

1 Procedure and Process Models

Vorgehens- und Prozessmodelle

Problem 1.1 (Procedure Models)

Aufgabe 1.1 (Vorgehensmodelle)

- Write down the procedure underlying the spiral model.

Geben Sie die Schritte der dem Spiralmodell zugrundeliegende Prozedur an.

- Why is it called spiral model? Where is the spiral? Explain!

Warum wird das Spiralmodell "Spiralmodell" genannt? Wo ist die Spirale? Erläutern Sie!

Correction:

- 0.5 points for each item of the procedure
- 1 point for correct answer (reduce 0.5 if too imprecise)

Spiralmodell:

- - determine Risks \rightarrow if $R = \emptyset \Rightarrow$ yes
 - assign Risk value to Risk
 - max(Risk) \rightarrow determine Risk \rightarrow if $\forall R \neq \emptyset \Rightarrow$ yes
- - goes in circles
 - if also technical incorrect it becomes a spiral (spiral)

Time goes on over time

Problem 1.2 (V-Modell XT)

Aufgabe 1.2 (V-Modell XT)

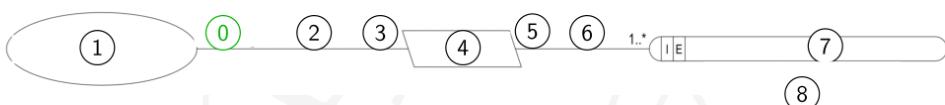


Figure 1: Elements of V-Modell XT.

Abbildung 1: Elemente des V-Modell XT.

Assign the following eight labels to their correct place in Figure 1 (similar to the example "0" in green).¹
Weise die folgenden acht Beschriftungen ihrem korrekten Platz in Abbildung 1 zu (analog dem Beispiel "0" in grün).

0	1..*	5	*	3	1..*	G	benötigt needs	4	Entscheidungspunkt decision point	7	Produkt Product
R [im Zustand 'fertig gestellt'] [in state 'completed']						2	legt Reihenfolge fest determines order/seq.				
1	Projektdurchführungsstrategie project conduction strategy						(2)				

Correction:

- 0.25 points per correct label
- putting two labels A and B at one place counts as the one label "A B", which is wrong

¹In the lecture, we considered figures from the German V-Modell XT document with ad-hoc translations to English.

Problem 2.1 (Lines of Code)

Aufgabe 2.1 (Anzahl Codezeilen)

```
1 public int convert(char[] str) throws Exception {  
2     if (str.length > 6)  
3         throw new Exception("Length exceeded");  
4  
5     int number = 0;  
6     int digit;  
7     int i = 0;  
8  
9     // none of the early submitters found this bug! :-)  
10    //  
11    if (str[0] == '-')  
12        i = 1;  
13  
14    while (i < str.length){  
15        digit = str[i] - '0';  
16        if (digit < 0 || digit > 9)  
17            throw new Exception("Invalid character");  
18        number = number * 10 + digit;  
19        i = i + 1;  
20    }  
21  
22    if (str[0] == '-)  
23        number = -number;  
24  
25    if (number > 32767 || number < -32768)  
26        throw new Exception("Range exceeded");  
27  
28    return number;  
29}
```

Figure 2: Function convert.

Abbildung 2: Funktion convert.

Consider the function convert shown in Figure 2.

- (i) Which lines (line numbers) contribute to the program size of convert? $\{1..29\} \setminus \{11\}$
- (ii) What is the net program size of convert? $29 - 6 = 23$
Which lines do not contribute to the net program size of convert? $\{1, 8, 13\}$
- (iii) What is the code size of convert? $23 - 2 = 21$
Which lines do not contribute to the code size of convert? $\{9, 10, 15 + \{11\}\}$

3 Decision Tables

Entscheidungstabellen

<i>T</i> : registration	<i>r</i> ₁	<i>r</i> ₂	<i>r</i> ₃	<i>r</i> ₄
<i>c</i> ₁ already registered	×	-	-	×
<i>c</i> ₂ $n < n_{\max}$	*	×	-	*
<i>c</i> ₃ delayed payments	*	-	-	×
<i>a</i> ₁ message: "already registered"	×	-	-	-
<i>a</i> ₂ message: "fully booked"	-	-	×	-
<i>a</i> ₃ message: "payment reminder"	-	-	-	×
<i>a</i> ₄ register applicant	-	×	-	-

Figure 3: Decision table.
Abbildung 3: Entscheidungstabelle.

Problem 3.1 (Analysing Decision Tables)

Aufgabe 3.1 (Analyse von Entscheidungstabellen)

Consider the decision table for a registration procedure as shown in Figure 3. In some cases, if applicants receive a message anyway, that message should be combined with a payment reminder if there are delayed payments. The maximum number of registrations is n_{\max} , the current number of registrations n .

Betrachten Sie die Entscheidungstabelle für eine Registrierungsprozedur in Abbildung 3. In einigen Fällen, in denen Antragsteller eh eine Nachricht bekommen, soll diese Nachricht mit einer Zahlungserinnerung kombiniert werden, falls Zahlungen ausstehen. Maximal können n_{\max} Registrierungen vorgenommen werden, n bezeichnet die aktuelle Anzahl an Registrierungen.

- (i) Is *T* as given in Figure 3 complete?

Prove your claim by giving a counter-example or a proof of completeness, respectively.

Ist *T* in Abbildung 3 vollständig?

Beweisen Sie Ihre Behauptung durch ein Gegenbeispiel bzw. einen Beweis der Vollständigkeit.

(2)

Correction:

- $\frac{2}{N}$ points for the correct answer, and for each of the *N* parts of the argumentation (example or proof)

- (ii) Is *T* as given i

Prove your cla

Ist *T* in Abbild
Beweisen Sie II

Correction:

- $\frac{2}{N}$ point

- (iii) The customer
a positive con
other message

Der Kunde hat
tion", also bere

anderen Nachrichten. Wird dieser Grundsatz von *T* in der Sammelsemantik garantiert? Erläutern Sie!

(1)

- max. 1 point for correct answer and explanation

(i)

<i>c</i> ₁	<i>c</i> ₂	<i>c</i> ₃	<i>c</i> ₁	<i>c</i> ₂	<i>c</i> ₃	<i>r</i> ₁	<i>r</i> ₂	<i>r</i> ₃	<i>r</i> ₄
0	0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0
0	1	1	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0
1	1	1	1	0	0	0	0	0	0
1	1	1	1	1	0	0	0	0	0

Andere Methode

1	0	0	1	?	?	0	1
1	0	1	1	0	?	0	1
1	1	0	1	?	?	0	1
1	1	1	1	0	?	0	1

für $c_1 = 0$

$c_2 = 0$

$c_3 = 1$

- (iii) The customer in addition stated that payment reminders should be combined with "other messages with a positive connotation", i.e. being already registered or having been successfully registered, but not with other messages. Is this policy ensured by T in the collecting semantics? Explain!

Der Kunde hat zusätzlich geäußert, daß Zahlungserinnerungen mit "anderen Nachrichten mit positiver Konnotation", also bereits registriert sein oder erfolgreich registriert worden sein, kombiniert werden sollen, aber nicht mit anderen Nachrichten. Wird dieser Grundsatz von T in der Sammelsemantik garantiert? Erläutern Sie!

(1)

- max. 1 point for correct answer and explanation

7(1n4)

c_1	c_2	c_3	c_1	$1 \wedge 1 \wedge 2 \wedge 3$	$1 \wedge 1 \wedge 2 \wedge 3$	$c_1 \wedge c_3$	$1 \wedge (1 \wedge 2)$	$1 \wedge (2 \wedge 3)$	$1 \wedge (1 \wedge 3)$	$1 \wedge \overline{1}$
0	0	0	0	0	1	0	1	1	1	1
0	0	1	0	0	0	0	1	0	1	1
0	1	0	1	0	0	0	1	1	1	1
0	1	1	0	0	0	0	1	1	1	1
1	0	0	1	0	0	1	1	1	1	1
1	0	1	1	0	0	1	1	1	1	1
1	1	0	1	0	0	1	1	1	1	1
1	1	1	1	0	0	1	1	1	1	1
1	h	h	1	0	0	1	1	1	1	1

\Rightarrow nicht deterministisch für $c_1 = 1$

$c_2 = 0$

$c_3 = 1$

- (iii) The customer in addition stated that payment reminders should be combined with "other messages with a positive connotation", i.e. being already registered or having been successfully registered, but not with other messages. Is this policy ensured by T in the collecting semantics? Explain!

Der Kunde hat zusätzlich geäußert, daß Zahlungserinnerungen mit "anderen Nachrichten mit positiver Konnotation", also bereits registriert sein oder erfolgreich registriert worden sein, kombiniert werden sollen, aber nicht mit anderen Nachrichten. Wird dieser Grundsatz von T in der Sammelsemantik garantiert? Erläutern Sie!

(1)

- max. 1 point for correct answer and explanation

(iii)

c_1	c_2	c_3	c_1	$c_1 \wedge c_2 \wedge c_3$	$c_1 \wedge c_2 \wedge \neg c_3$	$c_1 \wedge \neg c_2 \wedge c_3$	$\neg c_1 \wedge c_2 \wedge c_3$
0	0	0	0	0	1	0	0
0	0	1	0	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	0	0	0	0	0
1	0	0	1	0	0	0	0
1	0	1	0	0	0	0	0
1	1	0	0	0	0	0	0
1	1	1	0	0	0	0	0

\Rightarrow Darstellen von
moral
grödzen
und
Rationalität
und
Berechtigung

Einer deckt die Rech
menken auf

$$h = \sum_{(a_2, a_3), (a_3, a_2)} \text{grödzen} \cdot \text{Rationalität}$$

T : registration		r_1	r_2	r_3	r_4
c_1	already registered	\times	-	-	\times
c_2	$n < n_{\max}$	*	\times	-	*
c_3	delayed payments	*	-	-	\times
a_1	message: "already registered"	\times	-	-	-
a_2	message: "fully booked"	-	-	\times	-
a_3	message: "payment reminder"	-	-	-	\times
a_4	register applicant	-	\times	-	-

Collisions

T: registration		r_1	r_2	r_3	r_4
c_1	already registered	×	-	-	×
c_2	$n < n_{\max}$	*	×	-	*
c_3	delayed payments	*	-	-	×
a_1	message: "already registered"	○	×	-	-
a_2	message: "fully booked"	-	-	×	-
a_3	message: "payment reminder"	-	-	○	×
a_4	register applicant	-	×	-	-

Determinismus

T: registration		r_1	r_2	r_3	r_4
c_1	already registered	×	-	-	×
c_2	$n < n_{\max}$	*	×	-	*
c_3	delayed payments	*	-	-	×
a_1	message: "already registered"	○	×	-	-
a_2	message: "fully booked"	-	-	×	-
a_3	message: "payment reminder"	-	-	-	×
a_4	register applicant	-	×	-	-

Prämissen Teilmen konträr:
 \Rightarrow Nein

(prämissen disjunkt)

Problem 3.2 (Writing Decision Tables)

Aufgabe 3.2 (Entscheidungstabellen Erstellen)

Gathering requirements for the software of a new heating controller yielded the following statements by the customer:

- If the room temperature is below target temperature (condition c_1), shift to the next higher heating level (action a_1).
- If the room temperature is above the target temperature (condition c_2), shift to the next lower heating level (action a_2).
- When the “power heating” button is pushed (condition c_3), and the room temperature is not above the target temperature, shift to the next higher heating level.
- If room is neither above nor below the target temperature, and if “power heating” is not pressed, do not change heating level.

Eine erste Anforderungsanalyse für das Programm eines neuen Steuerungsgeräts einer Heizungsanlage hat die folgenden Aussagen des Kunden ergeben:

- Wenn die Raumtemperatur unterhalb der Zieltemperatur liegt (Bedingung c_1), schalte in die nächsthöhere Heizstufe (Aktion a_1).
- Wenn die Raumtemperatur oberhalb der Zieltemperatur liegt (Bedingung c_2), schalte in die nächstniedrigere Heizstufe (Aktion a_2).
- Wenn der “schnell aufheizen”-Knopf gedrückt wird (Bedingung c_3) und die Raumtemperatur nicht oberhalb der Zieltemperatur liegt, schalte in die nächsthöhere Heizstufe.
- Wenn die Raumtemperatur weder oberhalb noch unterhalb der Zieltemperatur liegt und der “schnell aufheizen”-Knopf nicht gedrückt ist, ändere die Heizstufe nicht.

- (i) Provide a decision table which formalises these requirements.

Formalisiere Sie die Anforderungen mit Hilfe einer Entscheidungstabelle.

(4)

Correction:

- one point per correct rule

	c_1	c_2	c_3	a_1	a_2	c_4
c_1 \leftarrow	X	-	-	-	-	-
c_2 \rightarrow	-	X	-	-	-	-
c_3 push	*	*	X	X	-	-
a_1	X	-	-	X	-	-
a_2	-	X	-	-	-	-

Nur

$$c_1 = 1$$

conflict action:

für

$$c_2 = 1$$

$$\neg (c_1 \wedge c_2)$$

$$c_3 = \frac{1}{0}$$

(ii) Analyse the requirements for completeness by checking the resulting decision table for completeness.

If the decision table is complete, provide a proof; if not, propose an environment assumption in the form of a conflict axiom (which is consistent with all existing rules in the table) such that the decision table is complete with respect to the conflict axiom.

Analysieren Sie die Anforderungen auf Vollstndigkeit indem Sie die resultierende Entscheidungstabelle auf Vollstndigkeit berprfen.

Wenn die Entscheidungstabelle vollständig ist, geben Sie einen Beweis an; wenn nicht, schlagen Sie eine Umgebungsannahme in Form eines Konfliktaxioms vor, das mit allen in der Tabelle vorhandenen Regeln konsistent ist und so, daß die Entscheidungstabelle vollständig bezüglich des Konfliktaxioms ist.

(1)

Nicht complete für $c_1 \mapsto 1, c_2 \mapsto 1$
 $c_3 \mapsto 0/1$

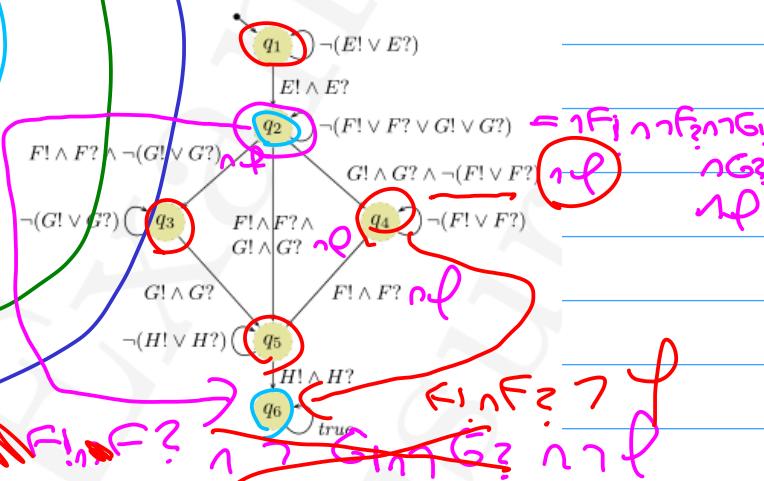
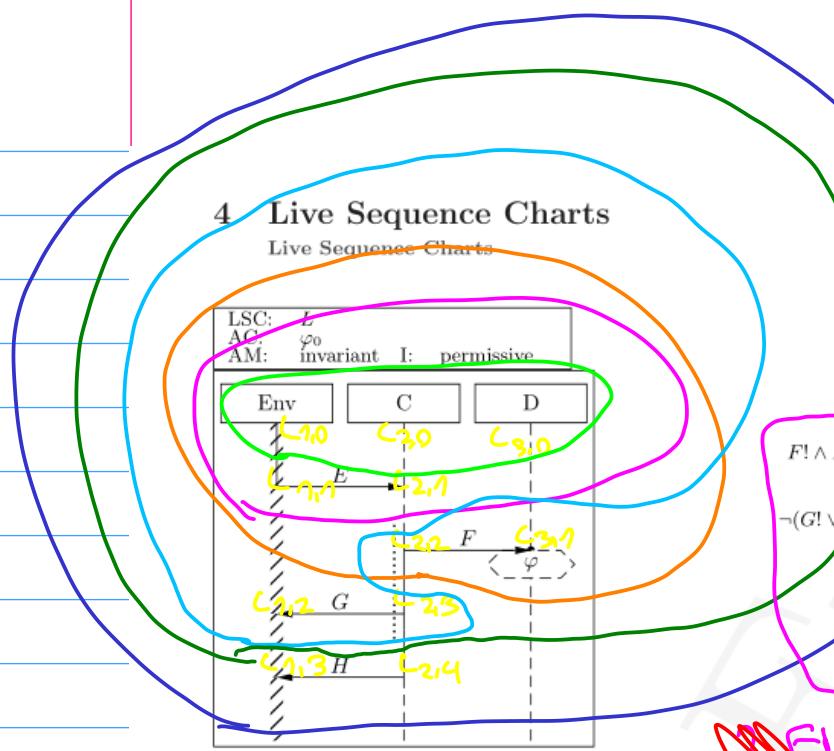


Figure 4: Live Sequence Chart and its TBA.
Live Sequence Chart und zugehöriger TBA.

Problem 4.1 (Locations and Cut Temperatures)

Aufgabe 4.1 (Locations und Cut Temperaturen)

- (i) What are the locations of the LSC L given in Figure 4 on page 6. Clearly mark them in the LSC in Figure 4.

Geben Sie die Locations der in Abbildung 4 auf Seite 6 gegebenen LSC an.
Markieren Sie die Locations eindeutig in der LSC in Abbildung 4.

- (ii) According to the LSC semantics, which states of the TBA shown in Figure 4 need to be accepting and which not?

Mark the states in the TBA in Figure 4 with single or double outlines accordingly.

Welche Zustände des in Abbildung 4 gezeigten TBA sind entsprechend der LSC Semantik akzeptierend und welche nicht?

Markieren Sie die Zustände im TBA in Abbildung 4 entsprechend mit einfachem oder doppeltem Rand.

(2)

Correction:

- $\frac{1}{3}$ point for each correct mark

Problem 4.2 (Computation Paths)

Aufgabe 4.2 (Berechnungspfade)

- (i) Provide a computation path which trivially satisfies L .
 - (ii) Provide a computation path which non-trivially satisfies L .
 - (iii) Provide a computation path which violates L . 4

You may disregard the condition for this task.

- (i) Geben Sie einen Berechnungspfad an, der L trivial erfüllt.
 - (ii) Geben Sie einen Berechnungspfad an, der L nicht-trivial erfüllt.
 - (iii) Geben Sie einen Berechnungspfad an, der L verletzt.

Die Bedingung können Sie für diese Aufgabe ignorieren.

Correction:

- 1 point for each of (i)

Problem 4.3 (Cold Conditions)**Aufgabe 4.3 (Kalte Bedingungen)**

- (i) The condition φ in LSC L has not been considered in the TBA shown in Figure 4. Complete the TBA such that the condition is properly represented.

Die Bedingung φ in LSC L wurde bei der Konstruktion des in Abbildung 4 gezeigten TBA nicht berücksichtigt. Vervollständigen Sie den TBA derart, daß die Bedingung korrekt repräsentiert wird.

(1)

Correction:

- $\frac{1}{7}$ point for each correct new transition and label (modification)

- (ii) Provide a computation path which satisfies L by taking a legal exit.

Geben Sie einen Berechnungspfad an, der L erfüllt, indem ein legaler Ausstieg genommen wird.

(1)

Correction:

- one point for correct path

5 Class Diagrams

Klassendiagramme



Figure 5: Class diagram.
Abbildung 5: Klassendiagramm.

**Problem 5.1 (Signature)****Aufgabe 5.1 (Signatur)**

Provide the (minimal) signature described by the class diagram in Figure 5.

Geben Sie die (kleinste) Signatur an, die vom Klassendiagramm in Abbildung 5 beschrieben wird.

Correction:

- 0.25 points for each correctly rewritten element
- max. -1 for notation errors

$\rho_0 = \{ \{ \{ \text{Int} \geq, \{ \text{Train}, \text{Segment} \}, \{ \text{speed} : \text{Int}, \text{length} : \text{Int}, n : \text{Segment}, n \} \} \} \}$
 $\{ \text{Train} \mapsto \{ \text{speed} \}, \text{Segment} \mapsto \{ \text{length}, n \} \}$
 $\{ \text{setSpeed} : \text{Int} \mapsto \emptyset \}$
 $\{ \text{Train} \mapsto \{ \text{setSpeed} \}, \text{Segment} \mapsto \emptyset \}$

Problem 5.2 (Associations)

Aufgabe 5.2 (Assoziationen)

Assume we add $s : Segment_*$ to V and s to $atr(Train)$ to the signature of the class diagram shown in Figure 5. Extend the class diagram in Figure 5 such that this additional modelling element is properly *graphically* represented, i.e. do not just add s to the attributes compartment.

Nehmen Sie an, in der Signatur des in Abbildung 5 gezeigten Klassendiagramms wird $s : Segment_*$ zu V und s zu $atr(Train)$ hinzugefügt.

Erweitern Sie das Klassendiagramm in Abbildung 5 derart, daß dieses zusätzliche Modellelement korrekt *graphisch* repräsentiert wird, d.h. s soll nicht einfach dem Bereich für Attribute hinzugefügt werden.

(1)

Correction:

- 0.25 points each for: line between correct things, arrow at correct side, labels at correct sides



Figure 5: Class diagram.
Abbildung 5: Klassendiagramm.

6 OCL

OCL

$$\sigma = \{u_1 \mapsto \{length \mapsto 27, n \mapsto u_2\}, u_2 \mapsto \{length \mapsto 13, n \mapsto \emptyset\}\}$$

Figure 6: System state.
Abbildung 6: Systemzustand.

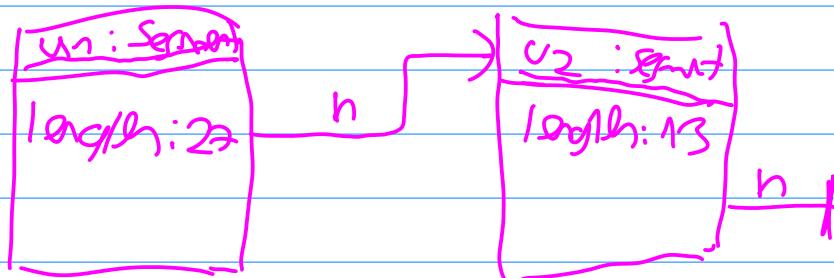
Problem 6.1 (Objectdiagrams)

Aufgabe 6.1 (Objektdiagramme)

Provide an object diagram which completely represents the system state shown in Figure 6.

Geben Sie ein Objektdiagramm an, das den in Abbildung 6 gegebenen Systemzustand vollständig darstellt.

(3)



Problem 6.2 (Proto-OCL Proof)

Aufgabe 6.2 (Proto-OCL Beweis)

$$F := \forall self : Segment \bullet length(self) > length(n(self))$$

Figure 7: Proto-OCL formula.

Abbildung 7: Proto-OCL Formel.

It is claimed that the Proto-OCL formula F shown in Figure 7 evaluates to \perp in the system state from Figure 6, i.e. that $\mathcal{I}[F](\sigma, \emptyset) = \perp$.

Prove this claim using the semantics of Proto-OCL.

Es wird behauptet, daß die in Abbildung 7 gegebene Proto-OCL Formel F in dem durch das Objektdiagramm in Abbildung 6 beschriebenen System State zu \perp ausgewertet wird, d.h. daß $\mathcal{I}[F](\sigma, \emptyset) = \perp$. Beweisen Sie diese Behauptung unter Verwendung der Proto-OCL Semantik.

(5)

$$\text{AllInterssegment} \wedge \forall self : Segment \bullet \text{length}(self) > \text{length}(n(self))$$

$$- \mathcal{I}(\text{AllInterssegment})(\sigma, \beta) = \{\text{U}_1, \text{U}_2\}$$

$$- \beta_1 = \{self \mapsto \text{U}_1\}$$

$$- \mathcal{I}(\text{length}(self), \text{length}(n(self)))(\sigma, \beta_1)$$

$$= \mathcal{I}(\text{length}(self)) \wedge \mathcal{I}(\text{length}(n(self)))_{(\sigma, \beta)}$$

$$= \mathcal{I}(27, 13)$$

= True

$$- \beta_1 = \{self \mapsto \text{U}_1\}$$

$$- \mathcal{I}(\text{length}(self), \text{length}(n(self)))(\sigma, \beta_2)$$

$$= \mathcal{I}(13, 1)$$

= 1

$\Rightarrow \perp$

Problem 6.3 (Proto-OCL Examples)

Aufgabe 6.3 (Proto-OCL Beispiele)

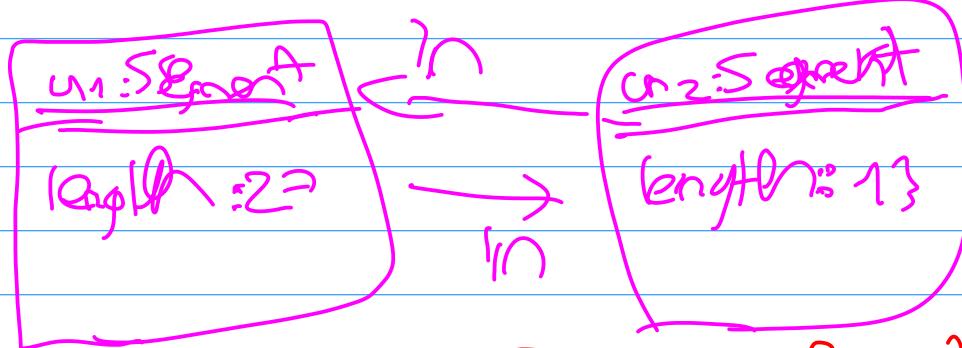
Provide two system states σ_1 and σ_2 such that $\mathcal{I}[F](\sigma_1, \emptyset) = \text{true}$ and $\mathcal{I}[F](\sigma_2, \emptyset) = \text{false}$.

Geben Sie zwei System States σ_1 und σ_2 an so, daß $\mathcal{I}[F](\sigma_1, \emptyset) = \text{true}$ und $\mathcal{I}[F](\sigma_2, \emptyset) = \text{false}$ gilt.

$$\delta_1 : \delta_1 = \emptyset$$

$$\sigma_1 = \text{Train} \mapsto \phi$$

O₂.



$\sigma_2 = \{ u \mapsto l \text{ report } \rightarrow B_2 \},$
 $in \mapsto \{ u_2 \} \}$,
on)

Problem 6.4 (Proto-OCL Formalisation)

Aufgabe 6.4 (Proto-OCL Formalisierung)

Formalise the following requirements using Proto-OCL formulae:

- (i) The value of the basic type attribute of each object of class *Segment* should be strictly bigger than 10.
 - (ii) The value of the *length* attribute of two different *Segment* instances to which a *Train* instance refers by an *s-link* differs by at most 1.

Formalisiere die folgenden Anforderungen mit Hilfe von Proto-OCL Formeln:

- (i) Der Wert des Basistyp-Attributs jedes Objektes der Klasse *Segment* soll streng größer als 10 sein.
 - (ii) Die Werte des *length* Attributs zweier verschiedener *Segment*-Instanzen, auf die eine *Train*-Instanz mit einem *s*-Link verweist, unterscheiden sich um höchstens 1.

(i) $\forall c \in \text{all_zimmers} \text{ segment } \bullet \text{ length}_{\text{v}}^{(c)} > 10$

(ii) $\forall E \in \text{all_edges} \cap \{V s_1 \in S \in E\} \cdot \forall s_2 \in E.s \cdot (S \neq \emptyset)$
 $- s_2 \neq s_1$

$(\wedge s_1 \neq s_2)$

7 Communicating Finite Automata

Communicating Finite Automata

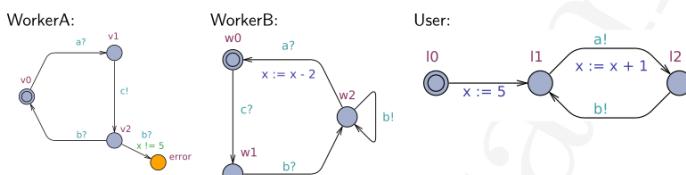


Figure 8: Network of Communicating Finite Automata (x is a global variable).
 Abbildung 8: Netzwerk Kommunizierender Endlicher Automaten (x ist eine globale Variable).

Problem 7.1 (Computation Paths)

Aufgabe 7.1 (Berechnungspfade)

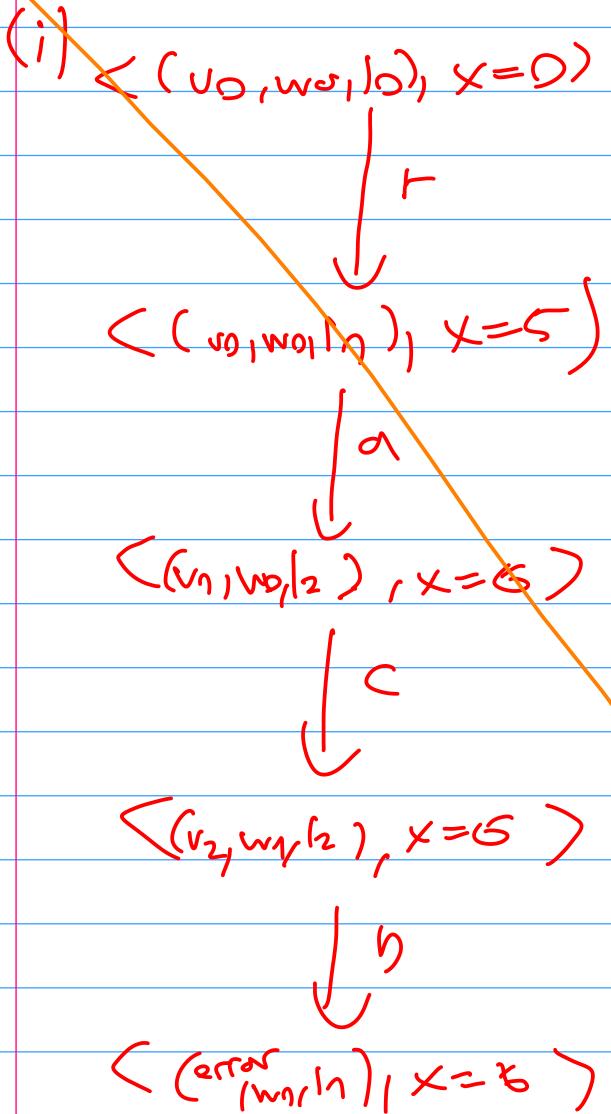
Consider the network \mathcal{N} of communicating finite automata given in Figure 8.

- (i) It is claimed that $\mathcal{N} \models_{\mathbb{E}\leftrightarrow} \text{WorkerA.error}$ holds.

Prove this claim by providing an appropriate computation path.

Es wird behauptet, daß $\mathcal{N} \models E \Leftrightarrow \text{WorkerA.error}$ gilt.

Beweisen Sie diese Behauptung, indem Sie einen entsprechenden Berechnungspfad angeben.

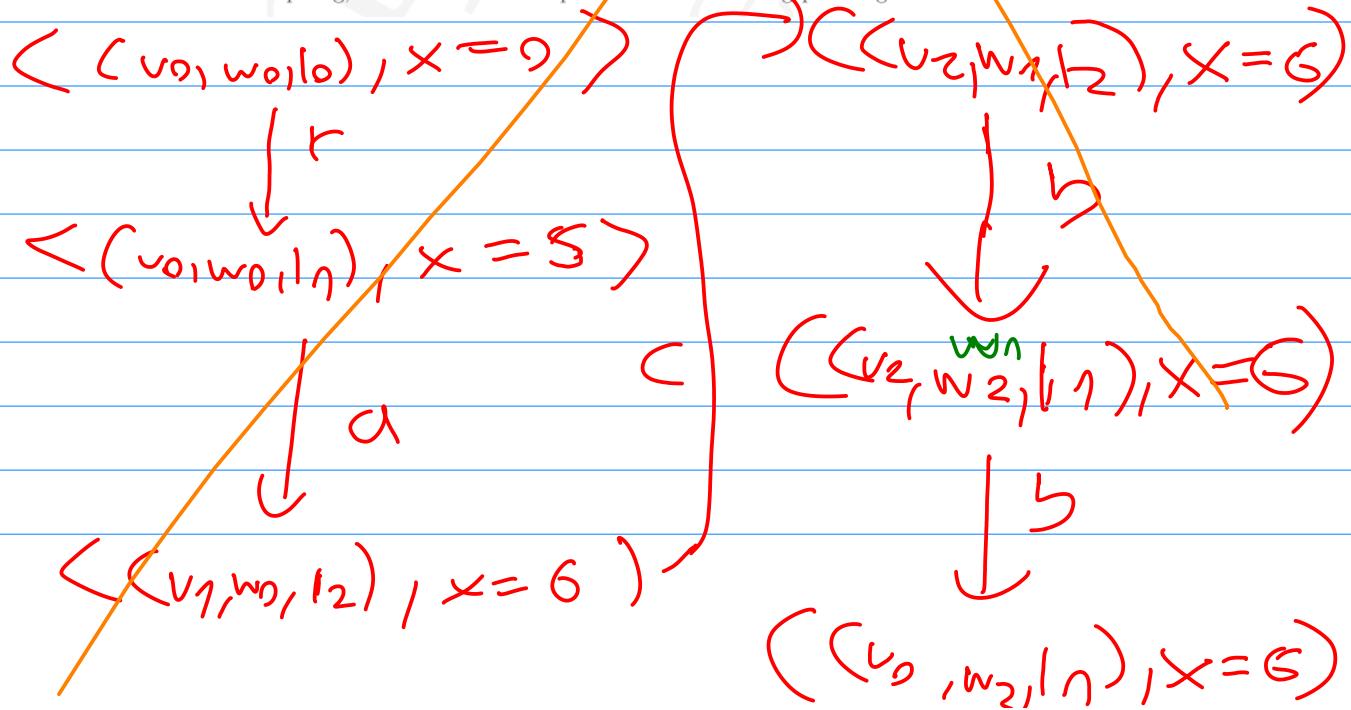


(ii) It is claimed that $\mathcal{N} \models A[] \text{WorkerA.error} \vee \text{not deadlock}$ does not hold.

Prove this claim by providing an appropriate computation path.

Es wird behauptet, daß $\mathcal{N} \models A[] \text{WorkerA.error} \vee \text{not deadlock}$ nicht gilt.

Beweisen Sie diese Behauptung, indem Sie einen entsprechenden Berechnungspfad angeben.



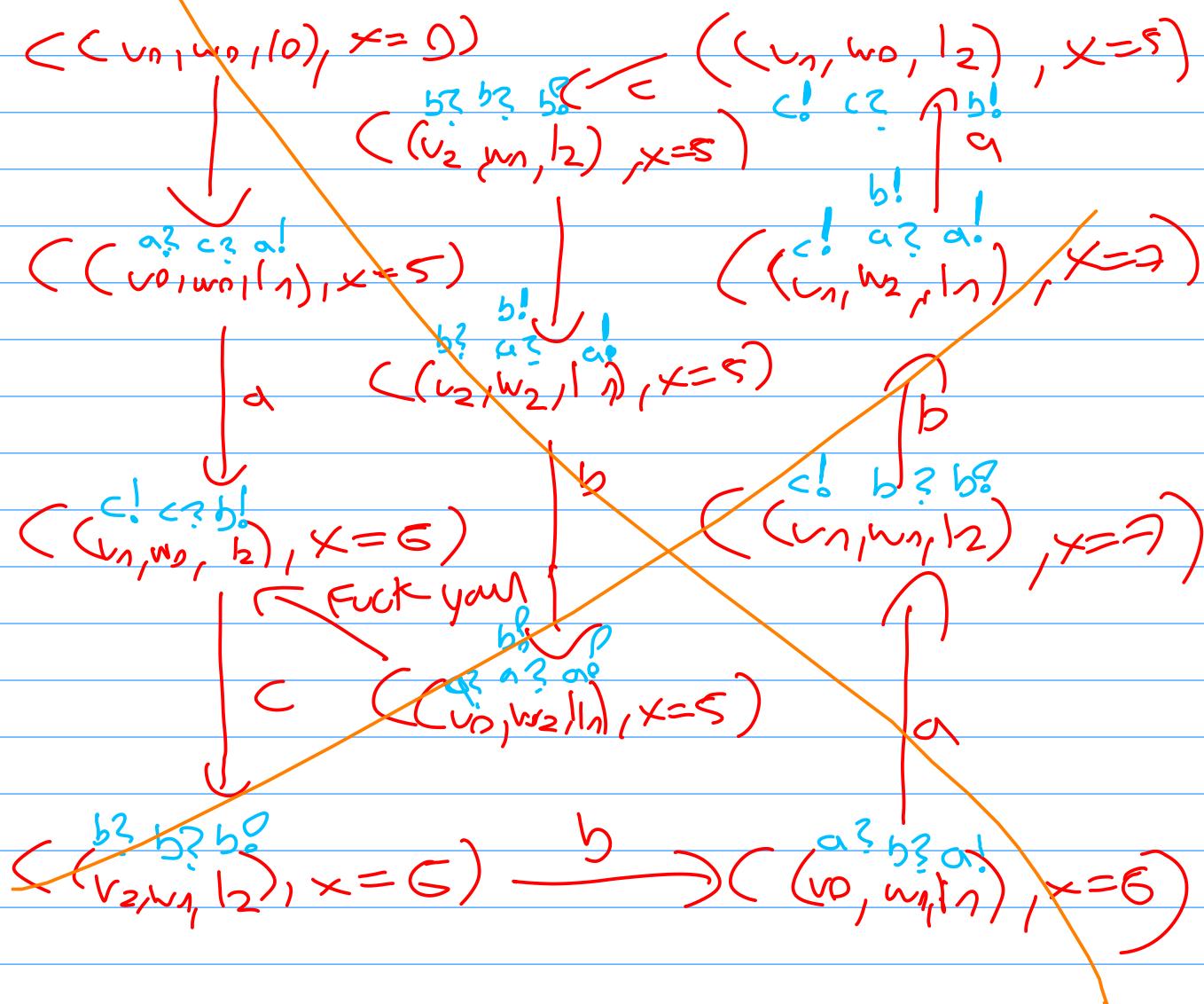
$\downarrow a$
 $\left(\langle v_0, w_0, l_2 \rangle, x = s \right)$
 $a? b? b!$
 deadlines

- (iii) It is claimed that $\mathcal{N} \models E[] \text{ not } \text{WorkerA.error}$ holds for an infinite computation path.

Prove this claim by providing an appropriate computation path.

Es wird behauptet, daß $\mathcal{N} \models E[] \text{ not } \text{WorkerA.error}$ für einen unendlichen Berechnungspfad gilt.

Beweisen Sie diese Behauptung, indem Sie einen entsprechenden Berechnungspfad angeben.



c)

$N \models \exists \langle \rangle \text{ writer}, \text{read} \rangle$

$\langle (v_0, w_0, b), x = 0 \rangle$

$\downarrow t$
 $\langle (v_0, w_0, b), x = 5 \rangle$

$\downarrow a$
 $\langle (v_1, w_0, b), x = 5 \rangle$

$\downarrow c$

$\langle (v_2, w_1, b), x = 5 \rangle$

\downarrow

$\langle (v_2, w_1, b), x = 6 \rangle$

(ii)

$N \not\models A \sqsubset$ vertex error \checkmark not deadlock

$N \models E \leftarrow$ \checkmark vertex. error \wedge deadlock

solche Transition die schon in einer 2-stell. $\xrightarrow{\text{post cond}}$

bringt, der bei bestimmten \star keine Transition hat (Präcondition)

$\langle (v_0, w_0, l_0), x=0 \rangle$

$\downarrow r$
 $\langle (v_0, w_0, l_1), x=5 \rangle$

$\downarrow a$
 $\langle (v_1, w_0, l_2), x=6 \rangle$ $\langle (v_0, w_2, l_2), x=6 \rangle$

$\left\{ \begin{array}{l} c \\ b \end{array} \right.$
 $\langle (v_2, w_2, l_2), x=6 \rangle$

(iii) It is claimed that $\mathcal{N} \models E[] \text{ not } \text{WorkerA.error}$ holds for an infinite computation path.

Prove this claim by providing an appropriate computation path.

Es wird behauptet, daß $\mathcal{N} \models E[] \text{ not } \text{WorkerA.error}$ für einen unendlichen Berechnungspfad gilt.

Beweisen Sie diese Behauptung, indem Sie einen entsprechenden Berechnungspfad angeben.

$\mathcal{N} \models E[] \text{ not } \text{workerA.error}$

$\langle (v_0, w_0, l_0), x=0 \rangle$

$\downarrow c$

$\langle (v_0, w_0, l_0), x=\leq \rangle$

$\downarrow a$

$\langle (v_1, w_0, l_0), x=\leq \rangle$

$\downarrow c$

$\langle (v_2, w_1, l_0), x=\leq \rangle$

$\downarrow b$

$\langle (v_2, w_2, l_1), x=\leq \rangle$

$\downarrow a$

$\langle (v_2, w_0, l_2), x=\leq \rangle$

$\downarrow b$

Problem 8.1 (Check PD Calculus Proof)

Aufgabe 8.1 (PD Kalkül-Beweis prüfen)

Consider the proof sketch for function SOMESUM in Figure 10 on page 13.

Betrachten Sie die Beweisskizze für die Funktion SOMESUM in Abbildung 10 auf Seite 13.

- (i) Complete the proof sketch by filling in the missing three formulae and label the marked steps by the axioms and rules uses for the step.
(The first step is already marked with axiom (A2) as an example.)

Vervollständigen Sie die Beweisskizze indem Sie die fehlenden drei Formeln einfügen und beschriften Sie die markierten Schritte mit dem Axiom bzw. der Formel, die für diesen Schritt verwendet wird.
(Der erste markierte Schritt ist als Beispiel bereits mit Axiom (A2) beschriftet.)

(6)

- (ii) Prove the step marked with (*).

You may use the propositions (1) and (2) given below.

Beweisen Sie den mit (*) markierten Schritt.

Sie können hierzu die unten angegebenen Beziehungen (1) und (2) verwenden.

(1)

$$(1) \sum_{k=1}^n k = \frac{1}{2}(n \cdot (n + 1))$$

$$(2) \sum_{k=1}^n k^2 = \frac{1}{6}n \cdot (n + 1) \cdot (2 \cdot n + 1)$$

(i)

$\{n \geq 0\}$

$\{n \geq 0 \wedge 0 = n \cdot \frac{1}{2}((0-1) \cdot 0) - \frac{1}{6} \cdot (0-1) \cdot 0 \cdot (2 \cdot 0 - 1) \wedge 0 \leq n+1 \wedge 0 = 0\} \quad \boxed{\text{A2}}$

$r := 0;$

$\{n \geq 0 \wedge r = n \cdot \frac{1}{2}((0-1) \cdot 0) - \frac{1}{6} \cdot (0-1) \cdot 0 \cdot (2 \cdot 0 - 1) \wedge 0 \leq n+1 \wedge 0 = 0\}$

$i := 0;$

$\{n \geq 0 \wedge r = n \cdot \frac{1}{2}((i-1) \cdot i) - \frac{1}{6} \cdot (i-1) \cdot i \cdot (2 \cdot i - 1) \wedge i \leq n+1 \wedge i = 0\}$

if $n > 0$ **then**

$\{n \geq 0 \wedge r = n \cdot \frac{1}{2}((i-1) \cdot i) - \frac{1}{6} \cdot (i-1) \cdot i \cdot (2 \cdot i - 1) \wedge i \leq n+1 \wedge i = 0 \wedge n > 0\}$

$\{n \geq 0 \wedge r = n \cdot \frac{1}{2}((i-1) \cdot i) - \frac{1}{6} \cdot (i-1) \cdot i \cdot (2 \cdot i - 1) \wedge i \leq n+1 \wedge n > 0\}$

while $i \leq n$ **do**

$\{n \geq 0 \wedge r = n \cdot \frac{1}{2}((i-1) \cdot i) - \frac{1}{6} \cdot (i-1) \cdot i \cdot (2 \cdot i - 1) \wedge i \leq n+1 \wedge i \leq n\}$

$\{n \geq 0 \wedge r + i \cdot (n-i) = n \cdot \frac{1}{2}(i \cdot (i+1)) - \frac{1}{6} \cdot i \cdot (i+1) \cdot (2 \cdot i + 1) \wedge (i+1) \leq n+1\}$

$\{n \geq 0 \wedge r + i \cdot (n-i) = n \cdot \frac{1}{2}(((i+1)-1) \cdot (i+1)) - \frac{1}{6} \cdot ((i+1)-1) \cdot (i+1) \cdot (2 \cdot (i+1) - 1) \wedge (i+1) \leq n+1\}$

$r := r + i \cdot (n-i);$

$i := i + 1;$

$\{n \geq 0 \wedge r = n \cdot \frac{1}{2}((i-1) \cdot i) - \frac{1}{6} \cdot (i-1) \cdot i \cdot (2 \cdot i - 1) \wedge i \leq n+1\}$

do

$\{n \geq 0 \wedge r = n \cdot \frac{1}{2}((i-1) \cdot i) - \frac{1}{6} \cdot (i-1) \cdot i \cdot (2 \cdot i - 1) \wedge i \leq n+1 \wedge \neg(i \leq n)\}$

$\{n = i+1 \wedge r = n \cdot \frac{1}{2}((i-1) \cdot i) - \frac{1}{6} \cdot (i-1) \cdot i \cdot (2 \cdot i - 1)\}$

$\{r = n \cdot \frac{1}{2}(n \cdot (n+1)) - \frac{1}{6} \cdot n \cdot (n+1) \cdot (2 \cdot n + 1)\}$

else

$\{n \geq 0 \wedge r = n \cdot \frac{1}{2}((i-1) \cdot i) - \frac{1}{6} \cdot (i-1) \cdot i \cdot (2 \cdot i - 1) \wedge i \leq n+1 \wedge i = 0 \wedge n \leq 0\}$

$\cancel{n=0 \wedge i=0}$

$\{n = 0 \wedge r = n \cdot \frac{1}{2}((n+1) \cdot n) - \frac{1}{6} \cdot n \cdot (n+1) \cdot (2 \cdot n + 1)\}$

skip

$\{r = n \cdot \frac{1}{2}((n+1) \cdot n) - \frac{1}{6} \cdot n \cdot (n+1) \cdot (2 \cdot n + 1)\}$

fi

$\{r = n \cdot \frac{1}{2}((n+1) \cdot n) - \frac{1}{6} \cdot n \cdot (n+1) \cdot (2 \cdot n + 1)\} =$

$\{r = \sum_{j=0}^n j \cdot (n-j)\} \quad (*)$

LG RS

R3

RC

A1

* :

$$r = n \cdot \frac{1}{2} ((n+1) \cdot n) - \frac{1}{6} \cdot n \cdot (n+1) \cdot (2 \cdot n + 1)$$

\Leftrightarrow 1. 2.

$$\Leftrightarrow r = n \cdot \sum_{\delta=0}^n \delta - \sum_{\delta=0}^n \delta^2$$

$$\Leftrightarrow r = \sum_{\delta=0}^n \delta \cdot (n-\delta)$$

Problem 8.2 (Prove with PD)

Aufgabe 8.2 (Beweisen mit PD)

$\{ \text{true} \} \ y := x; y = ((x - 1) \cdot x + y) + z; \text{while } z \text{ do skip } \{ y = x^2 \}$

Figure 9: A simple program.
Abbildung 9: Ein einfaches Programm.

Prove that the Hoare triple given in Figure 9 holds for partial correctness using the PD calculus.

Beweisen Sie mit Hilfe des PD-Kalküls, daß das in Abbildung 9 angegebene Hoare-Triple im Sinne von partieller Korrektheit gilt.

(3)

Correction:

- $\frac{1}{3}$ points for each rule application and each proof necessary for (R6)

~~$\Sigma_{\text{true}} \{ y = x, y = ((x-1) \cdot x + y) + z; \text{while } z \text{ do skip } \{ y = x^2 \}$~~

~~false~~

$x = ((x^2 - x + x) + z)^2 \wedge z = 0 \quad \} A_2$

$y = x$

$y = ((x-1) \cdot x + y) + z)^2 \wedge z = 0 \quad \} A_2$

$y = ((x-1) \cdot x + y) + z$

$y = x^2 \wedge z = 0$

$\text{while } z \text{ do}$

$z = 0 \wedge z \neq 0 \quad \} A \wedge$

~~skip~~

~~false~~

$y = x^2 \wedge z = 0 \wedge z \neq 0$

$y = x^2 \wedge \text{false}$

$y = x^2$

$i \leq n+1 \wedge i = n$

$i \leq n+1 \wedge i < n+1$

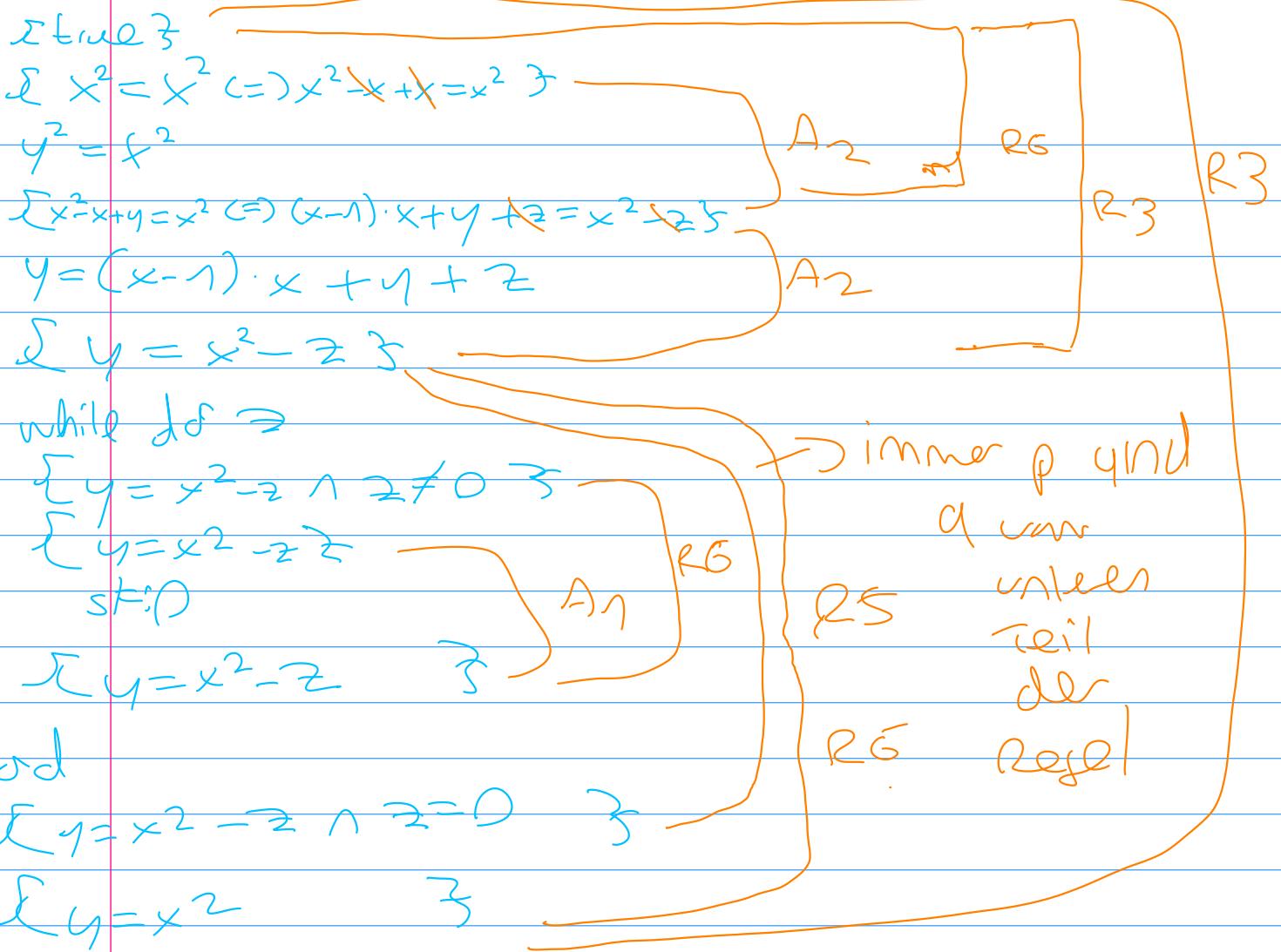
$i \cdot (n+1) \leq n \cdot (n+1) + 1$

$i \cdot \frac{n+1}{2} \leq n \cdot \frac{n+1}{2} + \frac{1}{2}$

$\Rightarrow i \leq n+1$

$\Rightarrow i \leq n$

$\Rightarrow i \leq n$



Problem 9.1 (Statement Coverage)

Aufgabe 9.1 (Anweisungsüberdeckung)

Provide a test suite which achieves 100% statement coverage for function `maxminavg` shown in Figure 11 on page 16. (The requirements on `maxminavg` are given in the caption of Figure 11.) For each test case, point out which statement it covers.

Geben Sie eine Menge von Testfällen an, die für die Funktion `maxminavg` aus Abbildung 11 auf Seite 16 eine Anweisungsüberdeckung von 100 % erreicht. (Die Anforderungen an `maxminavg` sind in der Bildunterschrift von Abbildung 11 gegeben.) Geben Sie für jeden Testfall an, welche Anweisungen dieser überdeckt.

(4)

```
1 public static void maxminavg( int[] values ) {  
2  
3     max = Double.MIN_VALUE;  
4     min = Double.MAX_VALUE;  
5  
6     int count = 0;  
7     double total = 0;  
8  
9     for ( int i = 0; i < values.length; ++i ) {  
10  
11         double v = values[i];  
12  
13         if ( v > max ) {  
14             max = v;  
15         }  
16         if ( v < min ) {  
17             min = v;  
18         }  
19  
20         count++;  
21         total += v;  
22     }  
23  
24     if ( count == 0 || count < 0 )  
25         avg = -27;  
26     else  
27         avg = total / count;  
28 }
```

Handwritten annotations:

- Line 3: max = Double.MIN_VALUE; → S1
- Line 4: min = Double.MAX_VALUE; → S1
- Line 6: int count = 0; → S1
- Line 7: double total = 0; → S1
- Line 9: for (int i = 0; i < values.length; ++i) { → S1
- Line 11: double v = values[i]; → S2
- Line 13: if (v > max) { → S2
- Line 14: max = v; → S2
- Line 15: } → S2
- Line 16: if (v < min) { → S3
- Line 17: min = v; → S3
- Line 18: } → S3
- Line 20: count++; → S5
- Line 21: total += v; → S5
- Line 23: } → S4
- Line 24: if (count == 0 || count < 0) → S4
- Line 25: avg = -27; → S5
- Line 26: else → S6
- Line 27: avg = total / count; → S7
- Line 28: } → value of test

Input

Soll

$s_1 i_{1T} i_1 \perp c_{1T} c_{1L} s_2 i_{2T} c_{2T} c_{2L} s_3 i_{3T} c_{3T} c_{3L} s_4 s_5 i_{4T} i_{4L} c_{4T} c_{4L} c_{5T} c_{5L} s_6 s_2$

Min Max

$$av = -27, \quad x$$

X X X

(4,2) avg=3,2,4 X X X X X X X X X X X X X X X X X X

Max values: \Rightarrow 100% statement \Rightarrow 100%, BrandM

$$\Rightarrow \frac{9}{20} = 90\% \text{ Trm}$$

Problem 9.4 (Undetected Errors)

Aufgabe 9.4 (Unerkannte Fehler)

Provide

- a test suite which achieves 100 % statement coverage for function `maxminavg` shown in Figure 11 on page 16, and
- a modification of `maxminavg`

such that the modification does not satisfy the requirements on `maxminavg` and all test cases are executed unsuccessfully.

Explain your solution!

Geben Sie

- eine Menge von Testfällen, die für die Funktion `maxminavg` aus Abbildung 11 auf Seite 16 eine Anweisungsüberdeckung von 100 % erreicht und
- eine Modifikation von `maxminavg` an

so, daß die Modifikation die Anforderungen an `maxminavg` nicht erfüllt und alle Testfälle erfolglos ausgeführt werden.
Erklären Sie Ihre Lösung!

(2)

Correction:

- one point for correct modification
- one point for explanation (why are requirements no longer met, why not detected by test suite?)

$\{ \langle [3, 5, 4], (4, 3, 5) \rangle, \langle [] \rangle, \langle -27, \text{MaxValue} \rangle \}^3$

Figure 11: Function `maxminavg`. For input $a[0], \dots, a[n]$, $n \geq 0$, with $\sum_{i=0}^n a[i] \leq \text{Double.MAX_VALUE}$, `maxminavg` should store the minimum value in the global variable `min`, the maximum number in `max`, and the average (up to the precision of Java's `double`) in `avg`. In case the input array is empty, `max` and `min` should get the values `Double.MIN_VALUE` and `Double.MAX_VALUE`, respectively, and `avg` the value -27.

Problem 9.5 (Path Coverage)

Aufgabe 9.5 (Pfadüberdeckung)

There is a notion of *path coverage* where 100 % is achieved if each path from an entry to an exit point is covered, including skipping loops and executing the loop body at least once.

Do you see a relation between this notion of path coverage and the McCabe complexity metrics? Explain.

Es gibt einen Begriff von *Pfadüberdeckung* bei dem für 100 % Überdeckung jeder Pfad von einem Eingangs- zu einem Ausgangspunkt überdeckt wird. Insbesondere Schleifenkörper sollen dabei einmal übersprungen und mindestens einmal oder mehrmals durchlaufen werden.

Sehen Sie einen Zusammenhang zwischen diesem Begriff von Pfadüberdeckung und der Komplexitätsmetrik von McCabe?

Erklären Sie.

~~- beide Spalten bei Kurztest nicht statwrg~~
~~- bei ADO 70 path cover hat man nur viele Pfade~~

~~cool~~

$\text{Pfadanzahl} \leq 2^{\text{McCabe Complexity}}$ $\rightarrow \text{Zahl} + 2$
 \rightarrow jede IF/While höchste Variable

$\text{max doppelt so viele Pfade}$ \rightarrow $\text{if } i > \text{if } i ? \text{ max}$

denn if