



Verification of Jaundice and Diabetes Protocols – Report



Castellon, September 17th, 2002

Michael Balser, Christoph Duelli, Mar Marcos,
Annette ten Teije, Peter Lucas

Overview (1)



Properties in Jaundice

- Termination
- 2 Intentions
- MAJIC indicator

Properties in Diabetes

- “No more than two drugs at the same time”

Overview (2)



Termination

- Phototherapy-intensive
- Phototherapy-normal-recommendation
- Phototherapy-normal-prescription
- Observation
- Feeding-alternatives
- Regular-treatments

Intentions

- Phototherapy-intensive (time annotation)
- Phototherapy-normal-prescription (no time annotation)

Indicator

- Regular-treatments
- Lemmas for sub plans

Overview (2)



Termination

- Phototherapy-intensive
- Phototherapy-normal-recommendation
- Phototherapy-normal-prescription
- Observation
- Feeding-alternatives
- Regular-treatments

Intentions

- Phototherapy-intensive (time annotation)
- Phototherapy-normal-prescription (no time annotation)

Indicator

- Regular-treatments
- Lemmas for sub plans

No verification for Diabetes

Indicator – Wrong version



Informal

“Only one more measurement after phototherapy is started”

Formal

Phototherapy-intensive#(; ...)

$\wedge \neg pd \text{ .under-phototherapy}$

$\wedge pd'' \text{ .under-phototherapy} \leftrightarrow pd' \text{ .under-phototherapy}$

$\wedge pd'' \text{ .tsb} \neq pd' \text{ .tsb} \wedge T_0 = t'$

$\rightarrow \bullet \square pd'' \text{ .tsb} \neq pd' \text{ .tsb} \rightarrow t' - T_0 \geq 12$

unless last

$\rightarrow \square pd \text{ .under-phototherapy} \wedge pd'' \text{ .tsb} \neq pd \text{ .tsb}$

$\rightarrow (pd'' \text{ .tsb} = pd \text{ .tsb} \textbf{ unless } \neg pd \text{ .under-phototherapy})$

Indicator – Right version



Informal

”Only one more measurement after phototherapy is **discontinued**”

Formal

Regular-treatments#(; ...)

$$\begin{aligned} \wedge \quad & pd'' .\text{under-phototherapy} \leftrightarrow pd' .\text{under-phototherapy} \\ & \wedge pd'' .\text{tsb} \neq pd' .\text{tsb} \wedge T_0 = t' \\ \rightarrow \bullet \quad & \square pd'' .\text{tsb} \neq pd' .\text{tsb} \rightarrow t' - T_0 \geq 12 \end{aligned}$$

unless last

$$\begin{aligned} \rightarrow \square \quad & pd .\text{under-phototherapy} \wedge \neg pd' .\text{under-phototherapy} \\ & \wedge pd .\text{tsb} = TSB_0 \\ \rightarrow \square \quad & pd .\text{tsb} = TSB_1 \wedge TSB_1 \neq TSB_0 \rightarrow pd .\text{tsb} \neq TSB_1 \end{aligned}$$

Indicator – Modular Approach (1st Try)



Lemma ob-no-tsb-readings

$\text{Observation\#}(\dots) \rightarrow ((pd' .tsb = pd .tsb \text{ unless last})$

Steps

- Lemmas verified
- Proof attempt for Regular-treatments

Indicator – Modular Approach (1st Try)



Lemma ob-no-tsb-readings

$\text{Observation\#}(\dots) \rightarrow ((pd' .tsb = pd .tsb \text{ unless last})$

Steps

- Lemmas verified
- Proof attempt for Regular-treatments

Result 1: Lemmas not strong enough

More information is needed about behaviour of **Observation**

Indicator – Modular Approach (1st Try)



Lemma ob-no-tsb-readings

$\text{Observation}\#(\dots) \rightarrow ((pd' .tsb = pd .tsb \text{ unless last})$

Steps

- Lemmas verified
- Proof attempt for Regular-treatments

Result 1: Lemmas not strong enough

More information is needed about behaviour of **Observation**

Result 2: Plan does not satisfy indicator

E.g.: **Observation** must not run longer than 24 hours.

Indicator – Assumptions



Assumption (1)

If phototherapy is discontinued, TSB (reading) will be **observation**.

Assumption (2)

Observation will run for less than 24 hours.

Assumption (3)

After phototherapy and observation, TSB (reading) will still be **observation**.

Indicator – Assumptions



Assumption (1)

If phototherapy is discontinued, TSB (reading) will be **observation**.

Assumption (2)

Observation will run for less than 24 hours.

Assumption (3)

After phototherapy and observation, TSB (reading) will still be **observation**.

Assumptions in addition to behaviour of plans!

Indicator – Modular Approach (2nd Try)



Lemma for Observation, v2

- ob-no-tsb-readings
- Assumptions (2), (3)

Indicator – Modular Approach (2nd Try)



Lemma for Observation, v2

- ob-no-tsb-readings
- Assumptions (2), (3)

⇒ Still not strong enough

Which behaviour of sub plan is relevant for property?

Indicator – Modular Approach (2nd Try)



Lemma for Observation, v2

- ob-no-tsb-readings
- Assumptions (2), (3)

⇒ Still not strong enough

Which behaviour of sub plan is relevant for property?

⇒ Too difficult to guess lemma

Indicator – Non-Modular Approach



Strategy

1. Let heuristics do proof
2. Keep track of case distinctions
3. Follow the most interesting branch

⇒ Strategy similar to interpreter

Results

- Error in formalization of Assumption (2)
- Environment assumption not strong enough
- 2 Errors in KIV formalization of **Observation**

⇒ Method to find environment assumption

Indicator – Generalization



Partial proof

- Proof with 1400 steps
- Restricted to main path of execution
- 120 open goals

Indicator – Generalization



Partial proof

- Proof with 1400 steps
- Restricted to main path of execution
- 120 open goals

Proven cases help in finding lemmas

Strategy

1. Analyze proven cases
2. Generalize cases to receive lemmas
3. Apply lemmas to other cases

Indicator – Generalization



Partial proof

- Proof with 1400 steps
- Restricted to main path of execution
- 120 open goals

Proven cases help in finding lemmas

Strategy

1. Analyze proven cases
2. Generalize cases to receive lemmas
3. Apply lemmas to other cases

Progress

- 5 lemmas generated
- 40 (of 120) open goals closed

Indicator – Lessons Learned



- (The only major) proof is not finished

Indicator – Lessons Learned



- (The only major) proof is not finished

Proof strategy is simple, proofs are not

Necessary KIV enhancements

- Reuse of temporal proofs!
- More automation
- Automatic generalization (?)

Indicator – Lessons Learned



- (The only major) proof is not finished

Proof strategy is simple, proofs are not

Necessary KIV enhancements

- Reuse of temporal proofs!
- More automation
- Automatic generalization (?)

Proof will not be finished during this assessment project!



Formalisation:

- Starting point: (semi-automatic) formalisation by Vienna/Augsburg
- Observations:
 - ★ missing time annotations
 - ★ problems with nested plans: e.g. missing continuation specification
 - ★ errors in list processing plans
 - ★ uneven translation of “do one” plans (any-order, wait-for one, and activate-mode manual subplans)

⇒ further revision was necessary



Verification:

- Starting point: list of properties by CBO
- Target property: combination of SU derivative, metformin and acarbose is not recommended
 - ★ *a priori*, non-trivial
 - ★ finally, trivially verified in the original/Asbru protocol
- Rest of properties:
 - ★ trivially satisfied/violated in the original protocol
 - ★ trivially satisfied/violated in the Asbru protocol
 - ★ not applicable

Results (1)



Main result

Jaundice protocol satisfies one of MAJIC indicators only under additional assumptions.

Assumptions

1. If phototherapy is discontinued, TSB (reading) is **observation**.
2. Observation for less than 24 hours.
3. After Phototherapy and observation, TSB (reading) is **observation**

Informal protocol can be improved

- Add assumptions, if approved by experts
- Change protocol, if assumptions too strong

Results (2)



Termination

- Proof failed

⇒ Assumption necessary?

Intentions

- Intentions hold for basic plans
- Problem with missing time annotation not detected

Results (3)



Improved formalization of Asbru plans

- Predicates for different conditions
- Ideas for separating state management from plans

Improved formalization of intentions

MAINTAIN INTERMEDIATE STATE φ

$$\begin{aligned} &\square \quad \langle plan \rangle\text{-state} = \text{activated} \\ &\quad \wedge (\text{last} \vee \langle plan \rangle\text{-state}' \neq \text{aborted}) \\ &\rightarrow \varphi \end{aligned}$$

Results (3)



Improved formalization of Asbru plans

- Predicates for different conditions
- Ideas for separating state management from plans

Improved formalization of intentions

MAINTAIN INTERMEDIATE STATE φ

$$\begin{aligned} &\square \quad \langle plan \rangle\text{-state} = \text{activated} \\ &\quad \wedge (\text{last} \vee \langle plan \rangle\text{-state}' \neq \text{aborted}) \\ &\rightarrow \varphi \end{aligned}$$

Proof patterns are possible

Results (4)



Improvement of proof strategy for Asbru

- Modular approach too difficult
- Strategy for generation of lemmas

KIV improvements

- Support for complex operators
- More comfortable proofs
- Heuristics