Formal Method Approaches

Approaches of Formal Methods

There are two key approaches to formal methods

- Model-oriented approach
- Algebraic or axiomatic approach

Model-Oriented Approach

The model-oriented approach to specification is based on mathematical models, where a model is a simplification or abstraction of the real world that contains only the essential details.

Example

For example, the model of an aircraft will not include the colour of the aircraft, and the objective may be to model the aerodynamics of the aircraft.

There are many models employed in the physical world, such as meteorological models that allow weather forecasts to be made

Importance

The importance of models is that they serve to explain the behaviour of a particular entity and may also be used to predict future behavior.

Different models may vary in their ability to explain aspects of the entity under study.

One model may be good at explaining some aspects of the behaviour, whereas another model might be good at explaining other aspects.

Adequacy of Model

- The adequacy of a model is a key concept in modelling, and it is determined by its effectiveness in representing the underlying behaviour, and in its ability to predict future behaviour.
- Model exploration consists of asking questions, and determining whether the model is able to give an effective answer to the particular question.
- A good model is chosen as a representation of the real world and is referred to whenever there are questions in relation to the aspect of the real world.

Best Model Criteria

- There may be more than one possible model of a particular entity

for example, the Ptolemaic model and the Copernican model are different models of the solar system.

- This leads to the question as to which is the best or most appropriate model to use, and on the criteria to use to determine which is more suitable.
- The ability of the model to explain the behaviour, its simplicity and its elegance will be part of the criteria

Principle of “Ockham’s Razor”

- The principle of “Ockham’s Razor” (law of parsimony) is used in modelling, and it suggests that the

simplest model with the least number of assumptions required should be selected.

Models replacement

- Models that are ineffective will be replaced with models that offer a better explanation of the manifested physical behaviour.
- There are many examples in science of the replacement of one theory by a newer one.

For example

The Copernican model of the universe replaced the older Ptolemaic model, and Newtonian physics was replaced by Einstein's theories of relativity

Model Oriented Approach to Software Engineering

Modelling can play a key role in computer science, as computer systems tend to be highly complex, whereas a model allows simplification or an abstraction of the underlying complexity, and it enables a richer understanding of the underlying reality to be gained. The model-oriented approach to software development involves defining an abstract model of the proposed software system, and the model is then explored to determine its suitability as a representation of the system

The modelling in formal methods is typically performed via elementary discrete mathematics, including set theory, sequences, functions and relations.

VDM and Z

- VDM and Z are model-oriented approaches to formal methods.
- VDM arose from work done at the IBM laboratory in Vienna in formalizing the semantics for the PL/1 compiler in the early 1970s
- It was later applied to the specification of software systems.
- The origin of the Z specification language is in work done at Oxford University in the early 1980s.

Axiomatic Approach

- The axiomatic approach focuses on the properties that the proposed system is to satisfy, and there is no intention to produce an abstract model of the system.
- The required properties and behaviour of the system are stated in mathematical notation.

Example

The difference between the axiomatic specification and a model-based approach may be seen in the example of a stack.

The axiomatic specification of the pop operation on a stack is given by

properties, for example, pop(push(s, x)) = s.

The model-oriented approach constructs an explicit model of the stack, and the operations are defined in terms of the effect that they have on

the model.