vagy **predikátumkalkulusban** (ezek szinonimák) a változók **objektumok egy halmazából**, úgy is mondják, hogy egy **univerzumból** veszik fel értékeiket, lesznek **függvények**, amik objektumokból objektumot képeznek (ilyen pl. az egész számok közt az összeadás, a szorzás, stb) és **predikátumok**, amik objektumokból igazságértéket készítenek (ilyen pl. hogy egy szám prímszám-e, páratlan-e, kisebb-e egy másik számnál stb).

Megint, mint ahogy ítéletkalkulusban is, a **szintaxis** azt adja meg, hogy mitől formula egy formula, „hogy nézhet ki”, a **szemantika** pedig azt, hogy hogy értékelünk ki egy formulát, „mit jelent”. Mindig a szintaxissal kezdjük, legelőször is a használható alapelemekkel, amiket felhasználhatunk a formulák felépítésekor:

Szintaxis

- (elsőrendű) **változókat**, ezeknek a jele általában az $x, y, z, \ldots$ környékéről lesz az ábécének; feltesszük, hogy a változókból használhatunk (megszámlálhatóan[1]) végtelen sokat.

  Ha majd szemantikával látjuk el a formulánkat, a változók valami objektumot fognak felvenni értékül.

- **függvényjeleket**, ezeknek a jele általában $f, g, h, \ldots$ lesz; ezekből is csak megszámlálható sok lehet[2], és mindnek van egy fix **aritása** avagy változószáma, ami egy ≥ 0 egész szám. Hogy az f egy n-változós függvényjel, annak jele f/n.

  Ha majd szemantikával látjuk el a formulákat, egy függvény**jel** jelentése valami objektumból objektumot képző függvény lesz, pl. az $f/2$ lehet az összeadás, $g/2$ a szorzás, $h/1$ az ellentett függvény, ahogy tetszik.

- **predikátumjeleket**, ezeknek a jele általában $p, q, r, \ldots$ lesz, szintén megszámlálhatóan sokan vannak, aritással, szintén p/n jelöli, hogy a p az egy n-változós predikátumjel.

  Ha majd szemantikával látjuk el a formulákat, egy predikátum**jel** jelentése valami objektumból igazságértéket képző leképezés lesz, ezt hívják **predikátum**nak, vagy **reláció**nak, mint pl. $p/2$ lehet a „kisebb” reláció, $q/1$ a „páratlan” predikátum stb.

- Használjuk még a szokásos logikai **konnektívák**at: $\wedge$, $\vee$, $\neg$, $\rightarrow$, $\leftrightarrow$, **kvantor**okat: $\forall$, $\exists$, **logikai konstans**okat: $\uparrow$, $\downarrow$ és zárójeleket, vesszőket szeparátornak.

[1] ez annyit jelent, hogy lesz az első, a második, stb. változó, fel tudjuk sorolni mindet 1-től indexelve, van, aki ahhoz ragaszkodik, hogy a változók halmaza $x_1, x_2, x_3, \ldots$ – mi az olvashatóság kedvéért használunk y-t, z-t stb. is

[2] vagyis vagy véges sok, vagy megszámlálhatóan végtelen

Az eddigiekből érezhető, hogy kétféle **szintaktikus kategória** van: lesznek dolgok, amik valami objektummá értékelődnek ki (ezek lesznek a **term**ek, avagy „kifejezés”ek), és dolgok, amik igazságértékké (ezek pedig a **formulák**, duh).

A termeket úgy építjük, hogy kiindulunk a változókból, és alkalmazhatjuk rajtuk a függvényjeleket ízlés szerint, figyelve a változószámra. Vagyis:

Definíció: Term

- minden változó term;
- ha f/n egy n-változós függvényjel és $t_1, \ldots, t_n$ már termek, akkor $f(t_1, \ldots, t_n)$ is term;
- más term nincs.

Tehát pl. ha x, y változók, $f/1$ és $g/2$ függvényjelek, akkor x term, y is term, ezekből g-vel felépíthetjük a $g(x, y)$-t, az is term, ezen alkalmazhatjuk f-et, $f(g(x, y))$, ez is term. Ha $c/0$ egy 0-változós függvényjel, amit **konstans**nak is hívunk, akkor pl. $c()$ is term: c-be helyettesítünk nulla darab argumentumot, és így pl. $g(c(), c())$ is term. Az üres nyitó-csukójeleket a könnyebb olvashatóság érdekében elhagyjuk, és ilyenkor csak $g(c, c)$-t írunk, ez is term.

Ebben a példa $g(c, c)$-ben nincs változó. Az ilyen termeket **alapterm**nek, vagy „ground term”nek hívjuk. A fenti jelkészletben pl. alaptermek c, $f(c)$, $f(f(c))$, $g(c, c)$, $g(c, f(c))$ stb.

Formulákat úgy kapunk, hogy termeken alkalmazunk **predikátum**jeleket, aztán ezeket összekötjük ízlés szerint logikai konnektívákkal:

Definíció: Formula

- Ha p/n predikátumjel és $t_1, \ldots, t_n$ termek, akkor $p(t_1, \ldots, t_n)$ egy **atomi formula**.
- $\uparrow$ és $\downarrow$ is formulák.
- Ha F formula, akkor $(\neg F)$ is formula.
- Ha F, G formulák, akkor $(F \vee G)$, $(F \wedge G)$, $(F \rightarrow G)$, $(F \leftrightarrow G)$ is formulák.
- Ha F formula és x változó, akkor $(\exists x F)$ és $(\forall x F)$ is formulák.
- Más formula nincs.

Nézzünk egy példát: ha $p/1$ és $q/2$ predikátumjelek és $f/1$ függvényjel, akkor

$$\exists x\Big(p(x) \wedge \forall y q(f(x), y)\Big)$$

egy formula, mert x változó, tehát akkor x **egy term**, akkor $p(x)$ **egy atomi formula**, mert az x termet helyettesítjük be a p egyváltozós predikátumjelbe, $f(x)$ **egy term**, mert az x termet helyettesítjük be az $f/1$ függvényjelbe, akkor $q(f(x), y)$ **formula**, mert az $f(x)$ és y termeket helyettesítjük a $q/2$ predikátumjele, ez elé $\forall y$-t rakva formulát kapunk, aztán ezt a $p(x)$ formulával összeéselve formulát, végül elérakva a $\exists x$-et szintén egy formulát.

Szemantika

Ítéletkalkulusban egy változó-értékadás kellett ahhoz, hogy kiértékeljünk egy formulát. Elsőrendű logikában egy **struktúra** kell hozzá, kicsit több mindent kell megadnunk. Konkrétan:

egy struktúra **három** dologból áll össze:

- Meg kell adjuk az **univerzumot**, az objektumok halmazát. Ez egy nemüres halmaz, általában A jelöli.
- Meg kell adjuk ezek után az összes függvény- és predikátum**jel**re annak a jelentését vagy **interpretációját**. Ezt az interpretációs függvényt általában I jelöli.
- Végül, minden változónak meg kell adjuk a „default” értékét. Ezt pedig általában φ jelöli.

Kicsit formálisabban:

Definíció: Struktúra

(Elsőrendű) struktúra egy $\mathcal{A} = (A, I, \varphi)$ hármas, ahol:

- A az objektumok nemüres halmaza;
- I az interpretációs függvény, ami minden p/n predikátumjelhez hozzárendel egy $I(p) : A^n \to \{0, 1\}$ predikátumot és minden f/n függvényjelhez egy $I(f) : A^n \to A$ függvényt;
- φ pedig minden x változóhoz egy $\varphi(x) \in A$ objektumot rendel.

Tehát például ha $f/2$ egy függvényjel és $p/2$ egy predikátumjel, akkor egy struktúra lehet az az (A, I, φ) vektor, ahol

- $A = \{0, 1, 2, \ldots\}$ a természetes számok,
- $I(f)(n, m) := n + m$, az összeadás,
- $I(p)(n, m)$ akor igaz, ha $n < m$;
- $\varphi(x) = 3, \varphi(y) = 1, \varphi(z) = 42, \ldots$

Annyi megszorítás van, hogy ha van $=$ jelünk, akkor az egy **bináris predikátumjel** kell legyen, és minden struktúrában tényleg az **egyenlőség**et kell jelentse, vagyis $I(=)(a, b)$ pontosan akkor kell igaz legyen, ha $a = b$.

Egy struktúrában minden termnek és formulának van egy **értéke**: a termek objektumot vesznek fel értékül, a formulák pedig igazságértéket, „értelemszerűen”. A t term értéke az $\mathcal{A}$ struktúrában $\mathcal{A}(t)$ lesz, az F formuláé pedig $\mathcal{A}(F)$.

A termekkel kezdjük, mert azok vannak mindig belül: a változók értékét a φ mondja meg, ha meg van egy $f(t_1, \ldots, t_n)$ alakú függvénytermünk, akkor rekurzívan ki kell értékeljük az argumentumokat, azok mind objektumba kiértékelődnek, és ezeken az objektumokon kell kiszámolnunk az f függvény értékét.

Például az előző struktúrában $f(x, f(x, y))$ értéke $3 + (3 + 1) = 7$ lesz.

Formálisabban:

Definíció: Term kiértékelése

A t term értéke az $\mathcal{A} = (A, I, \varphi)$ struktúrában a következő $\mathcal{A}(t)$ objektum lesz:

- ha $t = x$ változó, akkor $\mathcal{A}(t) := \varphi(x)$,

- ha pedig $t = f(t_1, \ldots, t_n)$ függvényterm, akkor $\mathcal{A}(t) := I(f)(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_n))$.

Ez a második sor tényleg csak annyit mond, hogy „ha a t függvénytermet ki akarod értékelni, akkor előbb értékeld ki az argumentumokat rekurzívan, aztán az eredmények vektorán alkalmazd azt a függvényt, amit f épp ebben a struktúrában jelent”.

A formula kiértékelése kicsit összetettebb a kvantorok miatt. Egy $\exists x$ vagy $\forall x$ kvantor[3] hatását tekintve olyan, mint egy lokálisan deklarált változó: „felülírja” x értékét a belsejében. Ehhez a „felülíráshoz” először is el kell jelöljük az **értékadás** műveletét valahogy:

Definíció: (Szemantikai) értékadás

Ha $\mathcal{A} = (A, I, \varphi)$ egy struktúra, x egy változó és $a \in A$ egy objektum, akkor

$$\mathcal{A}_{[x \mapsto a]}$$

jelöli azt a struktúrát, amit úgy kapunk $\mathcal{A}$-ból, hogy benne x default értékét a-ra állítjuk, vagyis: (A, I, φ') (tehát az univerzum és az interpretációs függvény ugyanaz marad), ahol $\varphi'(x) = a$ és $\varphi'(y) = \varphi(y)$ minden $y \neq x$-re (tehát x értéke a, minden másé ugyanaz, mint volt).

Tehát pl. az előző esetben $\mathcal{A}_{[z \mapsto 7]}$ az a struktúra, ahol az univerzum továbbra is a természetes számok, van összeadás meg rendezés, x alapértéke 3, y-é 1, de z-é már nem 42, hanem 7.

Ezeket a struktúrákat a kvantorok kiértékelésekor fogjuk használni. Nézzük akkor most, hogy egy F formulát az $\mathcal{A} = (A, I, \varphi)$ struktúrában hogy értékelünk ki, az egyszerű esetektől a bonyolultabbakig:

Definíció: Formula kiértékelése

Az F formula értékét az $\mathcal{A} = (A, I, \varphi)$ struktúrában $\mathcal{A}(F)$-fel jelöljük, értéke vagy 0, vagy 1 és a következőképp definiáljuk:

- Ha $F = \uparrow$, akkor $\mathcal{A}(F) := 1$. Tehát $\uparrow$ mindig igaz.
- Ha $F = \downarrow$, akkor $\mathcal{A}(F) := 0$. Tehát $\downarrow$ az azonosan hamis formula.
- Ha $F = p(t_1, \ldots, t_n)$ atomi formula, akkor

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

  Magyarul: ha egy atomi formulát (azaz: predikátumjel, benne termek) kell kiértékeljünk, akkor előbb értékeljük ki a termeket, azt már tudjuk, hogy kell, aztán ezen a kapott objektum-vektoron alkalmazzuk azt a predikátumot, amit ebben a struktúrában jelölünk a p-vel. Ez egy bit lesz.

  Például a természetes számos példastruktúránkban $p(x, f(y, y))$ értéke: $\mathcal{A}(x) = 3$, mert ezt mondta a φ, $\mathcal{A}(y) = 1$, mert ezt mondta a φ, $\mathcal{A}(f(y, y)) = I(f)(1, 1)$, tehát $1 + 1 = 2$, mert $I(f)$ az összeadás, és akkor $\mathcal{A}(p(x, f(y, y))) = I(p)(3, 2)$, tehát „$3 < 2$”, ami hamis: az érték 0.
- Ha $F = (G \vee H)$, akkor $\mathcal{A}(F) := \mathcal{A}(G) \vee \mathcal{A}(H)$, és a többi konnektívára hasonlóan: vagyis ha van egy konnektívánk, akkor előbb kiértékeljük a részformulákat (azt az

[3] ha nem érdekel, hogy $\forall$ vagy $\exists$, akkor sokszor írunk Qx-et, a Q a „Qmindegy, melyik kvantor”

egyet, ha a negálásról beszélünk, vagy azt a kettőt a többi esetben) és az eredményen alkalmazzuk a megfelelő konnektívát.

- A kvantorok: ha $F = \exists x G$, akkor

$$\mathcal{A}(F) := \begin{cases} 1 & \text{ha van olyan } a \in A \text{ objektum, amire } \mathcal{A}_{[x \mapsto a]}(G) = 1, \\ 0 & \text{egyébként.} \end{cases}$$

  Tehát: $\exists x G$ értéke akkor 1, ha felül tudjuk írni x értékét valami „alkalmas” a-ra úgy, hogy az így megváltoztatott $\mathcal{A}_{[x \mapsto a]}$ struktúrában a formula „belseje”, a **magja** igazzá váljon.

- Ha pedig $F = \forall x G$, akkor

$$\mathcal{A}(F) := \begin{cases} 1 & \text{ha minden } a \in A \text{ objektumra igaz, hogy } \mathcal{A}_{[x \mapsto a]}(G) = 1, \\ 0 & \text{egyébként.} \end{cases}$$

Például,

- ha $\mathcal{A} = (\mathbb{N}_0, I, \varphi)$ a természetes számok szokásos struktúrája: $I(0) = 0$, $I(1) = 1$, $I(+)$ összeadás, stb
- $I(<)$ a szokásos „kisebb” reláció
- $I(=)$ az egyenlőség (más nem is lehet)
- $\varphi(x) = 15$, $\varphi(y) = 16$

akkor pl. $\mathcal{A}$-ban

- $\mathcal{A}(x < y) = 1$, hiszen $\mathcal{A}(x) = 15$, $\mathcal{A}(y) = 16$ és $I(<)(15, 16)$ igaz („tizenöt kisebb, mint tizenhat”)
- $\mathcal{A}(\exists z(y < z))$ igaz, hiszen pl. az $\mathcal{A}_{[z \mapsto 20]}(y < z)$ igaz lesz: $16 < 20$
- $\mathcal{A}(\exists x(x < x))$ hamis
- $\mathcal{A}(\forall x(y < x))$ hamis, hiszen pl. $\mathcal{A}_{[x \mapsto 8]}(y < x)$ hamis ($16 < 8$ nem igaz)

Ugyanúgy, mint ítéletkalkulusban, azt, hogy $\mathcal{A}(F) = 1$, hogy F értéke igaz az $\mathcal{A}$ struktúrában, úgy is írjuk, hogy $\mathcal{A} \vDash F$, amit úgy olvasunk ki, hogy $\mathcal{A}$ **modellje** F**-nek**. Meg úgy is írhatjuk, hogy $\mathcal{A} \in \mathrm{Mod}(F)$. Itt a $\mathrm{Mod}(F)$ az F struktúra összes modelljének az osztálya[4]. Szintén ugyanúgy, mint ítéletkalkulusban, ha Σ formuláknak egy **halmaza**[5], akkor $\mathcal{A} \vDash \Sigma$ jelöli azt, hogy a $\mathcal{A}$ struktúrában kiértékelve a Σ **mindegyik eleme** igaz lesz, amit úgy is

[4] Az osztály olyan, mint egy halmaz, csak még annál is nagyobb lehet, mint egy halmaz. Pl. ha az összes halmazt egy nagy zsákba teszed, ez a zsák már nem lesz halmaz, mert ahhoz „túl nagy”, ez a zsák már egy osztály. Vannak, amik túl sokan vannak ahhoz, hogy elférjenek egy halmazban. Ha ennél jobban érdekel, vedd fel majd a Halmazelmélet tárgyat. Kivéve, ha már háromszor megbuktál belőle. Most pedig olvass tovább.

[5] na pl. azért volt fontos, hogy az összes jel megszámlálható sok legyen „csak”, hogy az összes formula is beférjen egyetlen halmazba. Így beférnek. Sőt, math says ez a halmaz is megszámlálható lesz, tehát fel tudjuk sorolni: lesz az első formula, a második, a harmadik stb. a kedvenc sorrendünk szerint. Meg a termek is így generálhatóak lesznek ciklusban az összes. Ez később fontos lesz majd.

mondjunk, hogy $\mathcal{A}$ **modellje Σ-nak**. Ha pedig Σ és Γ is formulahalmazok, akkor $\Sigma \vDash \Gamma$ azt jelöli, hogy Σ-nak a Γ következménye, azaz: ha egy $\mathcal{A}$ struktúrában igaz a bal oldal összes eleme, akkor abban igaz a jobb oldal összes eleme is. Amit úgy is írhatunk, hogy $\mathrm{Mod}(\Sigma) \subseteq \mathrm{Mod}(\Gamma)$: ami modellje a Σ-nak, az modellje kell legyen Γ-nak is.

Az is továbbra is igaz, hogy $\Sigma \vDash \downarrow$ pont azt jelenti, hogy Σ kielégíthetetlen: hiszen hogy $\Sigma \vDash \downarrow$, az egyrészt azt jelenti, hogy $\mathrm{Mod}(\Sigma) \subseteq \mathrm{Mod}(\downarrow)$, másrészt az ugye világos, hogy $\mathrm{Mod}(\downarrow) = \emptyset$ (az azonosan hamis formulának nincs modellje, modelljeinek halmaza üres) és ha a $\mathrm{Mod}(\Sigma)$ halmaz az $\emptyset$ üres halmaznak részhalmaza, akkor ő maga is üres kell legyen.

Az elsőrendű logika helyettesítési algoritmusa

A célja a helyettesítési algoritmusnak: az $\mathcal{A}_{[x\mapsto a]}$ értékadást szeretnénk úgy elvégezni, hogy a struktúráról közben nem tudunk semmit. Ez persze elég esélytelennek hangzik így, pontosítunk egy kicsit: a helyettesítési algoritmus egy olyan algoritmus, aminek

- inputja egy F formula, egy x változó és egy t term,
- outputja egy formula, amit $F[x/t]$-vel jelölünk,
- és azt várjuk el tőle, hogy **tetszőleges** $\mathcal{A}$ struktúrában

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

  igaz legyen.

Elolvasva az alsó sort ez mit jelent? Ha az $\mathcal{A}$ struktúrában az x értékét átállítjuk a t értékére, és ebben a megváltozott struktúrában értékeljük ki az F-et (ezt nem akarjuk megcsinálni, mert struktúrában kiértékelni nehéz), akkor ugyanazt kapjuk, mintha az eredeti struktúrában értékelnénk ki az algoritmus outputját, az $F[x/t]$ formulát.

Ezt konkrétan úgy kell csinálni, hogy

- az F-ben az x minden **szabad** előfordulását átírjuk t-re,
- és ha egy ilyen t-ben egy benne szereplő változó véletlenül „lekötődne”, akkor a kötő kvantor változóját átnevezzük valami egész újra (azokkal együtt, akikre ő alapból vonatkozott).

Ehhez még azt érdemes tudni, hogy az F-ben **kötött** egy x változó-előfordulás, ha egy Qx kvantor belsejében van, egyébként pedig **szabad**. Nézzük meg ezt egy példán:

$$\Big((\forall x\ p(g(x),y)) \wedge (\exists z\ \neg q(z,g(x)))\Big) \;\cdot\; [x/f(x,y,z)]$$

itt az első x (aki a $g(x)$-ben van a bal oldalon) az a $\forall x$ kvantor belsejében van, tehát azt nem bántjuk, a második x-et (a jobb oldalon levő $g(x)$-ben) viszont mivel szabad előfordulás, átírjuk $f(x,y,z)$-re. Ekkor a z bekerül a $\exists z$ scope-jába, ami miatt ezt a kötő kvantor z-jét átírjuk mondjuk u-ra, mert olyan még nincs. Az eredmény:

$$(\forall x\ p(g(x),y)) \wedge (\exists u\ \neg q(u,g(f(x,y,z))))$$

Termekre ugyanez a definíció azzal, hogy termben ofc nincs kvantor, ami lekötne a t-ben bármit, és minden változó-előfordulás szabad, tehát ott egy mezei replace-all a helyettesítési algoritmus.

Van ezekre induktív definíció[6] és lemmák is, hogy ezzel az algoritmussal tényleg megcsináljuk az értékadást a szintaktikai szinten, konkrétan

[6] soon

Állítás: a termekre vonatkozó helyettesítési lemma

Minden x változóra, t és u termekre és $\mathcal{A}$ struktúrára

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

Állítás: a formulákra vonatkozó helyettesítési lemma

Minden x változóra, t termre, F formulára és $\mathcal{A}$ struktúrára

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

Normálformák az elsőrendű logikában

Ahhoz, hogy következtető algoritmusokat futtassunk az input formulán, általában az valamilyen normálformára hozott inputot kér. A rezolúció például „zárt Skolem alakban levő formulákat, CNF-re hozott maggal” vár (minden változata, amit nézünk, mert bizony van több is). Nézzük mi ez:

Definíció

Egy formula **kiigazított**, ha

- különböző kvantorok különböző változókat kötnek le
- és nincs olyan változó, ami kötötten és szabadon is előfordul.

Például a

$$\exists x p(x,y) \;\wedge\; \forall x q(f(x),x) \;\wedge\; \exists y p(y,f(y))$$

nem kiigazított, mert pl.

- az x változót két különböző helyen is köti kvantor,
- az y pedig előfordul kötötten is és szabadon is.

(A fenti kettő közül az egyik ok is elég lenne.)

$$\exists x_1 p(x_1,y) \;\wedge\; \forall x_2 q(f(x_2),x_2) \;\wedge\; \exists y_1 p(y_1,f(y_1))$$

egy ekvivalens kiigazított formula. Általában is: ha az összes kvantor változóját valami újra cseréljük (pl. indexeléssel, mint fentebb), akkor kapunk egy ekvivalens kiigazított formulát.

De **mielőtt** ezt tennénk, érdemes a **nyilakat** eliminálni a szokásos

$$F \to G \equiv \neg F \vee G$$
$$F \leftrightarrow G \equiv (\neg F \vee G) \wedge (F \vee \neg G)$$

ekvivalenciákkal. Merthogy egy $\leftrightarrow$ belsejében levő kvantor ezzel az átírással duplikálódik és megint lesz két egyforma nevű lekötött változónk és megint igazíthatunk ki különben. Tehát előbb nyilak, aztán kiigazítás. Ezután:

Definíció

Egy formula **prenex alakú**, ha ki van igazítva és elöl vannak benne a kvantorok, vagyis

$$Qx_1Qx_2\dots Qx_nF$$

alakú, ahol az F-ben (a formula **magjában**)már nincs kvantor.

A prenex alakra hozás se nehéz, a kvantorokat ki lehet húzni kiigazított formulának az elejére azzal, hogy negáláson áthaladva átváltanak:

$$\neg(\exists xF) \equiv \forall x\ !(\neg F)$$
$$\neg(\forall xF) \equiv \exists x\ !(\neg F)$$
$$(\exists xF) \vee G \equiv \exists x(F \vee G),$$

és ezt az utóbbit variálhatjuk úgy, hogy $\vee$ helyett $\wedge$ legyen benne, vagy $\exists$ helyett $\forall$, esetleg F legyen a jobb oldalon és G a balon. Ez az így kapott nyolc ekvivalencia **akkor igaz, ha a formula ki van igazítva** (kicsit precízebben, akkor biztos igaz, ha F-ben nincs x szabadon – és ha az input ki van igazítva, akkor G-ben tényleg nem lehet x), ezért igazítunk ki az elején az algoritmusnak, hogy ezekkel tudjunk prenex alakra hozni.

Például a

$$\neg\Bigg(\bigg(\Big(\forall x\neg\forall y(p(x,y)\vee\exists zq(x,z))\Big)\wedge\exists wp(x,w)\bigg) \vee \neg\exists vq(v,v)\Bigg)$$

formulából ezekkel lesz egy

$$\forall w\exists v\exists x\forall y\exists z\neg\Bigg(\bigg(\Big(\neg(p(x,y)\vee q(x,z))\Big)\wedge p(x,w)\bigg)\vee\neg q(v,v)\Bigg)$$

formula néhány lépés után.

A prenex alakra hozott formula még mindig ekvivalens az eredetivel. Abból pedig elkészítünk egy Skolem (e. szkóólem) alakot:

Definíció

Egy formula **Skolem alakú**, ha prenex alakú és csak $\forall$ kvantor van benne, vagyis

$$\forall x_1\forall x_2\dots\forall x_nF$$

alakú, ahol F-ben már nincs kvantor.

Skolem alakot úgy kapunk egy prenex alakra hozott formulából, hogy

- végigmegyünk a prenex alakú formula kvantorain
- az összes $\exists y$, egzisztenciálisan kötött változóra
  - töröljük a $\exists y$ részt
  - a formula **magjában** minden y-t lecserélünk $f(x_1,\dots,x_n)$-re, ahol $x_1,\dots,x_n$ az y **előtt** deklarált, $\forall$-kötött változók, és f meg egy olyan új függvényjel (úgy hívják, hogy **Skolem függvény**), ami sehol máshol nem szerepel. (Tehát ha több formulából áll az input, akkor ez az új f egyikben se szabad legyen.)

Ha pl. ezt az algoritmust végrehajtjuk az

$$\forall w\exists v\exists x\forall y\exists z\neg\Bigg(\bigg(\Big(\neg(p(f(x),y)\vee q(x,z))\Big)\wedge p(x,w)\bigg)\vee\neg q(v,v)\Bigg)$$

formulán, akkor

- a $\exists v$-nél a v-ből egy $g(w)$ lesz, mert v előtt w volt $\forall$-deklarálva és g új függvényjel (f nem lehetne, minden más igen);
- a $\exists x$-nél x-ből mondjuk $h(w)$ lesz, mert x előtt is csak w volt $\forall$-deklarálva és h még újabb függvényjel (most már f, g nem játszik);
- a $\exists z$-nél z-ből mondjuk $i(w,y)$ lesz mindenhol, mert ezek voltak z előtt $\forall$-deklarálva.

És akkor az eredmény

$$\forall w\forall y\neg\Bigg(\bigg(\Big(\neg(p(f(h(w)),y)\vee q(h(w),i(w,y)))\Big)\wedge p(h(w),w)\bigg)\vee\neg q(g(w),g(w))\Bigg)$$

A kapott formula **nem** ekvivalens az eredetivel! Persze nem is nagyon lehet, hát van benne egy csomó új függvényjel, amiről szó nem volt eredetileg. Viszont **s-ekvivalens** vele. Ez azt jelenti, hogy ha az eredeti formula kielégíthető volt, akkor a Skolem alakja is, ha meg nem, akkor a Skolem alakja sem. És ez működik formula*halmaz*okra is: ha az input formulahalmaz minden elemét Skolem alakra hozzuk, úgy, hogy minden egyes Skolem függvény bevezetésekor teljesen új függvényjeleket gyártunk le, akkor az eredmény az Skolem normálformák olyan halmaza lesz, ami s-ekvivalens az eredetivel, vagyis kielégíthető, ha az input az volt és nem az, ha nem volt az.

Itt az s egyébként a „satisfiability"-nek a rövidítése.

És ez azért jó, mert eleve csak arra vagyunk kíváncsiak sokszor, hogy az input formulahalmazunk kielégíthető-e. Hogy miért? Mert hogy $\Sigma \vDash F$, hogy a Σ-nak következménye az F, azt sok következtető motor úgy bizonyítja, hogy indirekten megmutatja $\Sigma\cup\{\neg F\}$ kielégíthetetlenségét.

Itt meg még lesz az összes föntebbinek a bizonyítása is[7].

Ja az inputot még **le is zárjuk**: ez azt jelenti, hogy elérjük, hogy a formulákban ne legyen szabad változóelőfordulás. Mégpedig úgy, hogy minden szabad változóelőfordulást lecserélünk egy-egy új konstansra.

Herbrand struktúrák, a Herbrand tétel

Tehát ott tartunk, hogy van egy halmazunk, benne zárt Skolem normálformájú formulákkal[8] és arra vagyunk kíváncsiak, hogy kielégíthető-e.

Arra játszunk, hogy kielégíthetetlen legyen, annak örülünk (mert általában azt akarjuk, hogy valami következménye legyen valami másnak, amit pedig indirekten úgy bizonyítunk, hogy egy átalakított formulahalmazról belátjuk, hogy kielégíthetetlen). Ahhoz viszont, hogy belássuk, hogy kielégíthetetlen, meg kéne mutatni, hogy nincs neki semmilyen modellje, minden

[7] SOON

[8] amikben nincs egyenlőség. Az egyenlőség kezelése macerás. Egyelőre ne legyen.

struktúrában hamis. De struktúrából nagyon sok[9] van, mindet kipróbálni értelemszerűen nem tudjuk. (Mindenféle univerzummal, azon belül mindenféle függvény-interpretációval...)

Most csökkenteni fogjuk ezt a végtelen nagy keresési teret:

- Csak spéci alakú struktúrákban gondolkodunk, amiket Herbrand struktúrának hívunk;
- a Herbrand struktúrák úgy vannak definiálva, hogy ha valaminek[10] van egyáltalán akármilyen modellje, akkor van Herbrand modellje is (azaz. akkor van olyan Herbrand struktúra is, ami kielégíti).

Ez azért jó, mert ha ezek szerint azt meg tudjuk mutatni a zárt Skolem normálformáink halmazáról, az inputról, hogy nincs olyan Herbrand struktúra, ami kielégíti, akkor abból kijön az is, hogy semmilyen struktúra nincs, ami kielégíti, tehát akkor kielégíthetetlen.

Egyébként pl. az alap rezolúció (ld később) az pont azt mutatja meg az inputról, hogy nincs neki Herbrand modellje. Ezért lesz az egy helyes és teljes következtető rendszer.

Na tehát mi is tesz egy Herbrand struktúrát Herbrand struktúrává: hogy az objektumai maguk az alaptermek és hogy a függvényjelek alkalmazása függvényjelek alkalmazását jelenti:

Definíció: Herbrand struktúra

Egy $\mathcal{A} = (A, I, \varphi)$ struktúra **Herbrand-struktúra**, ha

- az A univerzum maga az alaptermek halmaza;
- ha f/n függvényjel és $t_1, \ldots, t_n \in A$ alaptermek, akkor

$$I(f)(t_1, \ldots, t_n) \;=\; f(t_1, \ldots, t_n)$$

Tehát φ-re és a predikátumjelek interpretációjára nincs semmi kikötés, csak az objektumok halmazára és a függvényjelek interpretációjára.

Azért, hogy az objektumok halmaza ne legyen üres, ebben a fejezetben arra is szükség van, hogy egyáltalán legyen alapterm. Emlékszünk: alapterm az volt, amit fel lehetett építeni csak függvényjelekből változók nélkül – tehát kiindulva a konstansokból, és alkalmazva rajtuk a nemnulla-változós függvényeket. Például ha $f/1$, $g/2$ és $c/0$ a függvényjeleink, akkor alapterm c, $f(c)$, $f(f(c))$, $g(c,c)$, $g(f(c),c)$ stb. **Nem** alapterm pl. x (termnek term, de nem alapterm, mert van benne változó), sem $g(c,x)$. Ha nincs konstansjel, alapterm sincs – ezért olyankor, ha nincs a formuláinkban egyetlen konstansjel sem, akkor gyártunk egy újat. Úgy már lesznek alaptermek.

Tehát ha $f/1$, $g/2$ és $c/0$ a függvényjeleink, akkor egy Herbrand-struktúrában:

- az objektumok maguk a c, $f(c)$, $f(f(c))$, $g(c,c)$, stb, az összes alapterm;
- a függvényinterpretációra például: ha c egy objektum és $f(c)$ egy objektum, és ezeken az f interpretációját akarjuk alkalmazni, akkor azt így kell kiszámolni:

$$I(f)(c, f(c)) \;=\; f(c, f(c))$$

[9]hja, ez is valódi osztály, annyira sok, hogy nem fér halmazba

[10]zárt Skolem normálformák halmazának

Easy enough. Elképzelni el lehet olyan struktúrát persze, ahol mondjuk a c konstansjelet az $f(c)$ objektummal interpretáljuk (why not), vagy ahol az $I(f)(c) := c$ (pl. ez van abban a struktúrában, amiben az objektumok a számok, c a nulla és f a négyzetreemelés), de azok nem Herbrand-struktúrák: Herbrand struktúrában $I(f)(c) = f(c)$ és $I(c) = c$, period. Szóval számolni könnyű Herbrand-struktúrában, mert minden alapterm önmagára értékelődik ki:

Állítás

Ha $\mathcal{A}$ egy Herbrand struktúra, t pedig egy alapterm, akkor $\mathcal{A}(t) = t$.

Ez azért jó még, mert egy Herbrand struktúrában minden objektumhoz van alapterm: konkrétan ha a t objektumra akarok „rámutatni” egy alaptermmel, akkor a t pont jó lesz erre a célra. Vannak olyan struktúrák, ahol nem minden elemet lehet kijelölni, pl. ha az alaphalmaz mondjuk az összes egész szám, de neked csak összeadásod van, 1-ed és 0-d van, abból nem tudsz negatív számra kiértékelődő alaptermet készíteni.

És ha egy struktúrában minden objektumra van alapterm, akkor az input Σ formulahalmazunk ekvivalens az ő **Herbrand-kiterjesztésével**, amit $E(Sigma)$-val jelölünk és úgy kapunk, hogy a formulából elhagyjuk a kvantorokat és a magban minden változó helyébe ízlés szerint alaptermeket helyettesítünk.

Például ha $F = \forall x \forall y \Big(p(x) \wedge q(x, f(y)) \Big)$, akkor (ha még van $c/0$ is az $f/1$-en kívül) pl. $E(F)$-ben, az F Herbrand kiterjesztésében van benne a $p(c) \wedge q(c, f(c))$ formula (x és y helyébe c került), a $p(f(c)) \wedge q(f(c), f(c))$ formula (x helyébe $f(c)$, y helyébe c) és még sokan mások.

Az alap rezolúció arra játszik, hogy ilyenekből legyártson annyit, ami már ellentmond önmagának.

Két tétel kombója miatt fog ez működni:

Állítás: Herbrand tétel

Zárt Skolem normálformák tetszőleges halmaza pontosan akkor kielégíthető, ha van Herbrand modellje.

Tehát a lényeg: ha kielégíthető, akkor van őt kielégítő Herbrand struktúra is. Ha nincs ilyen Herbrand struktúra, akkor az input kielégíthetetlen.

A másik tétel:

Állítás: Kompaktsági tétel

Egy Σ formulahalmaz pontosan akkor kielégíthető, ha minden véges részhalmaza kielégíthető.

Ez ebben a másik formában talán érthetőbb:

Állítás: Kompaktsági tétel

Ha Σ kielégíthetetlen, akkor van olyan véges része is, ami már kielégíthetetlen.

Tehát nem baj, ha végtelen nagy Σ halmaz kielégíthetetlenségét kell igazoljuk (ami tipikusan a helyzet akkor, ha egy Herbrand kiterjesztést nézegetünk: mivel alaptermből általában végtelen sok van, így $E(\Sigma)$ is általában végtelen nagy lesz), mert akkor van egy véges része is, ami már kielégíthetetlen. Tehát elég azt csinálni, hogy $E(\Sigma)$-nak szépen egyesével generálni az elemeit (itt ér össze az a rész, hogy megszámlálható sok mindenféle jelünk van: ezért tudunk termeket és formulákat szépen sorrendben generálni úgy, hogy mindenki sorra kerüljön előbb-utóbb), és ha már elég sokat kigeneráltunk, akkor ellent fog mondani magának, ha az egész Σ kielégíthetetlen.

A Herbrand tételnek van pár következménye is. Itt az egyik:

Állítás: A Herbrand tétel egy következménye

Ha zárt Skolem normálformák egy halmaza kielégíthető, akkor van olyan modellje is, aminek csak megszámlálhatóan sok objektuma van.

Ezt úgy is mondják, hogy „van megszámlálható modellje”. Persze ez meg azért igaz, mert a Herbrand tétel szerint van neki Herbrand modellje, amiben az univerzum az alaptermek halmaza; azok meg megszámlálható sokan vannak. easy.