DD1350 Logik för dataloger

Rättningsmall till tentamen
15 december 2010, 16.15 - 18.00

Dilian Gurov
KTH CSC

Kravet för godkänt på tentan är att vara godkänd på båda E–delar **och** att ha deltagit i kamraträttningen.

Del 1E

1. Betrakta följande resonemang: 5p

   Bankomaten ger ut ett kvitto eller ger ett felmeddelande. Om det inte finns pengar i bankomaten, så ger den inte ut något kvitto. Därför finns det pengar i bankomaten.

   Föreslå en formalisering av resonemanget i form av en satslogisk *sekvent*, och visa att resonemanget är felaktigt genom att hitta en *motvaluering*.

   – Atomer och deras tolkning:

   p : bankomaten ger ut ett kvitto
   q : bankomaten ger ut ett felmeddelande
   r : det finns pengar i bankomaten

   – Sekvent:

   $$p \lor q,\ \neg r \to \neg p \ \vdash\ r$$

   – Motvaluering:

   $$\{p : F,\ q : T,\ r : F\}$$

   – Finns det fler motvalueringar? Svar: Nej.

   – Visa en *sanningsvärdestabell* för att motivera dina svar:

	p	q	r	$p \lor q$	$\neg r$	$\neg p$	$\neg r \to \neg p$
	T	T	T	T	F	F	T
	T	T	F	T	T	F	F
	T	F	T	T	F	F	T
	T	F	F	T	T	F	F
	F	T	T	T	F	T	T
$\to$	F	T	F	T	T	T	T
	F	F	T	F	F	T	T
	F	F	F	F	T	T	T

2. Presentera ett *bevis* i naturlig deduktion till följande sekvent: 5p

$$\exists x P(x) \to r \vdash \forall y\, (P(y) \to r)$$

Rita tydligt alla boxar för att visa räckvidden för alla antaganden och nya variabler i beviset.

Bevis:

1	$\exists x P(x) \to r$	premiss
2	y_0	
3	$P(y_0)$	antagande
4	$\exists x P(x)$	$\exists x$ i 3
5	r	$\to$e 4,1
6	$P(y_0) \to r$	$\to$i 3–5
7	$\forall y\, (P(y) \to r)$	$\forall y$ i 2–6

Del 2E

1. Induktiva BNF-definitionen av listor som termmängder ser ut så här: $\boxed{\text{5p}}$

$$\mathit{List} \ ::= \ \mathsf{empty} \mid \ \mathsf{cons}\,(\mathit{Letter}, \mathit{List})$$

Definiera *induktivt* funktionen $\mathbf{shuffle}\,(u, v)$ som blandar in två listor av samma längd. T.ex. är

$$\mathbf{shuffle}\,(\mathsf{cons}\,(a, \mathsf{cons}\,(b, \mathsf{empty})),\ \mathsf{cons}\,(c, \mathsf{cons}\,(d, \mathsf{empty})))$$

lika med

$$\mathsf{cons}\,(a, \mathsf{cons}\,(c, \mathsf{cons}\,(b, \mathsf{cons}\,(d, \mathsf{empty}))))$$

– Induktiv definition (Tips: induktionen borde vara över *båda* argumenten!):

$$\begin{aligned} \mathbf{shuffle}\,(\mathsf{empty},\ \mathsf{empty}) &\stackrel{\mathsf{def}}{=} \mathsf{empty} \\ \mathbf{shuffle}\,(\mathsf{cons}\,(a, u),\ \mathsf{cons}\,(b, v)) &\stackrel{\mathsf{def}}{=} \mathsf{cons}\,(a, \mathsf{cons}\,(b, \mathbf{shuffle}\,(u, v))) \end{aligned}$$

Använd din definition för att *stegvis* beräkna:

$$\mathbf{shuffle}\,(\mathsf{cons}\,(f, \mathsf{cons}\,(o, \mathsf{empty})),\ \mathsf{cons}\,(i, \mathsf{cons}\,(l, \mathsf{empty})))$$

– Stegvis beräkning (OBS: slutresultatet måste vara en korrekt lista!):

$$\begin{aligned} & \mathbf{shuffle}\,(\mathsf{cons}\,(f, \mathsf{cons}\,(o, \mathsf{empty})),\ \mathsf{cons}\,(i, \mathsf{cons}\,(l, \mathsf{empty}))) \\ = \ & \mathsf{cons}\,(f, \mathsf{cons}\,(i,\ \mathbf{shuffle}\,(\mathsf{cons}\,(o, \mathsf{empty})),\ \mathsf{cons}\,(l, \mathsf{empty}))) \\ = \ & \mathsf{cons}\,(f, \mathsf{cons}\,(i,\ \mathsf{cons}\,(o, \mathsf{cons}\,(l,\ \mathbf{shuffle}\,(\mathsf{empty}, \mathsf{empty}))))) \\ = \ & \mathsf{cons}\,(f, \mathsf{cons}\,(i,\ \mathsf{cons}\,(o, \mathsf{cons}\,(l,\ \mathsf{empty})))) \end{aligned}$$

2. Betrakta följande beteendeegenskap för bankomater: $\boxed{\text{5p}}$

   Så småningom, dvs oavsett hur man interagerar med bankomaten, kommer man kunna vara aktiv för all framtid.

   Föreslå en formalisering av egenskapen i form av en CTL–formel, där du använder atomen active.

   – CTL formel:

$$\mathsf{AF\ EG\ active}$$

   Låt $Atoms \stackrel{\mathsf{def}}{=} \{\mathsf{entry}, \mathsf{active}\}$, och låt $\mathcal{M}$ vara modellen definierad som:

$$\begin{array}{rcl} S & \stackrel{\mathsf{def}}{=} & \{s_0, s_1, s_2, s_3\} \\ \rightarrow & \stackrel{\mathsf{def}}{=} & \{(s_0, s_1), (s_1, s_1), (s_1, s_2), (s_2, s_3), (s_3, s_2), (s_3, s_3), (s_3, s_0)\} \\ L & : & s_0 \mapsto \{\mathsf{entry}\} \\ & & s_1 \mapsto \{\} \\ & & s_2 \mapsto \{\mathsf{active}\} \\ & & s_3 \mapsto \{\mathsf{active}\} \end{array}$$

   – Gäller beteendeegenskapen du formaliserade i tillståndet s_0? Motivera ditt svar genom att hänvisa till CTLs semantik:

   Nej, egenskapen gäller inte, därför att i stigen
   $s_0 \rightarrow s_1 \rightarrow s_1 \rightarrow s_1 \rightarrow \ldots$
   man *inte* kommer till något tillstånd där $\mathsf{EG\ active}$ gäller;
   notera att $\mathsf{EG\ active}$ bara gäller i s_2 och s_3.

3. Skriv en *specifikation* i form av en Hoare–trippel till ett program Pow som beräknar funktionen x^{2^y} för positiva heltal x och y. Det skall vara entydigt från specifikationen hur programmet ska användas *utan* att känna till själva koden. $\boxed{\text{5p}}$

– Specifikation med Hoare–trippel:

$$(\!|\ x > 0 \land y > 0 \land x = x_0 \land y = y_0\ |\!)\ \mathsf{Pow}\ (\!|\ \mathsf{z} = \mathsf{x_0}^{2^{\mathsf{y_0}}}\ |\!)$$

Implementera Pow, dvs skriv kod till Pow så att den uppfyller din specifikation. (Tips: du kan använda iterativ kvadrering.)

– Program:

```
z = x;
while (y > 0) {
   z = z * z;
   y = y - 1;
}
```

Del 2C

1. Induktiva definitionen av längden på listor $\mathbf{length}\,(u)$ ser ut så här: $\boxed{9\text{p}}$

$$\begin{aligned}\mathbf{length}\,(\mathsf{empty}) &\stackrel{\mathsf{def}}{=} 0\\ \mathbf{length}\,(\mathsf{cons}\,(a,u)) &\stackrel{\mathsf{def}}{=} 1+\mathbf{length}\,(u)\end{aligned}$$

Använd din definition på $\mathbf{shuffle}\,(u,v)$ från uppgift 2E.1 och bevisa med *strukturell induktion* att:

$$\forall u\,(\mathbf{length}\,(\mathbf{shuffle}\,(u,u)) = 2\cdot\mathbf{length}\,(u))$$

– Bevis med strukturell induktion (OBS: *inte* med fullständig induktion!):

- Fall $u = \mathsf{empty}$
  Vi har:

$$\begin{aligned} & \mathbf{length}\,(\mathbf{shuffle}\,(\mathsf{empty},\ \mathsf{empty})) & \\ = \;& \mathbf{length}\,(\mathsf{empty}) & \{\text{Def. }\mathbf{shuffle}\}\\ = \;& 0 & \{\text{Def. }\mathbf{length}\}\\ = \;& 2\cdot 0 & \{\text{Aritmetik}\}\\ = \;& 2\cdot\mathbf{length}\,(\mathsf{empty}) & \{\text{Def. }\mathbf{length}\}\end{aligned}$$

- Fall $u = \mathsf{cons}\,(a,u')$
  Antag $\mathbf{length}\,(\mathbf{shuffle}\,(u',u')) = 2\cdot\mathbf{length}\,(u')$ (Induktionshypotes)
  Vi har:

$$\begin{aligned} & \mathbf{length}\,(\mathbf{shuffle}\,(\mathsf{cons}\,(a,u'),\ \mathsf{cons}\,(a,u'))) & \\ = \;& \mathbf{length}\,(\mathsf{cons}\,(a,\mathsf{cons}\,(a,\mathbf{shuffle}\,(u',u')))) & \{\text{Def. }\mathbf{shuffle}\}\\ = \;& 1+\mathbf{length}\,(\mathsf{cons}\,(a,\mathbf{shuffle}\,(u',u'))) & \{\text{Def. }\mathbf{length}\}\\ = \;& 1+1+\mathbf{length}\,(\mathbf{shuffle}\,(u',u')) & \{\text{Def. }\mathbf{length}\}\\ = \;& 1+1+2\cdot\mathbf{length}\,(u') & \{\text{Induktionshypotes}\}\\ = \;& 2\cdot(1+\mathbf{length}\,(u')) & \{\text{Aritmetik}\}\\ = \;& 2\cdot\mathbf{length}\,(\mathsf{cons}\,(a,u')) & \{\text{Def. }\mathbf{length}\}\end{aligned}$$

$\square$

2. För modellen från uppgift 2E.2, förklara intuitivt, med hänvisning till CTLs semantik, varför CTL–formeln $\boxed{\text{6p}}$

$$\mathsf{EF\ EG\ (active \land EX\ entry)}$$

gäller i tillstånd s_0.

– Intuitiv förklaring:

> Formeln gäller, därför att det finnst en stig, nämligen
> $s_0 \longrightarrow s_1 \longrightarrow s_2 \longrightarrow s_3 \longrightarrow s_3 \longrightarrow s_3 \longrightarrow \ldots$
> där man kommer till ett tillstånd, nämligen s_3,
> där $\mathsf{EG\ (active \land EX\ entry)}$ gäller, därför att
> $\mathsf{active \land EX\ entry}$ gäller i alla senare tillstånd i samma stig;
> notera att $\mathsf{active \land EX\ entry}$ bara gäller i s_3.

Utgå från detta för att konstruera det kortaste möjliga formella bevis du kan i bevissystemet för CTL.

– Bevis i form av bevisträd (OBS: glöm inte att ange reglernas namn i beviset!):

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{-}{\mathcal{M}, s_3 \vdash_{[\,]} \mathsf{active}}\ \mathsf{active}
\qquad
\dfrac{\dfrac{-}{\mathcal{M}, s_0 \vdash_{[\,]} \mathsf{entry}}\ \mathsf{entry}}{\mathcal{M}, s_3 \vdash_{[\,]} \mathsf{EX\ entry}}\ \mathsf{EX}
}{\mathcal{M}, s_3 \vdash_{[\,]} \mathsf{active \land EX\ entry}}\ \land
\qquad
\dfrac{-}{\mathcal{M}, s_3 \vdash_{s_3} \mathsf{EG\ (active \land EX\ entry)}}\ \mathsf{EG}_1
}{\mathcal{M}, s_3 \vdash_{[\,]} \mathsf{EG\ (active \land EX\ entry)}}\ \mathsf{EG}_2
}{\mathcal{M}, s_3 \vdash_{s_2, s_1, s_0} \mathsf{EF\ EG\ (active \land EX\ entry)}}\ \mathsf{EF}_1
}{\mathcal{M}, s_2 \vdash_{s_1, s_0} \mathsf{EF\ EG\ (active \land EX\ entry)}}\ \mathsf{EF}_2
}{\mathcal{M}, s_1 \vdash_{s_0} \mathsf{EF\ EG\ (active \land EX\ entry)}}\ \mathsf{EF}_2
}{\mathcal{M}, s_0 \vdash_{[\,]} \mathsf{EF\ EG\ (active \land EX\ entry)}}\ \mathsf{EF}_2
$$