Tik-79.154 Logiikka tietotekniikassa: erityiskysymyksiä II (2 ov)

Luennot: torstaisin klo 14–16, sali TB353
Luennoitsija: TkT Tomi Janhunen, TB335,
puh. 451 3255, e-mail: Tomi.Janhunen@hut.fi.

Laskuharjoitukset: tiistaisin klo 16–17, sali TB353
Laskuharjoitusassistentti: DI Tommi Syrjänen, TB350,
puh. 451 5082, e-mail: Tommi.Syrjanen@hut.fi.

Kotisivu: `http://www.tcs.hut.fi/Teaching/Tik-79.154/`

Uutisryhmä: `opinnot.tik.logiikka`

Kurssin sisältö

- Lauselogiikan parhaat toteutusmenetelmät: Davis-Putnam, BDDs, stokastiset menetelmät.
- Sääntöpohjainen päättely (looginen pohja, toteutusmenetelmät)
- Sovellutuksia
- Tietojenkäsittelyssä usein toistuvat käsitteet:
  - formaali malli
  - ristiriidattomuus ja täydellisyys
  - tehokkuus; laajojen ongelmien monimutkaisuus

Kurssin suorittaminen

Kurssin suorittaminen edellyttää hyväksyttyjä

- **kolmea kotitehtävää**
  - Ongelman mallintaminen
  - Ratkaisun löytäminen opetetuilla menetelmillä
  - Arvostelu: hyväksytty / hylätty
- **tenttiä**
  maanantaina 11.12.2000 klo 9–12, sali T1

Kurssin arvosana määräytyy tentin arvosanan mukaan.

Lauselogiikka tietojenkäsittelyssä

➤ Formaalit menetelmät yleistyvät

➤ Logiikkapohjaisten työkalujen käyttö tavallista

The use of formal verification tools is well established and becoming more so. Simulation- and emulation-based methodologies aren't sufficient to guarantee correctness with today's complex chips.

(Carl Pixley, Motorola Inc. in IEEE Spectrum, Jan 1997, p. 61)

☞ Tietokoneiden suorituskyvyn ja muistin määrän nopea kasvu

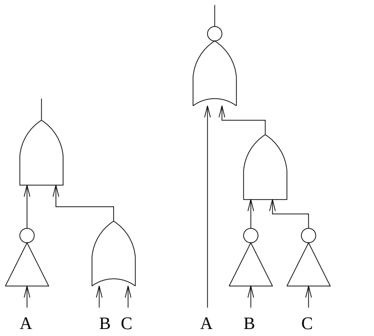
☞ Toteutusmenetelmien kehitys

Sovellutusalueita

- Digitaalipiirien verifiointi
- Digitaalipiirien synteesi
- Vikadiagnoosi
- Testien generointi
- Rinnakkaisten ja hajautettujen järjestelmien verifiointi
- Suunnittelu
- Logistiikka

Esimerkki: digitaalipiirien verifiointi

- Piirin määrittely ja toteutus esitetään logiikan lauseina.
- Toteutuksen oikeellisuus verifioidaan tarkastamalla looginen ekvivalenssi määrittelyn kanssa.



$\neg A \wedge (B \vee C)$ vs $\neg(A \vee (\neg B \wedge \neg C))$

Esimerkki: rajoiteohjelmointi

3-väritysongelma: Voidaanko annetun graafin solmut värittää kolmella värillä siten, ettei naapureilla ole sama väri.

Graafin jokaista solmua n kohti 3 atomilausetta: n_p, n_s, n_v

Rajoitteet:
(i) kullekin solmulle n,
$n_p \vee n_s \vee n_v$

(ii) jos solmujen n ja m välillä on kaari:
$\neg n_p \vee \neg m_p$
$\neg n_s \vee \neg m_s$
$\neg n_v \vee \neg m_v$

☞ Graafilla on 3-väritys jos ja vain jos lausejoukko on toteutuva.

Kertausta

Lauselogiikan syntaksi

Lauselogiikan *aakkosto*:

$A_1, A_2, A_3, \ldots$	atomilauseet
$\neg$	negaatio, ei
$\wedge$	konjunktio, ja
$\vee$	disjunktio, tai
$\rightarrow$	implikaatio, jos...niin
$\leftrightarrow$	ekvivalenssi, ...jos ja vain jos...
$()$	sulut

Symbolit $\neg, \vee, \wedge, \rightarrow, \leftrightarrow$ ovat *lausekonnektiiveja*.

Lauselogiikan *lauseenmuodostussäännöt*:

1. atomilauseet ovat *lauseita*.
2. jos P ja Q ovat lauseita, niin myös
   $(\neg P)$,
   $(P \vee Q)$,
   $(P \wedge Q)$,
   $(P \rightarrow Q)$ ja
   $(P \leftrightarrow Q)$
   ovat *lauseita*.
3. muita *lauseita* ei ole.

Sulkeita voidaan jättää pois presedenssisääntöjen nojalla:
$\neg$ vahvin konnektiivi; sitten $\vee$ ja $\wedge$; heikoimmat $\rightarrow$ ja $\leftrightarrow$.

Lauselogiikan semantiikka

Lauselogiikan *malli* on joukko atomilauseita.

(Usein käytetty vaihtoehtoinen määritelmä: kielen, jonka atomilauseiden joukko on $\mathcal{A} = \{A_1, A_2, \ldots\}$, mallit ovat funktioita v (valuaatio) joukolta $\mathcal{A}$ joukolle $\{t, e\}$.)

Olkoon malli $M = \{A_1, A_4\}$. Tässä mallissa ovat tosia atomilauseet A_1 ja A_4. Muut atomilauseet, esim. A_2, A_3 ja A_5, eivät ole tässä mallissa tosia.

Määritellään induktiivisesti lauseille P ja malleille M, milloin P on *tosi* M:ssä ($M \models P$).

- $M \models A$ jos ja vain jos (joss) $A \in M$ atomilauseelle A.
- $M \models \neg P$ joss $M \not\models P$.
- $M \models P \wedge Q$ joss $M \models P$ ja $M \models Q$.
- $M \models P \vee Q$ joss $M \models P$ tai $M \models Q$.
- $M \models P \rightarrow Q$ joss $M \not\models P$ tai $M \models Q$.
- $M \models P \leftrightarrow Q$ joss joko $M \models P$ ja $M \models Q$ tai $M \not\models P$ ja $M \not\models Q$.

Huom.
$M \models P_1 \vee \cdots \vee P_n$ joss on olemassa $i, 1 \leq i \leq n$ siten, että $M \models P_i$.

$M \models P_i \wedge \cdots \wedge P_n$ joss kaikille $i, 1 \leq i \leq n$, $M \models P_i$.

Määritelmä 1 *Lause P on* pätevä *joss P on tosi jokaisessa lauselogiikan mallissa. Tämä merkitään $\models P$.*

Määritelmä 2 *Lauseet P ja Q ovat* loogisesti ekvivalentteja *jos $M \models P$ joss $M \models Q$ kaikille malleille M.*

Huomaa yhteys: P ja Q ovat loog. ekvivalentit joss $\models P \leftrightarrow Q$.

Määritelmä 3 *Lause P on* toteutuva *joss P on tosi ainakin yhdessä lauselogiikan mallissa.*

Määritelmä 4 *Olkoon Σ joukko lauseita ja olkoon M malli. Sanomme, että M* on Σ:n malli *jos jokainen Σ:n lause on tosi M:ssä. Merkintätapa: $M \models \Sigma$.*

Määritelmä 5 *Lause P on Σ:n* looginen seuraus *joss P on tosi jokaisessa Σ:n mallissa. Merkintätapa: $\Sigma \models P$.*

Huomaa yhteys: $\Sigma \models P$ joss $\Sigma \cup \{\neg P\}$ ei ole toteutuva.

Normaalimuodot

Määritelmä 6 *Jos A on atomilause, niin A ja $\neg A$ ovat* literaaleja.

Määritelmä 7 *Lause α on* konjunktiivisessa normaalimuodossa *jos α on muotoa $\beta_1 \wedge \beta_2 \wedge \cdots \wedge \beta_n$, ja kukin β_i on disjunktio $l_1 \vee l_2 \vee \cdots \vee l_{m_i}$, missä $l_1, l_2, \ldots, l_{m_i}$ ovat literaaleja.*

Konjunktiivisessa normaalimuodossa oleva lause $\beta_1 \wedge \beta_2 \wedge \cdots \wedge \beta_n$ esitetään usein joukkona disjunktioita $\{\beta_1, \beta_2, \ldots \beta_n\}$.

Kukin disjunktio β_i esitetään usein klausuulina (joukkona literaaleja) $\{l_1, l_2, \ldots, l_{m_i}\}$ tai muodossa $A_1 \vee \cdots \vee A_n \leftarrow B_1 \wedge \cdots \wedge B_m$ missä A_i:t ovat klausuulin positiiviset ja B_j:t negatiiviset atomit.

Esim. disjunktio $\neg A \vee B \vee \neg C \vee D$ voidaan esittää muodossa $\{\neg A, B, \neg C, D\}$ tai $B \vee D \leftarrow A \wedge C$.

Normaalimuotoon muuttaminen

Teoreema 8 *Jokaiselle lauselogiikan lauseelle α on olemassa konjunktiivisessa (disjunktiivisessa) normaalimuodossa oleva lause β, joka on loogisesti ekvivalentti α:n kanssa.*

1. Poista konnektiivit $\leftrightarrow$ seuraavanlaisilla korvauksilla:

   $\alpha \leftrightarrow \beta \quad \Rightarrow \quad (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha) \qquad (1)$

   $\alpha \leftrightarrow \beta \quad \Rightarrow \quad (\neg\alpha \vee \beta) \wedge (\neg\beta \vee \alpha) \qquad (1')$

2. Poista konnektiivit $\rightarrow$ seuraavanlaisilla korvauksilla:

   $\alpha \rightarrow \beta \quad \Rightarrow \quad \neg\alpha \vee \beta \qquad (2)$

3. Siirrä negaatiot välittömästi atomilauseiden eteen:

   $\neg\neg\alpha \quad \Rightarrow \quad \alpha \qquad (3)$

   $\neg(\alpha \vee \beta) \quad \Rightarrow \quad \neg\alpha \wedge \neg\beta \qquad (4)$

   $\neg(\alpha \wedge \beta) \quad \Rightarrow \quad \neg\alpha \vee \neg\beta \qquad (5)$

4. (CNF) Lopuksi siirrä $\wedge$-konnektiivit $\vee$-konnektiivien ulkopuolelle:

   $\alpha \vee (\beta \wedge \gamma) \quad \Rightarrow \quad (\alpha \vee \beta) \wedge (\alpha \vee \gamma) \qquad (6)$

   $(\alpha \wedge \beta) \vee \gamma \quad \Rightarrow \quad (\alpha \vee \gamma) \wedge (\beta \vee \gamma) \qquad (7)$

   Tai (DNF) siirrä $\vee$-konnektiivit $\wedge$-konnektiivien ulkopuolelle:

   $\alpha \wedge (\beta \vee \gamma) \quad \Rightarrow \quad (\alpha \wedge \beta) \vee (\alpha \wedge \gamma) \qquad (8)$

   $(\alpha \vee \beta) \wedge \gamma \quad \Rightarrow \quad (\alpha \wedge \gamma) \vee (\beta \wedge \gamma) \qquad (9)$

Predikaattilogiikasta lauselogiikkaan

- Useissa sovellutuksissa lauselogiikka riittää (muuttujat toimivat lyhennysmerkintänä: $Dom(x) \wedge P(x) \rightarrow Q(x)$)
- Predikaattilogiikan päättely voidaan palauttaa lauselogiikan päättelyksi seuraavasti. Olkoon Σ predikaattilogiikan lausejoukko.
  - Muunnetaan Σ klausuulijoukoksi S siten, että Σ on toteutumaton joss S on toteutumaton.
    $\Rightarrow$ prenex-muotoon $\Rightarrow$ skolemointi $\Rightarrow$ konj. normaalimuotoon
  - S on toteutumaton joss sen Herbrand-instanssien joukko S' on toteutumaton.
  - S on toteutumaton joss on olemassa äärellinen toteutumaton Herbrand-instanssien S' osajoukko.

Lauseiden muuttaminen prenex-normaalimuotoon

Prenex-normaalimuoto: $\mathcal{Q}_1 x_1 \mathcal{Q}_2 x_2 \cdots \mathcal{Q}_n x_n \phi$,

missä $\mathcal{Q}_i$ ovat kvanttoreita $\forall$ tai $\exists$, ja ϕ ei sisällä kvanttoreita

- Poistetaan konnektiivit $\rightarrow$ ja $\leftrightarrow$ (kuten CNF-muunnoksessa).
- Negaatiot sisään (konnektiiveille $\vee, \wedge$ kuten CNF), kvanttorit ulos (z on uusi muuttuja):

$$\begin{aligned} \vec{\mathcal{Q}}x \neg \forall y \varphi &\Rightarrow \vec{\mathcal{Q}}x \exists y \neg \varphi \\ \vec{\mathcal{Q}}x \neg \exists y \varphi &\Rightarrow \vec{\mathcal{Q}}x \forall y \neg \varphi \\ \vec{\mathcal{Q}}x (\forall y \varphi \vee \psi) &\Rightarrow \vec{\mathcal{Q}}x \forall z (\varphi(y/z) \vee \psi) \text{ (ja 7 varianttia)} \end{aligned}$$

Skolemointi

- Olkoon $\vec{\mathcal{Q}}x\phi$ prenex-normaalimuodossa. Sisältäköön $\vec{\mathcal{Q}}x$ kvanttorin $\exists x_i$, ja $\exists x_i$:tä edeltää universaalikvanttorit $\forall x_{n_1}, \forall x_{n_2}, \ldots, \forall x_{n_m}$.
- Poista kvanttori $\exists x_i$, ja korvaa x_i:n jokainen esiintymä termillä $f(x_{n_1}, x_{n_2}, \ldots, x_{n_m})$, missä f on uusi funktiosymboli.
- Jos $\exists x_i$:tä ei edellä ainutkaan universaalikvanttori, korvataan x_i uudella vakiolla c.

Huom! Skolemointi ei säilytä loogista ekvivalenssia mutta säilyttää toteutuvuuden.

Konjunktiivinen normaalimuoto

Lause prenex-normaalimuotoon $\Rightarrow$ skolemisoidaan $\Rightarrow$ konjunktiiviseen normaalimuotoon.

$$\begin{aligned} \forall x(\forall y P(x,y) \rightarrow \exists y Q(x,y)) &\Rightarrow \forall x(\neg \forall y P(x,y) \vee \exists y Q(x,y)) \\ \forall x(\exists y \neg P(x,y) \vee \exists y Q(x,y)) &\Rightarrow \forall x \exists z \exists v(\neg P(x,z) \vee Q(x,v)) \\ &\Rightarrow \forall x(\neg P(x, f_1(x)) \vee Q(x, f_2(x))) \end{aligned}$$

Disjunktioista jätetään usein universaalikvanttorit pois ja ne esitetään klausuuleina (literaalijoukkona)

$$\{\neg P(x, f_1(x)), Q(x, f_2(x))\}$$

tai esim. muodossa $Q(x, f_2(x)) \leftarrow P(x, f_1(x))$

Herbrand-mallit

- Lausejoukon *Herbrand-universumi* on niiden muuttujattomien termien joukko, joka voidaan rakentaa lausejoukossa esiintyvistä vakio- ja funktiosymboleista. Jos lausejoukossa ei esiinny vakio- ja funktiosymboleja on Herbrand-universumi $\{c\}$.
- Lausejoukon *Herbrand-kanta* koostuu atomisista lauseista, jotka voidaan konstruoida käyttäen joukossa esiintyviä predikaattisymboleja ja Herbrand-universumin termejä.
- *Herbrand-malli* on osajoukko Herbrand-kannasta.
- Klausuulijoukon *Herbrand-instanssit* saadaan sijoittamalla muuttujille Herbrand-universumin termejä.

Esimerkki. Olkoon lausejoukko $\Sigma = \{\neg P(x) \lor Q(f(x,x))), P(c)\}$.

Lausejoukossa esiintyvät vakio c ja funktiosymboli $f(\cdot,\cdot)$.

- Herbrand-universumi on
  $c, f(c,c), f(f(c,c),c), f(c,f(c,c)), f(f(c,c),f(c,c)), \ldots$.
- Herbrand-kanta $P(c), Q(c), P(f(c,c)), Q(f(c,c)), \ldots$
- $\{P(c), P(f(c,c))\}$ on Herbrand-malli.
- Herbrand-instanssit:
  $P(c), \neg P(c) \lor Q(f(c,c))), \neg P(f(c,c)) \lor Q(f(f(c,c),f(c,c)))), \ldots$

Tietämyksen esittäminen

- Jokaisen vakiosymbolin viitattava eri alkioon (unique names):

$$\neg(a = b), \neg(b = c), \neg(c = a)$$

- Ei muita objekteja kuin nimetyt (domain closure):

$$\forall x(x = a \lor x = b \lor x = c)$$

☞ Herbrand-mallit

☞ Jos lauseissa ei esiinny funktiosymboleja,
Herbrand-instansseja on äärellinen määrä $\Rightarrow$ ratkeavuus.