

First Experiences in KIV – Verification



Augsburg, 26.11.2001, Mar Marcos, Michael Balser

- Termination

$$\begin{array}{ll} \text{Regular-treatments}\#(\mathbf{var} \text{ time}, \dots), & \text{System} \\ \Box \text{ time}'' = \text{time}' + 1 & \text{Environment} \\ \vdash \Diamond \mathbf{last} & \text{Property} \end{array}$$

- Intention

$$\begin{array}{ll} \text{Regular-treatments}\#(\mathbf{var} \text{ time}, \text{tsb}, \dots), & \text{System} \\ \Box \text{ time}'' = \text{time}' + 1, & \text{Environment} \\ \vdash \text{get-bilirubin}(\text{tsb}) \neq \text{transfusion} \mathbf{until last} & \text{Property} \end{array}$$

Modelling of EFFECTS?

Goal

Apply standard KIV proof method of

Symbolic Execution with a Little Induction
--

to ASBRU plans

Principle

1. Execute steps of ASBRU plans one after the other
2. Use induction, if execution loops

KIV enhancements

- proof support for new program constructs
- example proof rule

$$\frac{\varepsilon, \mathbf{last}, \Gamma \vdash \Delta \quad x := \tau; \mathbf{break} \ \alpha \ \mathbf{if} \ \varepsilon, \Gamma \vdash \varepsilon, \Delta}{\mathbf{break} \ x := \tau; \alpha \ \mathbf{if} \ \varepsilon, \Gamma \vdash \Delta} \textit{apar left}$$

proof rules related to operational semantics

First try

Executing top level plan with call to sub plans, if necessary

⇒ Verification too complicated!

Modular Approach

Verification bottom-up:

- verify atomic plans (with adjusted property)
- apply results to verify larger plans

Implemented modular proof method in KIV

Assumption-Guarantee Proofs

⇒ Verification of large ASBRU plans is feasible

Verification – Current Standings (1)



Treatment-hyperbilirubinemia

Regular-treatments

Feeding-alternatives

Breastfeeding

Breastfeeding-with-formula

Formula-only

Phototherapy-intensive

Prescribe-intensive-phototherapy

Phototherapy-normal-prescription

Prescribe-normal-phototherapy

Phototherapy-normal-recommended

Observation

Prescribe-observation

Exchange-transfusion

Prescribe-exchange-transfusion

Jaundice

- termination partly verified
- first steps in verification of intention

Protocure

Protocure goal

verification of some properties for two ASBRU protocols

should be possible

Results

- part of verification of termination finished
- verification of ASBRU is feasible
- KIV has been improved (modular proof method)

Next steps

- discuss: modelling of effects
- missing proof rules for some ASBRU constructs
- automation of proofs
- lots of KIV enhancements possible
 - ★ more ASBRU constructs
 - ★ more comfortable verification