PREDIKAATLOOGIKA

- Predikaatloogika on lauseloogika tugev laiendus. Predikaatloogikas saab nimetada asju ning rääkida nende omadustest.

  Väljendusvõimsuselt on predikaatloogika seega oluliselt peenekoelisem kui lauseloogika. Samas on predikaatloogikate valemite tõesuse, üldkehtivuse või kehtestatavuse kontroll oluliselt raskem kui lauseloogika valemite oma.

PREDIKAATLOOGIKA: SÜNTAKS

- Predikaatloogika *signatuur* on paar $(\mathrm{FC}, \mathrm{PC})$, kus $\mathrm{FC} = \{f, g, \ldots, c, d, \ldots\}$ on tähestik, mille sümboleid nimetatakse *funktsioonisümboliteks*; igale sümbolile on määratud mingi lõplik aarsus; ja $\mathrm{PC} = \{p, q, \ldots\}$ on tähestik, mille sümboleid nimetatakse *predikaatsümboliteks*; ka neil on kõigil fikseeritud lõplik aarsus.

  0-aarseid funktsioonisümboleid kutsutakse ka *indiviidsümboleid*, 0-aarseid predikaatsümboleid kutsutakse ka *lausesümboliteks*. Kõiki nimetatud sümboleid on (meil siin) mõistlik lugeda konstantideks.

- Lisaks eeldame loenduvat tähestikku $\mathrm{Var} = \{x, y, \ldots\}$, mida nimetame muutujavaruks. Tema elemente nimetame *(indiviid)muutujateks*.

- Predikaatloogika *termid* (üle signatuuri $(\mathrm{FC}, \mathrm{PC})$) on hulk väljendeid ehk keel $\mathrm{Tm} = \{t, u, \ldots\}$, mis on defineeritud induktiivselt järgmiste tingimustega:
  - iga indiviidmuutuja x on term;
  - iga indiviidkonstant c on term;
  - kui f on n-aarne funktsioonikonstant ja $t_1, \ldots, t_n$ on termid, siis $f(t_1, \ldots, t_n)$ on term.
- Näide: x, c, $f(x, c)$, $g(f(x, c), h(d))$ on termid.

WAI 3720 Loogika arvutiteaduses Sügis 2002 / Tarmo Uustalu Loeng 5

- Predikaatloogika *valemid* (üle signatuuri $(\mathrm{FC}, \mathrm{PC})$) on hulk väljendeid ehk keel $\mathrm{Fma} = \{A, B, \ldots\}$, mis on defineeritud induktiivselt järgmiste tingimustega:
  - kui p on n-aarne predikaatkonstant ja $t_1, \ldots, t_n$ on termid, siis $p(t_1, \ldots, t_n)$ on valem (nn atomaarvalem);
  - $\top$ (verum, tõde), $\bot$ (falsum, väärus) on valemid;
  - kui A on valem, siis $\neg A$ (mitte-A) on samuti valem;
  - kui A, B on valemid, siis $A \land B$ (A ja B), $A \lor B$ (A või B), $A \supset B$ (kui A, siis B e A implitseerib B) on ka valemid;
  - kui x on indiviidmuutuja ja A on valem, siis $\forall x.\ A$ (iga x korral A) ja $\exists x.\ A$ (leidub x, et A) on valemid.
- Sümboleid $\forall$ (üldisuskvantor), $\exists$ (olemasolukvantor) nimetatakse kvantoriteks.
- Näide: $\top$, $\neg p(x)$, $\forall x.\ (\neg p(x) \supset q(h(x), c))$, $\forall x.\ \forall y.\ \exists z.(f(x, z) \land f(y, z))$ on valemid.

- Kvantorid *seovad* muutujaid valemis, täpsemalt muutujate esinemisi. Kvantoriteta valemis on kõik muutujaesinemised vabad. Valemis $\forall x.\ A$ [$\exists x.\ A$] on muutuja x vabad esinemised valemis A välimise kvantori $\forall$ [$\exists$] poolt seotud.
- Näide: Valemis $p(x) \wedge \forall x.\ (q(x) \vee \exists x.\ r(x))$ on muutuja x esimene esinemine vaba, teine seotud üldisuskvantoriga, kolmas eksistentsikvantoriga.
- $A[t/x]$ tähistab valemit, mis saadakse valemist A muutuja x kõigi vabade esinemiste asendamisel termiga t.
- Näiteid: $(p(x, y) \vee r(a, x))[f(z)/x] = p(f(z), y) \vee r(a, f(z))$;
$(p(x) \wedge \forall x.\ q(x))[c/x] = p(c) \wedge \forall x.\ q(x)$.

WAI 3720 Loogika arvutiteaduses Sügis 2002 / Tarmo Uustalu Loeng 5

- Valemi *alamvalemiteks* on kõik temas alamväljenditena esinevad valemid. Laiemas mõttes on valemi alamvalemiteks kõigi temas alamväljenditena esinevate valemite kõik substitutsioonieksemplarid (valemid, mis on saadud vabade muutujate süstemaatilisel asendamisel mingite termidega).
- Näide: Valemi $\forall x.\ \forall y.\ \exists z.(f(x, z) \wedge f(y, z))$ alamvalemiteks võib lugeda mh. valemid $\forall y.\ \exists z.(f(h(c), z) \wedge f(y, z))$ ja $f(h(w), d) \wedge f(f(c, w), d)$

Predikaatloogika: Semantika

- Olgu $(\mathrm{FC}, \mathrm{PC})$ fikseeritud predikaatloogiline signatuur, st funktsioonikonstantide (sh indiviidkonstantide) ja predikaatkonstantide tähestik.
- *Struktuur* on siis suvaline paar $M = (D, I)$, kus D on mingi mittetühi hulk (*põhihulgaks* ehk *kandja*) ning I on sõltuv funktsioon (*interpretatsioon*), mis igale n-aarsele funktsioonikonstandile seab vastavuse mingi funktsiooni $D^n \to D$ (sh igale indiviidkonstandile mingi elemendi hulgast D) ja igale n-aarsele predikaatkonstandile mingi funktsiooni $D^n \to \{1, 0\}$.
- *Omistus* (assignment) on suvaline funktsioon $\alpha : \mathrm{Var} \to D$.
- Suvalise omistuse α ja suvaliste $x \in \mathrm{Var}$, $d \in D$ jaoks defineerime modifitseeritud omistuse $\alpha\{d/x\}$ järgmiselt:

$$\alpha\{d/x\}(y) = \begin{cases} d & \text{kui } y = x \text{ (süntaktiliselt)} \\ \alpha(y) & \text{muidu} \end{cases}$$

- Predikaatarvutuse termide *väärtustus* struktuuris $M = (D, I)$ ja omistuse α suhtes on funktsiooon $[\![\cdot]\!]^{M,\alpha} : \mathrm{Tm} \to D$, mis on defineeritud induktsiooniga järgmiselt:
  - $[\![x]\!]^{M,\alpha} = \alpha(x)$, kui x on indiviidmuutuja;
  - $[\![c]\!]^{M,\alpha} = I(c)$, kui c on indiviidkonstant;
  - $[\![f(t_1, \ldots, t_n)]\!]^{M,\alpha} = I(f)([\![t_1]\!]^{M,\alpha}, \ldots, [\![t_n]\!]^{M,\alpha})$, kui f in funktsioonikonstant.

- Predikaatarvutuse valemite *väärtustus* struktuuris $M = (D, I)$ ja omistuse α suhtes on funktsioon $[\![\cdot]\!]^{M,\alpha} : \mathrm{Fma} \to \{1, 0\}$, mis on defineeritud induktsiooniga järgmiselt:
  - $[\![p(t_1, \ldots, t_n)]\!]^{M,\alpha} = I(p)([\![t_1]\!]^{M,\alpha}, \ldots, [\![t_n]\!]^{M,\alpha})$, kui p on predikaatkonstant;
  - $[\![\top]\!]^{M,\alpha} = 1$, $[\![\bot]\!]^{M,\alpha} = 0$;
  - $[\![\neg A]\!]^{M,\alpha} = 1 - [\![A]\!]^{M,\alpha}$;
  - $[\![A \wedge B]\!]^{M,\alpha} = \min([\![A]\!]^{M,\alpha}, [\![B]\!]^{M,\alpha})$;
  - $[\![A \vee B]\!]^{M,\alpha} = \max([\![A]\!]^{M,\alpha}, [\![B]\!]^{M,\alpha})$;
  - $[\![A \supset B]\!]^{M,\alpha} = \max(1 - [\![A]\!]^{M,\alpha}, [\![B]\!]^{M,\alpha})$;
  - $[\![\forall x.\, A]\!]^{M,\alpha} = \min_{d \in D}([\![A]\!]^{M,\alpha\{d/x\}})$;
  - $[\![\exists x.\, A]\!]^{M,\alpha} = \max_{d \in D}([\![A]\!]^{M,\alpha\{d/x\}})$.

- Valem A loetakse struktuuris M omistuse α suhtes *tõeseks* (tähistus $M \models A[\alpha]$), kui $[\![A]\!]^{M,\alpha} = 1$.
- Võime veenduda, et iga $M = (D, I)$ ja α korral
  - $M \models p(t_1, \ldots, t_n)[\alpha]$ parajasti siis, kui $I(p)([\![t_1]\!]^{M,\alpha}, \ldots, [\![t_n]\!]^{M,\alpha}) = 1$, kui p on predikaatkonstant;
  - $M \models \top[\alpha]$ alati; $M \models \bot[\alpha]$ mitte kunagi;
  - $M \models \neg A[\alpha]$ parajasti siis, kui $M \not\models A[\alpha]$;
  - $M \models A \wedge B[\alpha]$ parajasti siis, kui $M \models A[\alpha]$ ja $M \models B[\alpha]$;
  - $M \models A \vee B[\alpha]$ parajasti siis, kui $M \models A[\alpha]$ või $M \models B[\alpha]$;
  - $M \models A \supset B[\alpha]$ parajasti siis, kui $M \not\models A[\alpha]$ või $M \models B[\alpha]$;
  - $M \models \forall x.\, A[\alpha]$ parajasti siis, kui iga $d \in D$ korral $M \models A[\alpha\{d/x\}]$;
  - $M \models \exists x.\, A[\alpha]$ parajasti siis, kui leidub $d \in D$, et $M \models A[\alpha\{d/x\}]$;

- Struktuur $M = (D, I)$ *kehtestab* valemi A, A *kehtib* M-is, A on M-is *tõene* ehk M on A *mudel* (tähistus $M \models A$), kui $M \models A\ [\alpha]$ (st. $[\![A]\!]^{M,\alpha} = 1$) iga omistuse α korral.
- Valem A on *üldkehtiv*, *tautoloogiline* ehk *loogiliselt tõene* (tähistus $\models A$), kui A kehtib igas struktuuris.

- Näiteid predikaatloogika väljendusvõimalustest:
  - $\forall x.\ \forall y.\ (p(x, y) \supset p(y, x))$: p on sümmeetriline relatsioon;
  - $\forall x.\ \exists y.\ p(x, y)$: funktsioonina mõistetuna on p totaalne;
  - $\exists x.\ \exists y.\ (p(x) \wedge \neg p(y))$: mõnel põhihulga elemendil on omadus p, mõnel pole (see valem saab olla tõene ainult siis, kui põhihulgas on vähemalt kaks elementi);
  - $\forall x.\ p(a, x)$: a on põhihulga vähim element relatsiooni p suhtes.

- Näiteid predikaatloogika tautoloogiatest:

$$\forall x.\, A \equiv \neg\exists x.\, \neg A$$
$$\exists x.\, A \equiv \neg\forall x.\, \neg A$$
$$\forall x.\, A \supset \exists x.\, A$$
$$\exists x.\, \forall y.\, A \supset \forall y.\, \exists x.\, A$$
$$\forall x.\, (A \wedge B) \equiv \forall x.\, A \wedge \forall x.\, B$$
$$\exists x.\, (A \vee B) \equiv \exists x.\, A \vee \exists x.\, B$$
$$\forall x.\, A \vee \forall x.\, B \supset \forall x.\, (A \vee B)$$
$$\exists x.\, (A \wedge B) \supset \exists x.\, A \wedge \exists x.\, B$$
$$(\exists x.\, A \supset \forall x.\, B) \supset \forall x.\, (A \supset B)$$
$$\exists x.\, (A \supset B) \equiv (\forall x.\, A \supset \exists x.\, B)$$

- Erinevalt lauseloogika juhust, on TAUT predikaatloogika puhul poollahenduv, st leiduvad algoritmid, mis etteantud valemi kohta vastavad "jah", kui see valem on üldkehtiv, ning vastavad "ei" või ei lõpeta, kui ta on vääratav.

  Samaaegselt on TAUT ka kopoollahenduv, st leiduvad algoritmid, mis etteantud valemi kohta vastavad "jah" või ei lõpeta, kui see valem on üldkehtiv, ning vastavad "ei", kui ta on vääratav.

  Sama kehtib SAT kohta.