Formal Specification Languages

The Vienna Development Method

- VDM was developed by a research team at the IBM research laboratory in Vienna.
- This group was specifying the semantics of the PL/1 programming language using an operational semantic approach.
- VDM is a model-oriented approach and this means that an explicit model of the state of an abstract machine is given, and operations are defined in terms of the state.

VDM

- Operations are defined in a precondition and post-condition style.
- Each operation has an associated proof obligation to ensure that if the precondition is true, then the operation preserves the system invariant
- The initial state itself is, of course, required to satisfy the system invariant.

VDM

- VDM uses keywords to distinguish different parts of the specification, e.g. preconditions, post conditions, as introduced by the keywords pre and post, respectively.
- In keeping with the philosophy that formal methods specify what a system does as distinct from how, VDM employs post conditions to stipulate the effect of the operation on the state.
- The previous state is then distinguished by employing hooked variables, e.g. v(and the postcondition specifies the new state which is defined by a logical predicate relating the prestate to the poststate

VDM

- VDM is more than its specification language VDM-SL and is, in fact, a software development method, with rules to verify the steps of development
- The rules enable the executable specification, i.e. the detailed code, to be obtained from the initial specification via refinement steps. Thus, we have a sequence S = S0, S1, …, Sn = E of specifications, where S is the initial specification and E is the final(executable) specification.

VDM

In view of this approach to types, it is clear that VDM types may not be “statically type checked”.

VDM specifications are structured into modules, with a module containing the module name, parameters, types, operations, etc.

Z-Specification Language

- Z is a formal specification language founded on Zermelo set theory, and it was developed by Abrial at Oxford University in the early 1980s
- It is used for the formal specification of software and is a model-oriented approach.
- An explicit model of the state of an abstract machine is given, and the operations are defined in terms of the effect on the state.
- It includes a mathematical notation that is similar to VDM and the visually striking schema calculus

Z Language

- The schema calculus is a powerful means of decomposing a specification into smaller pieces or schemas.
- This helps to make Z specification highly readable, as each individual schema is small in size and self-contained
- Mathematical data types are used to model the data in a system, and these data types obey mathematical laws.
- Operations are defined in a precondition/postcondition style. However, theprecondition is implicitly defined within the operation; that is, it is not separated out as in standard VDM

Z language

- The initial state itself is, of course, required to satisfy the system invariant.
- Postconditions employ a logical predicate which relates the prestate to the poststate and the poststate of a variable v is given by priming, e.g. v′.
- Various conventions are employed, e.g. v? indicates that v is an input variable and v! indicates that v is an output variable.
- The symbol N Op operation indicates that this operation does not affect the state, whereas D Op indicates that this operation affects the state.

Z language

- Many data types employed in Z have no counterpart in standard programming languages.
- It is, therefore, important to identify and describe the concrete data structures that will ultimately represent the abstract mathematical structures.

B Method

- The B-Technologies consist of three components: a method for software
- development, namely the B-Method; a supporting set of tools, namely the BToolkit; and a generic program for symbol manipulation, namely the B-Tool (from which the B-Toolkit is derived).
- The B-Method is a model-oriented approach and is closely related to the Z specification language.
- Abrial developed the B specification language, and every construct in the language has a set theoretic counterpart, and the method is founded on Zermelo set theory.
- Each operation has an explicit precondition