Overview of Formal Methods

When developing a new system, the first step is to write the requirement specification which is usually written in natural language and it should describe the behavior of our system in a complete way which can be hard to achieve since it depends on the programmer's skills to understand the specification correctly and this may lead to faults in the code. Formal methods introduce tools and techniques that use specified mathematical models to build software or hardware systems to describe a system in a specification. The methods used are mathematical proofs to ensure correct behavior. There are many types of formal methods and notations that we can use to build our software and hardware systems. For example, Abstract State Machines (ASMs) which is a state machines operating on states, and a state machine is "a mathematical abstraction used to design algorithms", A Computer Logic for Applicative Common Lisp (ACL2), Autonomic System Specification Language (ASSL) and many more. The importance of formal methods is to help disambiguate system specifications and expose errors in the system requirements process. The downside of using formal methods in building systems is the difficulty to write and proof it and it could be wrong even after we prove it. We said that formal methods are important in the system specifications process but in the real world they are not widely used because it has a high cost and is unfeasible. In formal methods, we use formality to avoid ambiguity in natural languages. Formal methods describe the system that is going to be developed. Another view of formal methods is proving properties about the specification which is called formal verification. Formal verification uses a logical system. For instance, first-order logic, and temporal logic. There are different ways to approach formal verification such as proof tools, and model checking. The first step used to choose a formal method is to find qualified people with a background in formal methods to help in deciding which formal method is going to be used in the project. Formal methods were developed for sequential programs at first then the focus changed to concurrent systems with the help of Petri nets. Petri nets are used for communication systems and mobile systems. Petri net is a "directed graph that has two types of elements, places, and transitions. Graphically we use circles for places and bars or rectangles for transitions. It is one of the several mathematical models that is used in Formal methods. In conclusion, Formal methods can be cost-effective and can reduce the number of possible flaws in the system. To take advantage of formal methods keep following the development of new methods and tools.

Written By Talal Albraik