T-79.3001 Logiikka tietotekniikassa: perusteet **Kevät 2008**
Laskuharjoitus 12 (predikaattilogiikka 15.1 – 15.5)
29.–30.4. ja 2.5.2008

Ratkaisuja demotehtäviin

Tehtävä 15.4

Opetusmoniste määritteli Boolen lauseet tiettyjen perustapausten avulla, muiden ollessa lyhennysmerkintöjä. Näin ollen:

$$\texttt{a==b} \equiv_{def} \texttt{!(a>b)\&\&!(b>a)}$$

ja

$$\begin{aligned} \texttt{a<b} &\equiv_{def} \texttt{b>a} \\ \texttt{a!=b} &\equiv_{def} \texttt{!(a==b)} \end{aligned}$$

Valitaan atomilauseiksi $A =$“$\texttt{a>b}$” ja $B =$“$\texttt{b>a}$”. Näin (a)-kohdan lause saa muodon

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

ja (b)-kohdan vastaavasti:

$$\neg(\neg A \wedge \neg B) \wedge \neg B$$

Havaitaan, että kun ensimmäiseen lauseeseen sovelletaan kerran De Morganin sääntöä saadaan jälkimmäinen lause. Näin ollen ne ovat ekvivalentit.

Tehtävä 15.5

Esitetyt ohjelmat koostuvat peräkkäisistä sijoituslausekkeista. Näin ollen ne voidaan ratkaista käyttämällä hyväksi opetusmonisteessa annettuja päättelysääntöjä:

Sijoituslauseke: $$\frac{}{[B\{\texttt{x}/E\}]\ \texttt{x=}E\ [B]}$$

Kompositio: $$\frac{[B_0]\ C_1\ [B_1] \qquad [B_1]\ C_2\ [B_2]}{[B_0]\ C_1\ \texttt{;}\ C_2\ [B_2]}$$

(a) $\models_p\ [\texttt{x>0}]\ \texttt{y=x+1}\ [\texttt{y>1}]$

Lähtemällä jälkiehdosta ja soveltamalla sijoituslausekkeen päättelysääntöä taaksepäin saadaan muoto $[\texttt{x+1>1}]\ \texttt{y=x+1}\ [\texttt{y>1}]$

$\texttt{x>0}$ on ekvivalentti lauseke $\texttt{x+1>1}$ kanssa, joten erityisesti siis sen vahvennus, jolloin väite pätee.

(b) $\models_p$ $[\texttt{true}]\ \texttt{y=x;y=x+x+y}\ [\texttt{y==3*x}]$

Soveltamalla kahteen kertaan sijoituslausekkeen päättelysääntöä saadaan muoto:

$$[\texttt{x+x+y==3*x}]\ \texttt{y=x+x+y}\ [\texttt{y==3*x}]$$
$$[\texttt{x+x+x==3*x}]\ \texttt{y=x}\ [\texttt{x+x+y==3*x}]$$

ja edelleen komposition sääntöä soveltamalla:

$$[\texttt{x+x+x==3*x}]\ \texttt{y=x;y=x+x+y}\ [\texttt{y==3*x}].$$

Lauseke $\texttt{x+x+x==3*x}$ on identtisesti tosi kokonaislukujen joukossa, jolloin väite pätee.

(c) $\models_p$ $[\texttt{x>1}]\ \texttt{a=1;y=x;y=y-a}\ [\texttt{y>0\&\&x>y}]$

Samoin kuin b-kohdassa sijoituslausekkeen päättelysääntöä tulee soveltaa peräkkäin. Saadaan:

$$[\texttt{y-a>0\&\&x>y-a}]\ \texttt{y=y-a}\ [\texttt{y>0\&\&x>y}]$$
$$[\texttt{x-a>0\&\&x>x-a}]\ \texttt{y=x}\ [\texttt{y-a>0\&\&x>y-a}]$$
$$[\texttt{x-1>0\&\&x>x-1}]\ \texttt{a=1}\ [\texttt{x-a>0\&\&x>x-a}].$$

Kompositiosäännön suoraviivainen sovellus sivuutetaan. Nyt ensimmäisen ehdon $\texttt{x-1>0\&\&x>x-1}$ jälkimmäinen konjunkti on tutkittavissa kokonaislukustruktuureissa aina tosi. Edelleen ehto $\texttt{x-1>0}$ on yhtäpitävä ehdon $\texttt{x>1}$ kanssa, joka esiintyy väitteessä.

Tehtävä 15.6

Tehtävän ratkaisuun tarvitaan edelläesitettyjen päättelysääntöjen lisäksi seuraava sääntö ehtolausekeelle:

$$\frac{[B_1\,\texttt{\&\&}\,B]\ C_1\ [B_2] \qquad [B_1\,\texttt{\&\&!}\,B]\ C_2\ [B_2]}{[B_1]\ \texttt{if}(B)\ \texttt{then}\,\{C_1\}\ \texttt{else}\,\{C_2\}\ [B_2]}$$

Pyritään osoittamaan $\texttt{z==}\min(\texttt{x},\texttt{y})$. Tämä on siis ylläolevan säännön ehto B_2. Tutkitaan komentoja C_1 ja C_2 erikseen. C_2:sta saadaan.

$$[\texttt{x ==} \min(\texttt{x},\texttt{y})]\ \texttt{z=x}\ [\texttt{z==}\min(\texttt{x},\texttt{y})]$$

Ehto $\texttt{x ==}\min(\texttt{x},\texttt{y})$ on yhtäpitävää lausekkeen $\texttt{x<=y}$ tai lausekkeen $\texttt{!(x>y)}$ kanssa. Luonnollisesti lauseke voidaan kirjoittaa myös muotoon $\texttt{true\&\&!(x>y)}$. Komennosta C_1 saadaan vastaavasti:

$$[\texttt{y} == \min(\texttt{x},\texttt{y})]\ \texttt{z=y}\ [\texttt{z} == \min(\texttt{x},\texttt{y})]$$

Ja edelleen samalla päättelyllä esiehdoksi `true&&(x>y)`. Nyt voidaan soveltaa ehtolausekkeen päättelysääntöä (viivan yläpuolella olevat lausekkeet on johdettu) ja saadaan:

```
[true]
if(x>y) then {
    z=y
} else {
    z=x
} [z == min(x, y)]
```

Tehtävä 15.8

Tehtävän a-kohdassa pitää todistaa muotoa $[B_1]$ `while(`B`)` $\{C\}$ $[B_2]$ oleva osittainen oikeellisuus. Tähän on annettu seuraava menettely:

A1. Valitaan I siten, että $\models_{\int}$ `(`I`&&!`B`)->`B_2.

A2. Haetaan heikoin esiehto I' siten, että $\models_p [I']\ C\ [I]$.

A3. Osoitetaan $\models_{\int}$ I`&&`B`->`I', minkä nojalla $\models_p$ $[I$`&&`$B]$ C $[I]$ ja edelleen $\models_p$ $[I]$ `while(`B`)` $\{C\}$ $[I$`&&!`$B]$.

A4. Osoitetaan $\models_{\int}$ B_1`->`I.

Menettelyssä I on invariantti, joka on aina voimassa silmukan lauseiden suorituksen jälkeen. Nyt silmukkaa tutkimalla havaitaan, että muuttujan z arvo kasvaa ja v pienenee, erityisesti siis niiden summa pysyy vakiona. Kun niille lisäksi annetaan alkuarvot x ja y on summa näiden vakioiden summan suuruinen. Olkoon siis I lauseke `z+v==x+y`. Nyt havaitaan, että menetelmän kohta A1 pätee, koska `!`B on lauseke `v==0`, josta luonnollisesti seuraa, että `z==x +y`. Lähdetään siis hakemaan silmukan komentojen heikoimpia esiehtoja. Saadaan:

$$[\texttt{z+v-1==x+y}]\ \texttt{v=v-1}\ [\texttt{z+v==x+y}]$$
$$[\texttt{z+1+v-1==x+y}]\ \texttt{z=z+1}\ [\texttt{z+v-1==x+y}]$$

Saadussa esiehdossa `+1` ja `-1` kumoutuvat, jolloin esiehto on sama kuin invariantti I. Menetelmän kohdassa A3 tulee osoittaa, että I`&&`B`->`I', so. lause:

$$\texttt{z+v==x+y\&\&!(v==0)} \rightarrow \texttt{z+v==x+y}$$

Tämä luonnollisesti pätee. Näin ollen pätee myös:

```
[z + v == x + y]
while(!(v == 0)) {
    z = z + 1;
    v = v - 1
} [z + v == x + y && v == 0]
```

Menetelmän kohta A4 redusoituu lauseen I `->` I todistamiseen. Todistuksen loppuunsaattamiseksi pitää vielä tutkia alun sijoituslauseet. Saadaan:

$$[\texttt{z+y==x+y}]\ \texttt{v=y}\ [\texttt{z+v==x+y}]$$
$$[\texttt{x+y==x+y}]\ \texttt{z=x}\ [\texttt{z+y==x+y}]$$

Ensimmäinen ehto `x+y==x+y` on luonnollisesti aina totta.

(b) $\models_t$ $[\texttt{0<=y}]\ \texttt{Sum}\ [\texttt{z==x+y}]$

Tehtävän b-kohdassa pyydetään todistamaan, että ohjelma myös päättyy ja että tällöin tarvitaan vahvempi esiehto. Täydellisen oikeellisuuden todistamisessa tarvitaan seuraavaa vahvempaa päättelysääntöä:

$$\frac{[B_1\ \texttt{\&\&}\ B_2\ \texttt{\&\&}\ \texttt{(}E\ \texttt{==}\ \texttt{n)}]\ C\ [B_1\ \texttt{\&\&}\ \texttt{(}E\ \texttt{<}\ \texttt{n)}]}{[B_1]\ \texttt{while(}B_2\texttt{)}\ \{C\}\ [B_1\ \texttt{\&\&}\ \texttt{!}B_2]}$$

Säännössä B_1 sisältää aiemman invariantin lisäksi vaatimuksen siitä, että kokonaislukulauseke E `>= 0`. Sääntö sanoo, että aina kun toistolausekkeen komentoja C suoritetaan invariantin ja toistolausekkeen ehdon ollessa voimassa niin valitaanpa kokonaislukumuuttujan `n` arvo miten tahansa, niin aina, kun esiehto on voimassa niin jälkiehto on myös. Jälkiehto puolestaan sanoo, että invariantti säilyy ja kokonaislukulauseke pienenee aidosti (säilyen kuitenkin ei-negatiivisena). Näin ollen komentojen C toistaminen johtaa väistämättä siihen, että toistolausekkeen ehto menee lopulta epätodeksi ja ohjelman suoritus täten päättyy.
Esimerkkiohjelmassa lausekkeeksi E voidaan valita `v`. Tällöin päättely komennoille C saa muodon:

$$[\texttt{z+v-1==x+y\&\&0<=v-1\&\&v-1<n}]\ \texttt{v=v-1}\ [\texttt{z+v==x+y\&\&0<=v\&\&v<n}]$$
$$[\texttt{z+v==x+y\&\&0<=v-1\&\&v-1<n}]\ \texttt{z=z+1}\ [\texttt{z+v-1==x+y\&\&0<=v-1\&\&v-1<n}]$$

Jotta päättelysääntöä voisi käyttää täytyy todistaa, että saatu esiehto on päättelysäännössä tarvittavan esiehdon $B_1\ \texttt{\&\&}\ B_2\ \texttt{\&\&}\ \texttt{(}E\ \texttt{==}\ \texttt{n)}$ looginen seuraus. Kyseinen esiehto saa muodon:

$$\texttt{z+v==x+y\&\&0<=v\&\&!(v==0)\&\&v == n}$$

Looginen seuraavuus pätee, koska muuttujalle `n` voidaan valita vain positiivisia arvoja, jotta vasen puoli saadaan todeksi. Näin ollen voidaan päätellä:

```
[z +v ==x +y &&0 <=v]
while(!(v ==0)){
    z=z+1;
    v=v-1
} [z +v ==x +y &&0 <=v &&v ==0]
```

Nyt `0<=v` on jälkiehdon totuusarvon kannalta luonnollisesti redundantti. Päättelyn loppuunsaattamiseksi pitää vielä tutkia alun sijoituslauseet:

$$[\texttt{z+y==x+y\&\&0<=y}]\ \texttt{v=y}\ [\texttt{z+v==x+y\&\&0<=v}]$$
$$[\texttt{x+y==x+y\&\&0<=y}]\ \texttt{z=x}\ [\texttt{z+y==x+y\&\&0<=y}]$$

Saatu esiehto redusoituu siis muotoon `0<=y` eli ohjelma päättyy vain jos muuttujan `y` arvo on ei-negatiivinen, kun ohjelman suoritus aloitetaan.