The Specification of Railway Signalling in CafeOBJ

Takahiro Seino

School of Information Science,
Japan Advanced Institute of Science and Technology

February 15, 1999

Keywords: Formal Method, Formal Specification, Verification, CafeOBJ, Railway Signalling.

1 Goal of our research

Railway signalling systems are the most successful instance in the large scale distributed systems. In the railway signalling, the important concepts are "block system" and "interlocking". Block system defines how to divide a train track into sections such that at most one train can be in each section. Interlocking defines how individual devices of a signalling system interact each other to achieve safe operations. When some devices are in "locking relations", if one device is active then other devices are not able to be active.

In the railway signalling domain, the most important issue is how to define these block system and locking relations. We specify block system and interlocking relation in CafeOBJ. The specification is done by adopting distributed object modeling available in CafeOBJ. Based on this specification, we also show that some proofs of interesting properties can be done.

Most of applications of formal specification in the railways domain are in the interlocking design in train stations. These specifications usually defines a interlocking system in some specific station, and proofs of safety properties are done only by simulations. Contrasting to these previous applications, we try to specify "scheme" of signalling system and to prove safety properties about this "scheme". This implies that the properties proved is true for all signalling systems which belong to the "scheme". A new safe signalling system can be designed by instanciating the "scheme". It can be said that our method is much more powerful than the previous instance based one.

2 Method of specifying and proving

In our research, we wrote the specifications in algebraic specification language CafeOBJ. CafeOBJ is a direct successor of OBJ, it is advanced specification language that supports powerful module system, order sorted algebra, hidden algebra that is object oriented model. CafeOBJ also can execute the specifications by term rewriting engine with the equations regard as the rules of term rewriting.

Hidden algebra proposed by Joseph Goguen and Grant Malcom. The objects in hidden algebra are formalized by the operators of "action" and "observation" on hidden sort. The action operators represent the state of the object. The observation operators express that can get the states of object as visible sort. The relations of between these operators mean the object's behaviours, are given the "visible contexts" that applying observation operator after any action operators contexts. The relations are formalized by equations in CafeOBJ. The specifications based hidden algebra are called "behavioral specification".

In the behavioral specification, the equivalence relations of the objects define only observation. If the results of observant operators on two objects are equal to each other, and the result of after each action operators applying are also equal, these objects is behaviroural equivalence.

The composition that a object is composed of some objects, defines "projection operator". Projection operators mapped the state space of a composed object to component one. The operators is a very useful method to reuse both specification codes and proofs. If the component objects is behavioral equivalence, then we can prove that property of the composed object reuse their properties.

In large specification, it is difficult to prove that behavioral equivalence with induction by action operators' contexts (the proof technique is called context-induction that proposed by R. Hennicker). So, we define a hidden congruence relations in the objects. We did know a theorm of behavioural equivalence is the largest hidden conguruence. Therefore, we can prove the property of behavioral equivalence with coinduction using a hidden congruence relation. CafeOBJ interpreter can prove this automatically, we can show some properties of the specification by coinduction.

3 Fruits of our research

This paper shows the specification of two concepts of block system and the implementations in Japanese railway's signalling systems in CafeOBJ. We describe the specification of concurrent distributed and objects oriented model in the hidden algebra formalism and CafeOBJ's module system. The interfaces of objects define as action and observant operators, and concept of "interlocking" appears as projection operators and related equations in the specification. And safety properties based block system of the specification is proved in formal approach.

In the first, we defined bare railway system object. The system consists only rails and trains objects, and no signals or any other security devices. We will expand this system to consturct safety railway system.

The signalling system in the double tracks, consists rails, trains, track circuits (are train exsitence sensor), and signal objects. The system called "automatic block system". In this system, trains run only one direction on a track, we considered to defend a rear-end collision. First, we divide tracks into some sections, and the track circuits construct these sections. Signals that build the beginning side of each sections. If there are one or more trains on its defending section, the signal show stop signal (R, is an abbreviation of red light) . If there is no trains on the section, the signal shows go signal(G, is green light). Today, signals show that not only G or R, also such as Y (is yellow light means caution) or YY (double yellow lights mean warning) or YG (yellow and green lights means slow down) give notice that next signal is R, because this signalling system matches high speed or high density train running. We describe the specifications of modern railway signalling system, and prove to keep the block system by coinduction without depending the number of sections, number of trains, or the length of tracks.

In single track railway, trains run bi-directions on a track between two stations. So, the signalling system defend not only a rear-end collision, but also a head-on collision. Therefore, that system needs a direction levers objects to determine a direction for trains running between two stations and the facilities for exchange trains. In japan, there are many solutions of this problem, we choose the most basically, but modern system that called automatic block system type-B. This system has interlocking relations on track-circuits, direction levers, exit signal levers, exit and entry signals objects, such as exit signal levers locked while there is train between two stations. We describe that specification, and show that system happens never a head-on collision, and keeps block system by coinduction. We show that locked devices can not transit other states, too.

These specification is a limited edition, but it does not depend the geometry of tracks. This paper shows new design method that railway system is composed already proved component tracks with railway signal. The methods are able to apply other implementations of block systems, and any other problems on the other domains.