Application Of Formal Verification Method's Tools

Ekta Patel

5009,corning ct,plainfield IL,60586

1st semester of master of computer science

Lewis university,Romiovilee

ektabenppatel@lewis.edu

Abstract-In this paper I would like to focus on how the formal methods is useful for digital system in the industry and also I like to discus about how the formal method is useful for analysis and verification in the program life-cycle. In the digital system formal method is widely use full for the safety and security purpose. In digital system there is a group of requirement where testing is mostly ineffective.

In industry for the digital system, formal method is repeatedly useful for the design and verification purpose. Also in this paper I would like to discuss how the open source formal tools and capacity of commercial formal method tools can be work in digital design workflows. Also there is some issue in industry when they adopt the formal method in there system. Based on that also we described and develop the verified software repository.

Key Words:

formal method verification, Digital system, verified software repository, safety and security verification, open source formal tools, capacity of commercial formal tools.

i. INTRODUCTION:

Hardware and software are use formal method for mathematically computerize in order to solve problem. Every think digital machinery it self work for computation logic. In the digital system they make combination through one state space with other different state space and make imagination for real problem.

In discover a mathematical rules also Calles the Turing halting problem, for normal digital system are at deterministic and unsure , and now a days , this is the main cause of the cyber security problem so much. And also for a certain level of security and safety purpose we can use the combination of formal method and digital design process.

For a testing and simulation purpose we can enter verity of input and make a combination with other randomly generated input from which we can get a certain output , which is helpful to us to reach some predictable result.

In the mathematical area user can analyze and verify model at any state of the program life cycle. Formal methods are also useful for extract, prompt and representing requirement.

ii. A SUMMARY OF PAPER :

In this paper they verify the digital system by applying the formal method and also doing some testing to get appropriate result . through the verification they verify that critical problem for simple digital system is also cannot be easily uncovered by the testing. For that we need to apply floating point bug in there system's processor. And it also not covered by extensive testing, and it is also prevent by rare user.

If we want to analyze mathematically of digital system then also we can consider formal method to do this. For the safety and security purpose in the digital system there is very vast combination of data so we need to transfer it to make quantitative by the use of formal method only. There is a two types of category available in formal method, one is model checker and another one is theorem proving.

There is a so many model checker are available , and for providing source code some of them are auto metically apply on design information. While commercial off-the shelf tools are very impressive because it focus only on specific domain problem and verify the proper and it is very helpful in industry level. there is also limitation of handling the problem by COTS. But whatever they handle that is very aggressively handle the problem and solve it.

If we looking solve the problem then at a complex level , specification of that complex level it may be unenhanced in to low level of specification. Witch is introduced the sub component of the system. For the software design we can also use the formal method. For data refinement it specify every state of the machines . Also it give us the very detail about it in allies we can tell that it also support for abstract level of information.

iii. APPLICATION THAT I CHOOSE FROM ONE OF THE PAPER:

I want to discuss about telecommunication area . I want to focus on how this area are work and which type of formal method are used in this area. And how it is effected to our application area of formal method. Formal method is very help full to solve the problem which is hard with informal method, that is help to solve the problem with mathematically formula and we can make sure about safety and security purpose.

A. RATIONALE OF THE GIVEN APPLICATION :

In this paper I want to focus on verifying the telecommunication process, in the other word if I can say that then it is the verification of call processing on telephone switches. telecommunication is open source facility. Now a day it is very punctually developed and maintained by the NASA. In 2001 it got award by the ACM software system. It show the how we can communicate very speedily with each other within a second or minute, from one place to another end place.

B. RELEVANCE OF THE FORMAL METHODS IN THE APPLICATION AND THE TYPE OF FORMAL METHODS USED:

In the processing on telephone switches , model checker are used as a formal method verification. On the model's state space of the desire property for the verification we need to apply model checker because it apply very short form of the algorithm for the verification. In that they use Spin type of model checker. On the software algorithm for the formal verification , spin is first preferable by everyone , specially for the simultaneous, and multy-threaded algorithm.

It is also very good model for the inequality in the system at the interconnected components. Spin models are also written in Promela. In the syntax it is same as C language.

For the verification state it is very small process that everyone can get. Most of promela method describe the high level property which is very difficult to solve. It is always analyze two type of property: one is detailed property of small model and other is high-level property of large system. We can also say that two type of method is that:

(1) detailed property of small model

(2) high-level properties of large systems

For the telecommunication process, Spin is an explicit-state model-checker. It test and verify for the rechability of the call when any number is dial from any use a and it reach at other end user side. It also provide the safety and security purpose, so no one can track your call and no one can here your personal conversation between each other.

If I talk about promela then it supports indeterminate environment. Promela also support the simple problem situation at low level communication process for the local call and also it support the complex linear temporal logic property for the large distance communication process for the international call.

For the concurrent system spin is very use full for analyzing it. There is also one solution of the exclusion problem, which is successful without atomic sequences. Spin is highly useful for analyzing co- existent systems.

Before the promela, Dikstra is the First attempted and work to get solutions to the mutual exclusion problem without using atomic sequences. And at that time for that there is number of presentation for same kind of algorithm , and most of them is going to be fail to get proper result. but formal method is work very calmly and great help full to solve the problem with telecommunication system. With the spin type of model checker in the formal verification method we can do the only small changes in our existence system abd get the appropriate result with only few kind of changes. That's why model checker is very much use full for the telecommunication process or the call processing on phone switching process.

So, basically for the telecommunication process or the call processing on telephone switches, we use the model checker type of the formal verification method.

C. SUMMARY OF AN EXTRA RESEARCH DONE ABOUT THE APPLICATION :

telecommunication system is first written in the informal language. But in that there is so many complication and so longer sufficient for describing their requirements. To solve this problem they use the formal verification language in that they use three type of different languages is the : Estelle, LOTOS, and SDL. In telecommunication system there is so mu ch requirement for solving the problem.

There is also two type of describing system one is interaction between user and devices in other word it is also called user and system means that it called interaction between user and device, another one is communication between telecommunication system with the one another in other word it is also called system to system. Means that there is only interact between system to system.

In other word in the telecommunication system there is a problem with the communication between one to end user, in that there is call crashes and record the communication between two user and for that problem they use formal verification method's model checker tools in that they handle and make the control between each and every action between one user to end user.

iv. CONCLUSION:

Personally I believe that formal methods had been applied to significant systems. Also I believe that formal method is mostly use for deciding that what actually software is to do ? , it is not about the how it is reach or achieve the solution of the critical problem.

Now a day's model checker are very use full by everyone , and specially for digital system, model checker are work very impressively for the testing and verification. In model checker of the formal verification , human do not need to do work much hard, because it work itself by use of system language and fix the high level of complex system. And it does not tack much time consume. It give the result very quickly.

Generally theorem proving is more power full then model checker but in theorem proving human need to be more intervention and he/she need to be creative in that type of formal verification method. Basically theorem proving is also mathematically solution of the problem but it is very time consuming process. It is very slow process compare to model checker.

v. REFERENCES:

[1] file:///C:/Users/eku/Desktop/Download/fm_app.pdf

[2] file:///C:/Users/eku/Desktop/Download/survey_formal_tools.pdf

[3] Abrial, J.-R. 1996. The B-book: Assigning Programs to Meanings. Cambridge University Press, Cambridge.

[4] Abrial, J.-R. 2007. Formal methods: Theory becoming practice. JUCS 13, 5, 619–628.

[5] Allen, R. 1997. A formal approach to software architecture. Ph.D. thesis, School of Computer Science, Carnegie Mellon University. Issued as CMU Technical Report CMU-CS-97-144.

[6] G. J. Holzmann, The Spin Model Checker. Addison Wesley, 2004.

[7] M. Ben-Ari, Principles of the Spin Model Checker. Springer, 2008.

[8] D. Jackson, Software Abstractions: Logic, Language, and Analysis. MIT Press, 2006.

[9] "Simulink design verifier." http://www.mathworks.com/.

[10] 1850-2005 IEEE Standard for Property Specification Language (PSL). IEEE, 2005.

[11] 1800-2009 IEEE Standard for Property Specification Language (PSL). IEEE, 2009.

[12] BLAST. http://mtc.epfl.ch/software-tools/blast/index-epfl.php, 2008.