A LOGICAL FRAMEWORK FOR INTEGRATING SOFTWARE MODELS VIA REFINEMENT

Marie Farrell
Supervisors: Dr. Rosemary Monahan & Dr. James Power
MOTIVATION

Ariane 5
€350,000,000

Therac-25
3 Fatalities

$312 BILLION
Formal software engineering is a set of mathematically grounded techniques for the specification, development and verification of software and hardware systems.

A formal specification is the exact definition in mathematical notation of what the system is required to do (and not do).
The Event B formal specification language is used in the verification of safety critical systems.

Event B models are an instance of the specification.
Refinement provides a way for us to model software at different levels of abstraction.
MACHINE
  mae1
SEES
cxt1
VARIABLES
  person
  rawcontent
  content
  owner
INVESTIGATIONS
  inv1 : person ⊆ PERSON
  inv2 : rawcontent ⊆ RAWCONTENT
  inv3 : content ∈ rawcontent ↔ person
  inv4 : owner ∈ rawcontent → person
EVENTS
  INITIALISATION ≡
    STATUS
    ordinary
BEGIN
  act1 : person := Ø
  act2 : rawcontent := Ø
  act3 : content := Ø
  act4 : owner := Ø
END

transmit ≡
  STATUS
  ordinary
ANY
  rc
  pe
WHERE
  grd1 : rc ∈ rawcontent
  grd2 : pe ∈ person
  grd3 : rc ↦ pe ∈ content
THEN
  act1 : content := content ∪ {rc ↦ pe}
END

MACHINE
  mae2
REFINES
  mae1
SEES
cxt1
  cxt2
VARIABLES
  person
  rawcontent
  content
  owner
  viewpermission
INVESTIGATIONS
  inv1 : visible ∈ rawcontent ↔ person
  inv2 : viewpermission ∈ person ↔ person
EVENTS
  INITIALISATION ≡
    extended
    STATUS
    ordinary
BEGIN
  act1 : person := Ø
  act2 : rawcontent := Ø
  act3 : content := Ø
  act4 : owner := Ø
  act5 : visible := Ø
  act6 : viewpermission := Ø
END

transmit ≡
  STATUS
  ordinary
REFINES
  transmit
ANY
  rc
  pe
WHERE
  grd1 : rc ∈ rawcontent
  grd2 : pe ∈ person
  grd3 : rc ↦ pe ∈ content
THEN
  act1 : visible := visible ∪ {rc ↦ pe}
  act2 : viewpermission := viewpermission ∪ {owner(rc) ↦ pe}
END
Different formalisms do not integrate well e.g. Event B models the specification it does nothing for the implementation and its proofs are not easily transferable to other formalisms.
Establish a theoretical framework within which refinement steps, and their associated proof obligations, can be shared between different formalisms.

Hypothesis: the theory of institutions can provide this framework and, we will construct an institution based specification of the Event B formalism.
Category Theory is a special branch of Mathematics that allows us not only to describe objects but also to investigate the relationships between them.

Institutions are an application of category theory that allow us to relate the syntactic and semantic structures of different formal languages.
ALFRED TARSKI
1901 - 1983

- Polish mathematician/logician
- Born Alfred Tajtelbaum
- Travelled to the USA in 1939
- Harvard, City College of New York, Princeton and University of California at Berkeley

"Snow is white" is true if and only if snow is white

The concept of truth in formalized languages

P is true if and only if P
UBER EINIGE FUNDAMENTALE BEGRIFFE DER METAMATHEMATIK
ON SOME FUNDAMENTAL CONCEPTS OF METAMATHEMATICS

- Formalized deductive disciplines form the field of research of metamathematics
- These disciplines are regarded as sets of sentences
- The set of all sentences is denoted by ‘S’
- From the sentences of an set $X$ certain other sentences can be obtained using rules of inference
- These sentences are called the ‘consequences’ of $X$
- The set of all consequences is denoted by ‘$Cn(X)$’
ON SOME FUNDAMENTAL CONCEPTS OF METAMATHEMATICS

1930

- **Axiom 2:**
  
  \[ \text{If } X \subseteq S, \text{ then } X \subseteq Cn(X) \subseteq S \]

- **Axiom 3:**
  
  \[ \text{If } X \subseteq S, \text{ then } Cn(Cn(X)) = Cn(X) \]

- **Axiom 4:**
  
  \[ \text{If } X \subseteq S, \text{ then } Cn(X) = \sum_{Y \subseteq X \text{ and } |Y| < \aleph_0} Cn(Y) \]
Π - INSTITUTIONS

Alternative to institution – replacing the notions of model and satisfaction by Tarski’s consequence operator.

Definition:

A π-institution is a triple (Sign, φ, {CnΣ}Σ:Sign) consisting of

1. A category Sign (of signatures)
2. A functor φ:Sign -> Set (set of formulae over each signature)
3. For each object Σ of Sign, a consequence operator CnΣ defined in the power set of φ(Σ) satisfying for each A, B ⊆ φ(Σ) and μ: Σ -> Σ

(RQ1) A ⊆ CnΣ(A) (Extensiveness)
(RQ2) CnΣ( CnΣ(A) ) = CnΣ(A) (Idempotence)
(RQ3) CnΣ(A) = ∪B≤A,B finite CnΣ(B) (Compactness)
(RQ4) φ(μ)(CnΣ(A)) ⊆ CnΣ(φ(μ)(A)) (Structurality)

Marie Farrell

Tarski: Axioms 2, 3 & 4
CONCLUSION

- Tarski provided the foundations for \( \pi \)-institutions
- Work to date:
  - Denotational Semantics
  - Communicating Sequential Processes (Hoare)
  - Tarski
  - Consequence
  - Category Theory/Institutions/\( \pi \)-institutions
Any Questions?