Labeled @-Calculus:
Formalism for Time-Concerned Human Factors

Tetsuya Mizutani(Univ. Tsukuba)
Shigeru Igarashi(Tokiwa Univ.)
Yasuwo Ikeda(Saitama Junior College)
Masayuki Shio(Tokiwa Univ.)

Contents

- Introduction
- Labeled @-Calculus :
  Syntax and Intended Meaning
- Formalization of Programs
  - Program Axioms and Axiom Tableaux
- Case Study: Formalization and Analysis of Shigaraki Kougen Railway Traffic Accident
- Conclusion

Aim of Study

- It becomes more and more important to analyze and verify realtime controlling complex external systems, like railways and airlines, whose serious accidents can be caused by human errors involved in recognition or decision.

Aim of Study

- Human factor will be represented formally by labeled @-calculus.
  - Labeled @-calculus :
    - for specification and verification of real-timing systems (@-calculus)
    - for time-concerned recognition, knowledge, belief and decision of humans

@-calculus

- An extension of Peano arithmetic
  - PA(∞): PA + ∞ + μ : pseudo-arithmetic (base)
  - introducing "@" (coincidental operator) to describe change of state
- A formal system for specification and verification of real-timing system using tense terms
- Identified a formula with its tense i.e. the natural number time-point when it holds

Examples:

- J: clock counting every ms
- $J=1000@0$
  - The clock value is 1000 now (at tense 0).
  - It can be written as $J=1000$ (@0 can be abbreviated).
- $J=1000+n@n$
  - J will be 1000+n after n[ms].
- $J=1000 \equiv J=1000+n@n$
  - $\forall xy(J=x \equiv J=x+y@y)$ in general
    - $\forall xyz(z=x \equiv z=x+y@y)$ is incorrect

- $\alpha<1[\mathrm{min}]@l$
  - l : a person
    expecting the train to depart within 1[min] later
- $\alpha=5[\mathrm{min}]@l'$
  - l' : another person
    knowing that the train will depart 5 [min] later
    - α : spur : generalization of schedular
      trigger of train starting
- l misunderstands the schedule of the train!

Labeled @-calculus

- label: l, l_1, l_2, ...
  - Personality : an extension of an observer in physics, involving subjective
- $A@\langle a\rangle$: A holds at tense a
  (A: formula, a: term)
  - tense: a relative time-point
    from the observation time (now)
- $A@\langle a, l_1,\ldots, l_n\rangle$:
  $\langle l_1,\ldots, l_n\rangle$ believe that A holds at a
- $A@\langle l_1,\ldots, l_n\rangle$:
  $\langle l_1,\ldots, l_n\rangle$ believe that A holds now
- λ: metavariable of $\langle a\rangle$, $\langle a, l_1,\ldots, l_n\rangle$, $\langle l_1,\ldots, l_n\rangle$, etc.

Labeled @-calculus

- Proof system
  - Axioms
    - sevaral axioms for “@”
      - eg. A@l@x≡A@<x, l>

        (x≤y)@λ≡μz(z=x@λ)≤μz(z=y@λ)
  - Proof Rules
    - Based on rules of NK

Axioms The following axioms are added to those of $PA(\infty)$ as the logical, *proper* axioms, where **false** is an abbreviation of $0 = 1$.

1. The equality substitution for @: $x = y \supset \mathbf{A}@x \supset \mathbf{A}@y$.
2. Elimination of tense 0: $\mathbf{A}@0 \equiv \mathbf{A}$.
3. Inductive valuation:
   (a) $\mathbf{false}@x \equiv x = \infty$,
   (b) $(x \leq y)@\lambda \equiv \mu z(z = x@\lambda) \leq \mu z(z = y@\lambda)$,
   (c) $\mathbf{A}@x@y \equiv \mathbf{A}@y\mathbf{;}\ x$,
   (d) $\mathbf{A}@x@l \equiv \mathbf{A}@\langle x,\ l\rangle$,
   (e) $x < \infty \supset ((\neg\mathbf{A})@x \equiv \neg(\mathbf{A}@x))$,
   (f) $\neg(\mathbf{A}@l) \equiv (\neg\mathbf{A})@l$,
   (g) $(\mathbf{A}\&\mathbf{B})@\lambda \equiv \mathbf{A}@\lambda\&\mathbf{B}@\lambda$,
   (h) $(\forall y\mathbf{A})@\lambda \equiv \forall y(\mathbf{A}@\lambda)$.

Inference Rules

1. *Restriction of* ∀*-E rule.* In ∀-E(elimination) rule:

   $$\frac{\forall x(\mathbf{A}[x])}{\mathbf{A}[\mathbf{a}]}$$

   only a pseudo-arithmetic expression $\mathbf{a}$ can be substituted for x if x occurs in a subformula of the form $\mathbf{B}[x]@\langle\mathbf{b},\ l\rangle$ or $\mathbf{B}[x]@\mathbf{b}$ of the upper formula, while the occurrence of x in $\mathbf{b}$ does not matter.

2. @-I(introduction rule):

   $$\frac{\mathbf{A}}{\mathbf{A}@x}$$

   where every assumption of $\mathbf{A}$ does not have any special constants.
3. @-E(elimination rule):

   $$\frac{\mathbf{A}@\mathbf{a}}{\mathbf{A}}$$

   where no special constant occurs in $\mathbf{A}$.

- Represented by program axioms
  - The forms of (A⇒B)@λ or A⇒(B@λ)
    - A: condition (e.g. Signal=green)
      B: action (e.g. α=(Signal=red))
    - ⇒ : implication symbol

      involving the axiom of conservation
      - The axiom of conservation:
        The values of program variables is kept unchanged whenever no corresponding action is done.
  - Spur α, β, γ, κ, ...
    - generalizations of program schedulers
      - Each process is assigned a distinct spur.

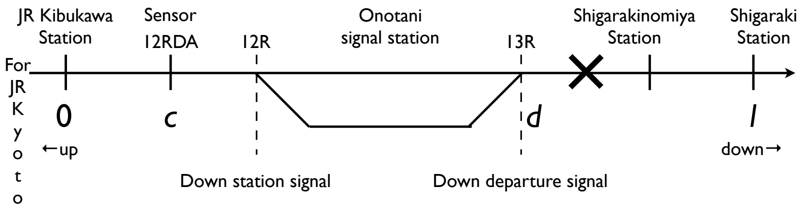
- $(A \Rightarrow B)@\lambda$

index	condition	act	tense	personality
i	A	B	a	$l_1,\ldots,l_n$

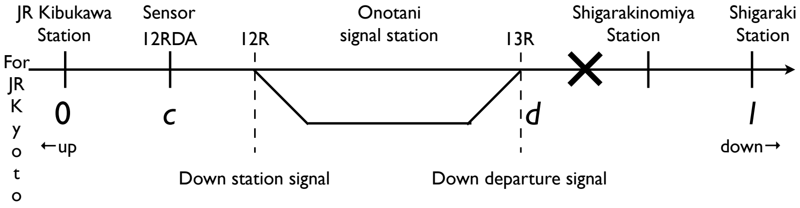
- $A \Rightarrow (B@ \lambda)$

index	condition	act	tense	personality
i	A, global	B	a	$l_1,\ldots,l_n$

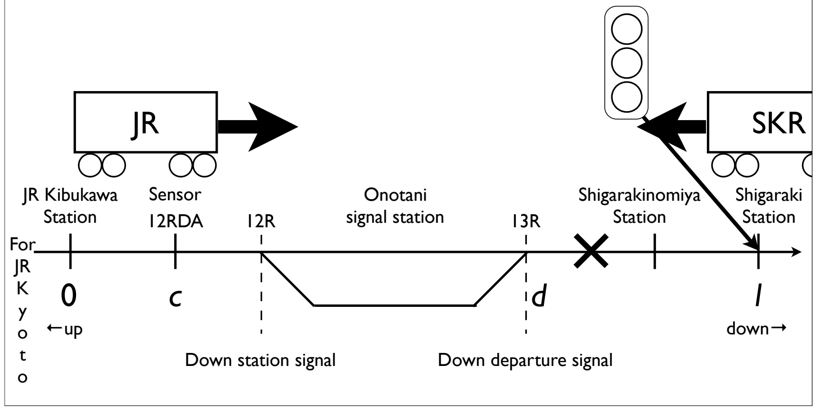
Shigaraki Kougen Railway Traffic Accident



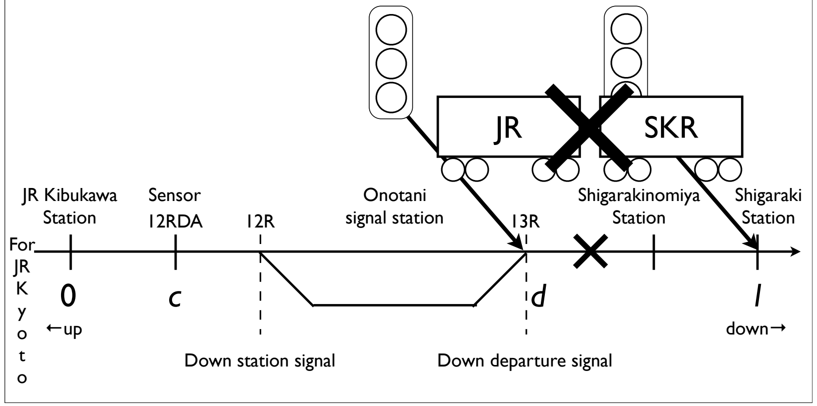
- Occurred about at 10:35, 14th May 1991
  - Between Onotani signal station and Shigaraki-no-Miya station
- An up train of Shigaraki Kogen Railway (SKR) for Kibukawa Station collided with a down train of Japan Railway (JR) for Shigaraki station.



- **Cause**
  - **When the SKR (up) train was to depart from Shigaraki station at 10:14 as scheduled, the signal at the station was still red.**
  - **The responsible person of SKR decided that the up train depart 11 minutes after the scheduled time.**



- **But the departure signal for the down trains at Onotani signal station was still green.**
- **Thus, the JR (down) train did not wait at the signal station and entered the interval between the signal station and Shigaraki station.**
- **Therefore, two trains collided.**



Formalization by Axiom Tableau

	index	condition	act	tense	personallity
Axioms	1	Clock=r, global		r	S, J
	2	A=l, B≦0 ¬13R, ¬lock, global		Clock=0	S, J
	3	r+≡r≦Clock, def			S, J
	4		α=10:25+1	A=l	S
	5		γ=α	〃	S
	5'	—	—	—	—
	6		γ=α	A=d+u	S
	7		κ=α	A=d	S
	8	¬13R	γ=lock		S
	9	lock	γ=¬lock		S
	10	0<i<imax	$\alpha^{i+1}=\alpha^i+1$		S, J
	11	0<i≦imax	A=l-i・u	α^i	S, J
	12		β=13R+1	B=d	S, J
	13	0<j<jmax, j≠jmid	$\beta^{j+1}=\beta^j+1$		S, J
	14	0<j≦jmid	B=j・v	β^j	S, J
	15	jmid<j≦jmax	B=d+j・w	β^j	S, J
	16		β=κ	B=c	S, J
	17		κ=12R		S, J
	18	¬lock	κ=13R		S, J
	19	10:16≦[B=0], global			S, J
	20	v≦c/(9・60), global			S, J
Inference by SKR	21	d<A<l⇒B≦ d		x+10:25+1	S
	22	¬Crash		x+10:25+1	S
Fact: 5 does not hold	21'	d<A<l∧d≦B<l		∃x.x+10:25+1	
	22'	Crash		∃x.x+10:25+1	

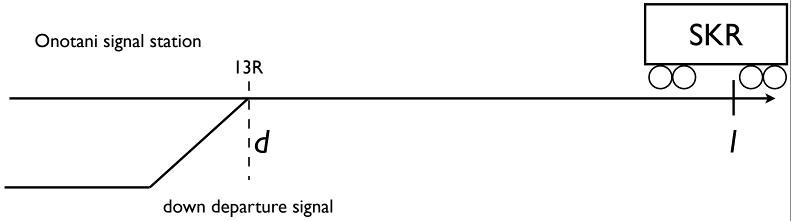
index	condition	act	tense	personality
1	Clock=r, global		r	S, J
2	A=*l*, B≦0 ¬13R, ¬lock, global		Clock=0	S, J

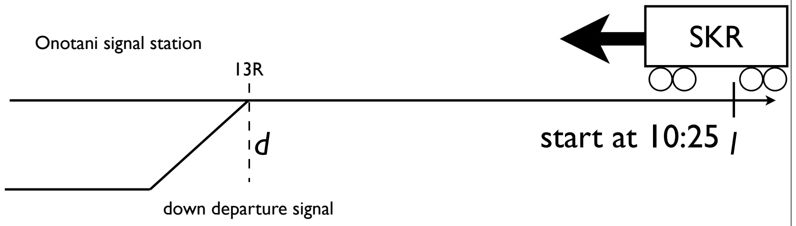
- Initialization (Personality: S:SKR, J:JR)
  - 1 The value of Clock is r when it is r [s] after the system starts.
  - 2 The initial values of the program variables:
    - A: the position of the SKR (up) train, initial : *l* (Shigaraki)
      B: the position of the JR (down) train, initial: ≤0(Kibukawa)
      13R:the status of 13R signal
      true: green, false: red initial: red

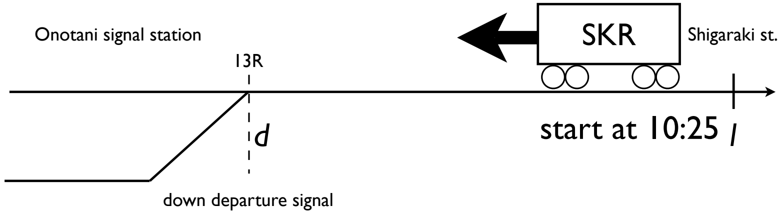
      lock: block signal for 13R signal occurring when up train starts from Shigaraki st. initial: open

index	condition	act	tense	personality
4		α=10:25+1	A=*l*	S
5		γ=α	〃	S
8	¬13R	γ=lock		S
9	lock	γ=¬lock		S

- Acts of SKR (up) train
  - Knowledge of SKR
    (JR does not know them)
  - α: spur of SKR train
  - 4 SKR train departs at 10:25.



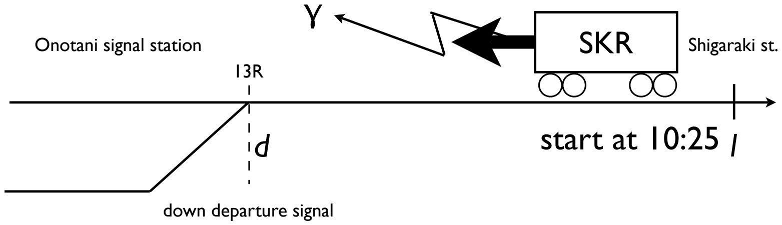




index	condition	act	tense	personality
4		α=10:25+1	A=l	S
5		γ=α	〃	S
8	¬13R	γ=lock		S
9	lock	γ=¬lock		S

- Acts of SKR (up) train
  - Knowledge of SKR

    (JR does not know them)
  - α: spur of SKR train
  - 4 SKR train departs at 10:25.
  - 5 The spur γ for the block signal rises.

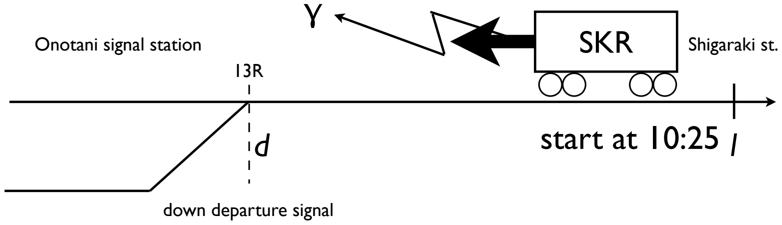


index	condition	act	tense	personality
4		α=10:25+1	A=l	S
5		γ=α	〃	S
8	¬13R	γ=lock		S
9	lock	γ=¬lock		S

- Acts of SKR (up) train
  - Knowledge of SKR
    (JR does not know them)
  - α: spur of SKR train.
  - 4 SKR train departs at 10:25.
  - 5 The spur γ for the block signal rises.
  - 8 If 13R is red, then 13R becomes locked.
  - 9 If 13R is locked, then 13R becomes open.

13R is
red⇒locked

locked⇒open

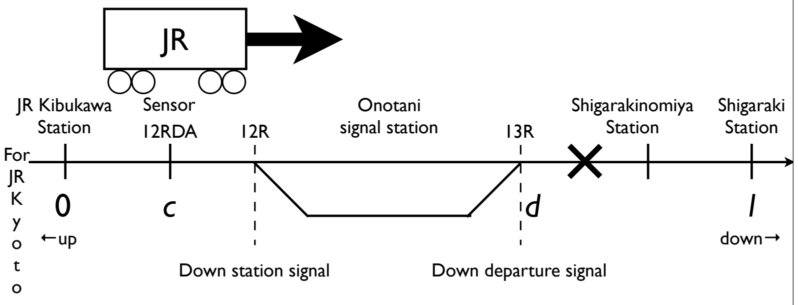


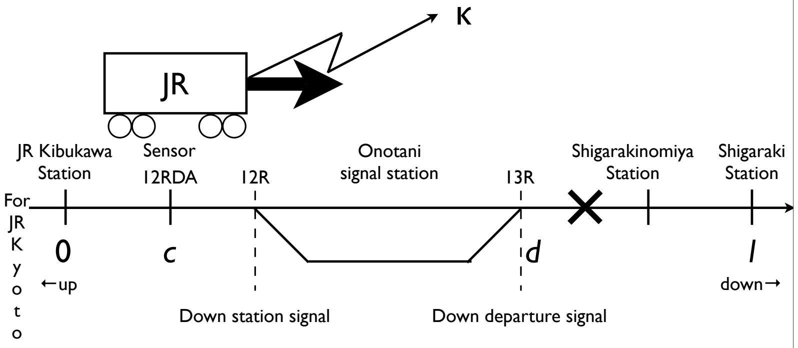
index	condition	act	tense	personality
12		β=13R+1	B=d	S, J

- Acts of JR (down) train
  - β: spur for JR train
  - 12 The train starts from Onotani signal station
    when 13R is green.

index	condition	act	tense	personality
16		β=κ	B=c	S, J

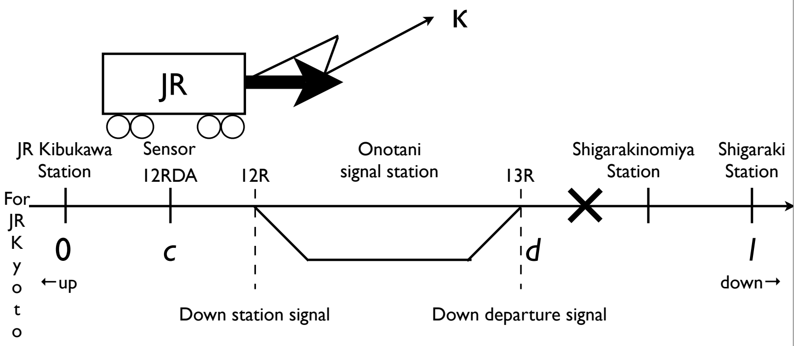
- Acts of JR (down) train
  - c: the position of the sensor for advance control of 12R
  - 16 When the train arrives at c, the spur κ for the control of 12R and 13R rises.

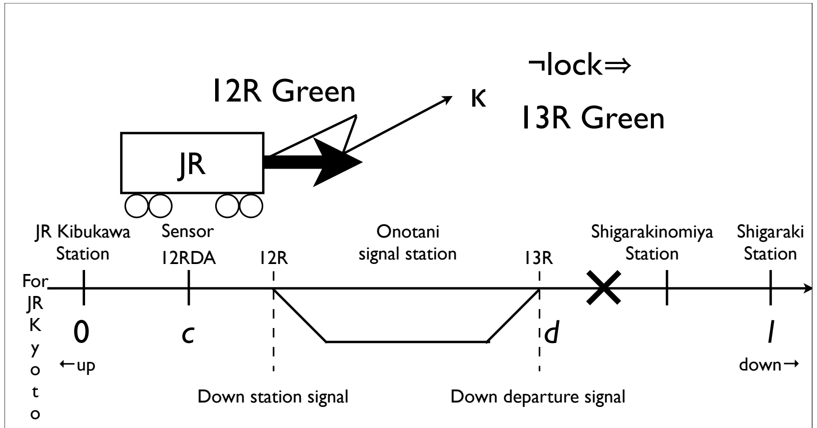




index	condition	act	tense	personality
17		κ=12R		S, J
18	¬lock	κ=13R		S, J

- Acts of JR (down) train
  - Control of signals
  - 17 When κ arises, 12R becomes green.
  - 18 If 13R is not locked at the period κ arises, then 13R becomes green.





index	condition	act	tense	personality
4		α=10:25+1	*A*=1	S
~~**5**~~		~~γ=α~~	~~〃~~	~~S~~
8	¬*13R*	γ=*lock*		S
9	*lock*	γ=¬*lock*		S
16		β=κ	B=c	S, J
17		κ=12R		S, J
18	¬lock	κ=13R		S, J

- 4 SKR train starts at 10:25.
- ~~5 The spur γ for the block signal~~ rises.
- 8 If 13R is red, then 13R is locked.
- 9 If 13R is locked, then 13R becomes open.
- 16 When the train arrives at c,
  the spur κ for the control of 12R and 13R rises.
- 17 When κ arises, 12R becomes green.
- 18 If 13R is not locked at the period κ arises,
  then 13R becomes green.

index	condition	act	tense	personality
10	0<i<imax	$\alpha^{i+1}=\alpha^i+1$		S, J
11	0<i≦imax	A=*l*-iu	α^i	S, J

- Acts of SKR (up) train
  - u: speed of the train
  - imax=(*l*-d)/u

  - 10 Spur α rises every 1 [s]
  - 11 the position of SKR train of the tense α^i
    - α^i: the tense of i-th rise of α

index	condition	act	tense	personality
13	$0<j<jmax, j \neq jmid$	$\beta^{j+1}=\beta^{j}+1$		S, J
14	$0<j \leqq jmid$	$B=j \cdot v$	β^{j}	S, J
15	$jmid<j \leqq jmax$	$B=d+j \cdot w$	β^{j}	S, J

- Acts of JR (down) train
  - v: speed of the train when it is between Kibukawa and Onotani
  - w: speed of the train when it is between Onotani and Shigaraki
  - $jmid=d/v$, $jmax=d/v+(l-d)/w$
  - 13 Spur rises every 1 [s] other than the train is in Onotani.
  - 14 the position of the train between Kibukawa and Onotani
  - 15 the position of the train between Onotani and Shigaraki

index	condition	act	tense	personality
19	$10{:}16 \leqq [B=0]$, global			S, J
20	$v \leqq c/(9 \cdot 60)$, global			S, J

- Acts of JR (down) train
  - 19 The train does not arrive at Kibukawa until 10:16.
  - 20 the upper limit of v
    (speed of the train between Kibukawa and Onotani)
    - ⇒ JR train takes more than 9 min. from Kibukawa to 12RDA.
  - From them,
  - the fact that JR train does not arrive until 10:25 is obtained.

Inference by SKR

- The responsible person of SKR inferred the fact that no collision could happen even if the SKR (up) train starts at 10:25 by his own knowlwdge, i.e.
- Suppose that up train will start at 10:25 as 4.
- 13R is locked from 5 and 8.
- Even if JR (down) train will not reach c after the aboves as 16, 13R will not turn green.

index	condition	act	tense	personality
4		$\alpha=10{:}25+1$	$A=l$	S

- JR train will not reach c till 10:25 from 19 and 20.
- Thus, 13R will not turn green.
- JR train will not beyond Onotani. (12)
- Therefoere any crash does not cause (21, 22), where $Crash \equiv d<A<l \wedge d<B<l \wedge |A- B|<\delta$

Inference by SKR

- The responsible person of SKR inferred the fact that no collision could happen even if the SKR (up) train starts at 10:25 by his own knowlwdge, i.e.
- Suppose that up train will start at 10:25 as 4.
- 13R is locked from 5 and 8.
- Even if JR (down) train will not reach c after the aboves as 16, 13R will not turn green.

index	condition	act	tense	personality
5		$\gamma=\alpha$	〃	S
8	$\neg 13R$	$\gamma=lock$		S

- JR train will not reach c till 10:25 from 19 and 20
- Thus, 13R will not turn green.
- JR train will not beyond Onotani. (12)
- Therefoere any crash does not cause (21, 22), where $Crash \equiv d<A<l \wedge d<B<l \wedge |A- B|<\delta$

Inference by SKR

- The responsible person of SKR inferred the fact that no collision could happen even if the SKR (up) train starts at 10:25 by his own knowlwdge, i.e.
- Suppose that up train will start at 10:25 as 4.
- 13R is locked from 5 and 8.
- Even if JR (down) train will not reach c after the above two things as 16, 13R will not turn green.
- JR train will not reach c till 10:25 from 19 and 20
- Thus, 13R will not turn red.

index	condition	act	tense	personality
16		β=κ	B=c	S, J
~~18~~	~~¬lock~~	~~κ=*13R*~~		~~S, J~~

- JR train will not beyond Onotani. (12)
- Therefoere any crash does not cause (21, 22), where Crash≡d<A<l∧d<B<l∧|A- B|<δ

Inference by SKR

- The responsible person of SKR inferred the fact that no collision could happen even if the SKR (up) train starts at 10:25 by his own knowlwdge, i.e.
- Suppose that up train will start at 10:25 as 4.
- 13R is locked from 5 and 8.
- Even if JR (down) train will not reach c after the above two things as 16, 13R will not turn green.
- JR train will not reach c till 10:25 from 19 and 20.
- Thus, 13R will not turn red.
- JR train will not beyond Onotani. (12)
- Therefoere any crash does not cause (21, 22), where Crash≡d<A<l∧d<B<l∧|A- B|<δ

index	condition	act	tense	personality
19	10:16≤[B=0], global			S, J
20	v≦c/(9・60), global			S, J

Inference by SKR

- The responsible person of SKR inferred the fact that no collision could happen even if the SKR (up) train starts at 10:25 by his own knowlwdge, i.e.
- Suppose that up train will start at 10:25 as 4.
- 13R is locked from 5 and 8.
- Even if JR (down) train will not reach c after the above two things as 16, 13R will not turn green.
- JR train will not reach c till 10:25 from 19 and 20.
- Thus, 13R will not turn green.
- JR train will not beyond Onotani from 12.
- Therefoere any crash does not cause (21, 22), where Crash≡d<A<l∧d<B<l∧|A- B|<δ

index	condition	act	tense	personality
12		β=13R+1	B=d	S, J

Inference by SKR

index	condition	act	tense	personality
21	d<A<l⇒B≦d		x+10:25+1	S
22	¬Crash		x+10:25+1	S

- The responsible person of SKR inferred the fact that no collision could happen even if the SKR (up) train starts at 10:25 by his own knowlwdge, i.e.
- Suppose that up train will start at 10:25 as 4.
- 13R is locked from 5 and 8.
- Even if JR (down) train will not reach c after the above two things as 16, 13R will not turn green.
- JR train will not reach c till 10:25 from 19 and 20
- Thus, 13R will not turn green.
- JR train will not beyond Onotani. (12)
- Therefoere any crash does not cause (21, 22), where Crash≡d<A<l∧d<B<l∧|A- B|<δ

Actual Action

- The responsibile person of SKR decided that SKR (up) train started at 10:25.(4)
- Block signal did not rise. (negation of 5)
- 13R was not locked (negation of 8),   and

  13R turned green for JR (down) train. (18)
- JR train entered the interval between Onotani and Shigaraki.(12)
- Therefore, there exists a tense x that 21and 22 do not hold.
- Namely, 21' and 22' hold, ie. Crash

index	condition	act	tense	personality
4		α=10:25-1	A=	S

Actual Action

- The responsibile person of SKR decided that SKR (up) train started at 10:25.(4)
- Block signal did not rise. (negation of 5)
- 13R was not locked (negation of 8),   and

  13R turned green for JR (down) train. (18)
- JR train entered the interval between Onotani and Shigaraki.(12)
- Therefore, there exists a tense x that 21and 22 do not hold.
- Namely, 21' and 22' hold, ie. Crash

index	condition	act	tense	personality
~~**5**~~		~~γ=α~~	~~//~~	~~S~~

Actual Action

- The responsibile person of SKR decided that SKR (up) train started at 10:25.(4)
- Block signal did not rise. (negation of 5)
- 13R was not locked (negation of 8),   and

  13R turned green for JR (down) train. (18)
- JR train entered the interval between Onotani and Shigaraki.(12)
- Therefore, there exists a tense x that 21and 22 do not hold.
- Namely, 21' and 22' hold, ie. Crash

index	condition	act	tense	personality
~~**8**~~	~~¬*13R*~~	~~γ=*lock*~~		~~S~~
18	*lock*	κ=*13R*		S, J

Actual Action

- The responsibile person of SKR decided that SKR (up) train started at 10:25.(4)
- Block signal did not rise. (negation of 5)
- 13R was not locked (negation of 8),   and

  13R turned green for JR (down) train. (18)
- JR train entered the interval between Onotani and Shigaraki.(12)
- Therefore, there exists a tense x that 21and 22 do not hold.
- Namely, 21' and 22' hold, ie. Crash

index	condition	act	tense	personality
12		β=13R=1	B=d	S, J

Actual Action

index	condition	act	tense	personality
~~21'~~	~~d<A<l∧d≦B<l~~		~~∃x.x+10:25+1~~	~~S~~
~~22'~~	~~Crash~~		~~∃x.x+10:25+1~~	~~S~~
21	d<A<l∧d≦B<l		∃x.x+10:25+1	
22	Crash		∃x.x+10:25+1	

- The responsible person of SKR decided that SKR (up) train started at 10:25 (4)
- Block signal did not rise. (negation of 5)
- 13R was not locked (negation of 8), and

  13R turned green for JR (down) train. (18)
- JR train entered the interval between Onotani and Shigaraki.(12)
- Therefore, there exists a tense x that 21and 22 do not hold.
- Namely, 21' and 22' hold, ie. Crash

Conclusion & Discussions

- Labeled @-calculus
  - a verification formalism for the time-concerned control systems involving human factor as human errors and unsuitable decision
    - based on the concrete and basic mathematical theory *PA*
    - Verification can be carried out in a consistent formal theory
  - An actual demonstration is shown: the formalism is easy to understand
  - Automated verification with human assistance may be relatively easy since it is besed on NK, whose automatic verification methods have beein studies well.