Föreläsning 6 i ADK

Korrekthetsbevis

Stefan Nilsson

KTH

Korrekthet

Bevis av att ett program uppfyller sin specifikation.

Specifikation av ett (del-)programs funktion:

- Ingångsvilkor **Pre** som måste vara uppfyllt då programmet startas. (Förutsättning)
- Utgångsvilkor **Post** som måste vara uppfyllt då programmet avslutas.

Programbevis:

- Matematiskt/logiskt bevis av att om **PRE** är sant och programmet exekveras till slut så kommer sedan **POST** att vara sant.

$$\textbf{PRE}\ \{\text{program}\}\ \textbf{POST}$$

Det är omöjligt att skriva ett program som bevisar att ett program är korrekt!

Grader av korrekthet

Partiell korrekthet

- För varje indata som uppfyller **PRE** så kommer programmet antingen att avslutas med **POST** uppfyllt eller att aldrig avslutas.

Total korrekthet

- För varje indata som uppfyller **PRE** så kommer programmet att avslutas och **POST** att vara uppfyllt

Det är oftast enklast att först visa partiell korrekthet och sedan visa att programmet alltid avslutas för korrekta indata

Slingor och rekursioner bryts $\Rightarrow$ programmet avslutas

Studera ett heltalsuttryck som minskar (ökar) i varje varv i slingan/rekursivt anrop och som har en undre (övre) absolut gräns!

Tips för programbevisning

- Specificera varje procedurs (önskade) beteende med ingångs- och utgångsvillkor.
- Specificera slingor med invarianter. Invarianten ska vara sann **precis innan** slingan börjar och **efter varje varv** i slingan.
- Specificera varje viktigt läge med en **försäkran** (assertion)

Exempel:

PRE A
kod1
while ... **do** INV B
  kod2
kod3
ASSERT C
kod4
POST D

Bevisa följande:

A {kod1} B
B {kod2} B
B {kod3} C
C {kod4} D

- Gräv inte ner dig i detaljer!