National Institute of
Advanced Industrial Science
and Technology
AIST

AIST-PS-2009-005

Fieldwork and the 4:6 Principle - Introduction to the Research Center for Verification and Semantics, AIST

Yoshiki Kinoshita

Research Center for Verification and Semantics (CVS)

算譜科学研究速報

Programming Science
Technical Report

Research Center
for Verification and Semantics

独立行政法人 産業技術総合研究所 システム検証研究センター 発行
Published by Research Center for Verification and Semantics
National Institute of Advanced Industrial Science and Technology

Fieldwork and the 4:6 Principle—Introduction to the Research Center for Verification and Semantics, AIST

Yoshiki Kinoshita
Research Center for Verification and Semantics (CVS)
National Institute of Advanced Industrial Science and Technology (AIST)
Senri, Japan
yoshiki@m.aist.go.jp

Abstract

The principles in the Research Center for Verification and Semantics (CVS) AIST are explained with summaries of some of its research projects.

1. Introduction

The principles in the Research Center for Verification and Semantics (CVS), The National Institute of Advanced Industrial Science and Technology (AIST) will be explained with summaries of some of its research projects. As CVS is one of the research centers of AIST, we cannot explain the prinples of CVS without mentioning that of the whole AIST.

So, this paper is organised as follows. In Section 2, we give an overall figure of how research centers are organised in AIST, and explain its motto 'Full Research,' as well as 'Type 1 Basic Research,' 'Type 2 Basic Research' and 'Product Realisation Research.' In Section 3, we introduce our 'Fieldwork', which could be considered as one of the methods of implementing Type 2 Basic Research, and Section 4 describes how CVS conducts the Type 1 Basic Research. Section 5 is about '4:6 principle,' how we expect interaction between the Fieldwork and Type 1 Basic Research. Finally, Section 6 summarises some of the research projects conducted by CVS.

2. Full Research

AIST launched the Laboratory for Verification and Semantics in April 2003, which changed its form to the Research Center for Verification and Semantics (CVS) in April 2004, a year later. Its mission is to transfer technology as well as to conduct research on Formal and Semiformal Methods in system verification and to transfer the related technology to the industry. Hereafter, we use the term *Mathematical Methods* to mean both Formal Methods and Semiformal Methods. Mathematical Methods inevitably includes the step of building mathematical models of the system, so research on semantics of information processing systems is naturally included in the mission of CVS.

AIST is a research institute governed by METI (the Ministry of Economy, Trade and Industry), conducting research in a wide range of area related to industry, not only in computer science and electronics but metrology, geology, life science and material science, chemistry and others. It has more than 3000 tenure position in research and management, and its ten regional centers spread all over Japan, amongst which Tsukuba center is the largest, more than half of tenure position located in it. Kansai (in Osaka), Chubu (in Nagoya) and Tokyo Waterfront centers are next largest ones, each having ca. 200 tenure positions.

AIST set up three kinds of its research units: Research Institutes, Research Centers and Research Initiatives. A Research Institute is established for each research field: Information Technology Research Institute and Intelligent Systems Research Institute are two informatics related research institutes.

AIST organises a Research Center for each contemporary research topic considered to be important, and allots research resource such as budgets and research positions with priority. On the other hand, a term of duration, maximum of seven years, is always decided for a Research Center upon its establishment, while no such term is settled for Research Institutes.

Research Initiatives could be considered as a preliminary form of Research Centers, so they may start with higher risk than the latter; they therefore have shorter maximum of term of duration: three years.

The establishment of Full Research structure has been the leading principle of AIST since Yiroyuki Yoshikawa, its president, introduced the notion in 2002[1]. As CVS is one of the research centers of AIST, its research principle is heavily influenced by this motto. So we need explain about Full Research principle here.

Full Research consists of three kind of research activities: Type 1 Basic Research, Type 2 Basic Research and Product Realisation Research. Moreover, these three are expected to be conducted in parallel, interacting with each other; they are not necessarily conducted in sequence.

Type 1 Basic Research amounts to usual scientific basic research. It is defined to be research to discover, clarify, and form universal theories, such as natural laws, principles, and theorems, by observing unknown phenomena, conducting experiments, and pursuing theoretical calculations.

Type 2 Basic Research, on the other hand, is an action of synthesis of a solution method, so that one can solve a given goal. It is defined to be research to find specific routes that can lead to universal and reproducible knowledge by integrating existing theories, such as natural laws, principles, and theorems, and conducting observations, experimentation, and theoretical calculation to fulfill certain socio-economic needs. It is *synthetic*, while Type 1 Basic Research is *analytic*, and is supposed to support the *Death Valley*.

When a new principle which seems to be useful for something is found, people instantly gather around enthusiastically. But such a enthusiasm goes away in a short period, while it of course takes years for that principle to become really usable. During those years, the researchers who seriously tackles the realisation of that principle must face with a worse and worse research environment: lost interest of people, less amount of budget, etc. Such nightmare period is generally called Death Valley.

The research needed during the Death Valley is to take every thing one can to synthesise the use of the new principle. That is exactly what Type 2 Basic Research aims at. Being a governmental research institute independent of universities, AIST finds Type 2 Basic Research to be central in its road map. The Type 1 Basic Research could be the main target of universities, and Product Realisation Research could be that of research institutes in industry. Of course it does not imply that AIST does not conduct any Type 1 Basic Research nor Product Realisation Research. In fact, if one looks closely at research conducted by a specific researcher in AIST, it may entirely be Type 1 Basic Research, while another researcher may be devoted totally to Product Realisation Research. The above view only states that the AIST research activity *as a whole* has emphasis on Type 2 Basic Research.

3. Fieldwork—Type 2 Basic Research

It is common nowadays for research institutes to insist on contribution to the society, not simply comfortably sitting inside an ivory tower. AIST is no exception. In order to meet this requirement CVS set up the principle of *Fieldwork*.

Fieldwork originally is a technical word used in ethnography and other area of social sciences, which means research carried out 'in the field.' In particular, we use the term in two meanings: to do with technical transfer and to observe the system development process, taking part in such a development project in industry. The former involves the information flow from CVS to industry, while the latter from industry to CVS. In both cases, Fieldwork is the gateway to the society for us and it is in course of Fieldwork that CVS can discharge its social responsibility.

It is often regarded that technology introduction is an issue which should be solved by consultation outside academia, but a brand new technology such as model checking and other techniques in Mathematical Methods could only be consulted at academia.

What CVS would expect to gain from Fieldwork is, above all, the case study of introducing a new technique to a development process. In order to apply a new methodology to an actual development process in industry, results of experiments *in vitro* is far from adequate and the analysis of case studies done in the field is necessary. Fieldwork also give researchers wider perspective, hence cause a better balance in research theme decision.

The research partner who provides the field would naturally profit by technology transfer. An introduction of a new technology to development process requires a great amount of knowledge left implicit and not written in textbooks. Also, the basic theory must be adapted to each field. All these happen inevitably during the experimental introduction of new technology.

3.1. A scenario for Fieldwork

An experiment is started by the engineers of the research partner who offers the field shows CVS some possible research themes which they think relates to the new technology, say, Mathematical Methods. Not being a specialist in Mathematical Methods, the research partner cannot judge whether Mathematical Methods could really be effective on those proposed themes, so they must discuss with CVS whether each of these possible themes is relevant to Mathematical Methods.

For the sake of such a discussion, CVS side must understand, often has to learn much about, the domain of the research partner's development. It is often the case that CVS researchers must understand even those technical words and concept which are not directly relevant to verification. This process is recently identified as *domain engineering* and is not an easy task. If the research partner has their own research institute, they could work as an interpreter between the engineers of the research partner and CVS.

After the discussion, the target theme of the experimental introduction is decided.

The partner's trust in CVS, by the way, is necessary for easy conduct of the project, and such trust often grows up as the collaboration proceeds.

Usually, the partner starts by providing 'dead examples,' such as the record of development project already finished or the document for an old prototype which was created several years ago. At this stage, doing a blind test could done whether Mathematical Methods can find a bug which is recorded in the documentation.

Through these works, more and more trust is often placed upon CVS and the partner eventually start to provide 'live' examples which is directly connected to their own development, which has its own severe deadline and whose failure immediately could cause a negative financial effect of their performance.

Such live examples, however, are exactly what is needed for experiments *in vivo*. So, it is only at this stage of the project that the problems in applying the new technique to the real development is made explicit and CVS can start necessary academic research to solve them, or can change the policy in personal training and education.

3.2. Publication

The result of Fieldwork should in principle be made public through academic journal or conference so that it can be shared in the research community. There are, however, some issues to considered in publicising Fieldwork results.

To keep the trade secrets of the partner is a large issue in publication. In the current case, Mathematical Methods themselves are seldom trade secrets, but the development process to which Mathematical Methods are being introduces has many information to be kept secret. Therefore, it is often the case that one can write necessary facts about the application of Mathematical Methods, still carefully avoiding the trade secrets of the partner.

It is advisable to make the conditions of publication of the research result as clear as possible in the collaboration contract at first.

3.3. Training as Product Relisation Research

Experimental introduction of Mathematical Methods to development processes in industry naturally involved training of engineers, since Mathematical Methods can never be introduced without such training. So, CVS prepared materials for engineers of short courses on model checking, for instance.

Such provision of personal training may be regarded as 'Product Realisation Research' in the case of research on methodologies such as Mathematical Methods.

3.4. Qualitative research on software engineering

Fieldwork has a number of analogies with clinical medicine. The partner corresponds to the patient, the disease to the problems in system development and the doctor to the Mathematical Methods researcher. This suggests that it takes a long time for meaningful results in this direction to make shape.

Another aspect of Fieldwork is its qualitative nature. People may tend to seek too much for quantitative framework of research. There are obviously fields where qualitative research[2] works better than quantitative approach. In some cases it only shows immaturity of the latter, but in other cases qualitative approach seems to be the only effective one. It is suggestive that qualitative approach is much appreciated in nursing and healthcare, which is closely related to clinical medicine. Narrative approaches, interviews, story or scenario setting and other techniques in qualitative research all seem to work well in experimental introduction of Mathematical Methods.

4. Type 1 Basic Research

Researchers in CVS do not have uniform common base of knowledge, as their background varies from mathematical logic, algebra to computer science and system engineering. Mathematicians in general must augment their knowledge by computer science, and Computer scientists by mathematics.

To make scientific communication easier, CVS recommends three subjects, which could work as vehicles for CVS researchers to exchange their ideas.

The recommended subjects are

1) **Category theory**, for communication related to semantics,
2) **Intuitionistic Type Theory**, for communication related to logic and theory of computation (λ calculus) and
3) **Haskell**, for communication reltated to programming.

This is only a recommendation and researchers are not forced to learn these nor inhibited to learn other things; there were in fact projects which used JAVA for the needed programming, for instance.

Among these three things, Intuitionistic Type Theory has been most successfully spread out in CVS. It is probably because Agda system, the language for a proof assistant which Chalmers University of Technology and CVS has been developing, is based on predicative Intuitionistic Type Theory. Several project in CVS used Agda. Researchers participated in those projects was exposed to the basic idea of Intuitionistic Type Theory through using Agda. So, it is now rather easy in CVS to exchange ideas in terms of Intuitionistic Type Theory.

The idea behind putting Category Theory in the list is to exchange mathematical ideas in terms of adjunctions, so that one could have saved many words. In spite of two intensive lecture courses held exclusively for CVS researchers, Category Theory unfortunately has not spread out well amongst CVS researchers yet.

Haskell is now being replaced by Agda language, regarded as a programming language. As written above, a number of researchers can now use Agda, so it is convenient to talk about programming in terms of Agda.

5. 4:6 principle

Fieldwork could be considered as 'industrial duty' which corresponds to 'educational duty' in universities. AIST researchers have no educational duty as a part of AIST job, although many researchers have university posts and take care for graduate students. So, such industrial duty seems to work as a good stimulation, which prevents researchers from being too narrow minded.

Such thought lead us to the idea that it would be good for every researcher to be involved both in Fieldwork and Type 1 Basic Research. Moreover, we naturally look for a good effect of interaction between Fieldwork and basic research.

Usually, CVS set up research themes of Fieldwork and assign it to researchers, while each researcher proposes his/her own basic research theme to CVS and CVS admits it unless it could not be placed in CVS's mission and achievement plan.

So, each researcher in CVS is asked for taking part in both Fieldwork and basic research, with the 40% of manpower for Fieldwork and 60% for basic research. Of course we do not try to measure these percentages in exact manner, but they only mean both should be seriously done, with a little more effort for basic research. Careless persons would instantly imply from the ratio that we attempt to do more on basic research, but in fact, our result could be found much more in Fieldwork than in basic research. It is because to produce an equal amount (not to mention about the exact definition of 'amount') of results, much more effort is required in basic research than in Fieldwork, as the direction of research is easily determined in Fieldwork while such decision is a large part of basic research.

It is important, by the way, that we seek for *synchronictic* relation, rather than *causality* relation, between Fieldwork and Type 1 Basic research.

One of the frequent questions we have got so far is which of the element technologies emerged out of basic research is used in Fieldwork, or which phenomenon observed in Fieldwork affects which theory emerged out of basic research. But such seek for causality between Fieldwork and basic research could easily become meaningless, since Fieldwork and basic research are done in different system of valuation. Fieldwork is done according to the valuation in the society (e.g., industry), while Type 1 Basic Research is done following the evaluation in academia, so they are simply different works.

We expect something may happen in one's brain when one is involved both in Fieldwork and basic research. Sometimes one may think about one's Type 1 Basic Research while one is doing some work for Fieldwork, and vice versa. Such may give rise to synchronictic relation between Fieldwork and basic research.

6. Some research projects in CVS

In this section we list some of the research projects conducted by CVS / AIST; some had been completed and the others are still being conducted. Among these, the development of Agda, study of pointer analysis using modal logic, study of equational tree automata (ETA) and study of first order modal μ calculus (FOMμ) can be classified as Type 1 Basic Research, while others can be regarded as Type 2 Basic Research.

6.1. Type 1 Basic Research

6.1.1. Agda. Agda[3] is a proof assistant based on predicative intuitionistic type theory. Enjoying Curry-Howard correspondence, its input language (Agda language) can be regarded both as a programming language as well as a specification and proof description language. Agda system consists of the type checker including term evaluator, the emacs interface to the type checker and the compiler. The former two together forms a structural editor.

Agda has been developed by the Programming Logic group in Chalmers University of Technology, and CVS started colloaboration with respect to the development of Agda in 2004.

6.1.2. Pointer analysis using modal logic. Takahashi and others introduced an approach to verification of pointer handling programs[4], [5], [6]. There, they consider a Kripke model where the base set is the set of memory cells and the binary relation is the 'being pointed to' relation. They further develope the alternation free propositional μ calculus with nominals, which can conveniently be used to represent properties of those Kripke models.

Although precice comparison with Reynolds' separation logic, another logic for pointer analysis, still remains, alternation free modal μ calculus with nominals works well with global properties of pointer structure. In fact, Takahashi et. al. reported a best balanced result on verification of Schorr-Waite algorithm, which is remarkably faster than the previous results using solely automated verification tools, with much shorter description than the previous results using proof assistants[7].

6.1.3. Equational tree automata (ETA). Ohsaki gave some pioneering results as for decidability in the theory of equational tree automata, where the acceptance of tree languages by a tree automaton modulo equations is studied[8], [9], [10], [11], [12]. Decision problems for acceptance modulo various classes of equations, e.g., commutative laws, identitiy laws, associativity was studied, as well as whether the class of accepted languages is closed under union, intersection and complement.

The equational tree automata theory is considered to open a new technique for automated verification. For instance, one may wish to consider a tree language modulo commutativity in the verification of correctness for encripted communication protocol, where operations for encription and those for water marking are supposed to be commutative.

6.1.4. First order modal μ calculus. Okamoto introduced the syntax and (standard) semantics, as well as deduction rules of the first order modal μ calculus (FOMμ), a natural extention of the propositional modal μ calculus to the first order setting[13]. The set of all valid sentences of FOMμ, however, is not recursively enumerable, if one takes the standard semantics for the definition of validity. This means FOMμ is not recursively axiomatisable. Therefore Kashima and Okamoto introduced the general semantics, with the similar idea of general semantics for the higher order logic, and showed it is sound and complete with respect to the deduction rules of Okamoto[14]. To investigate the applicability of the system to the description of reactive systems, Okamoto gave a FOMμ formalisation of Dijkstra's algorithm of mutual exclusion for unbounded number of processes and its proof of correctness.

6.2. Fieldwork

6.2.1. Experimental introduction of model checking. CVS has a series of project in introducing model checking to software development lines in industry. The most notable result is a case where a guideline for a task of verifying a module, which had taken two months by an experienced person, was provided so that it takes nine days by a person. The development of that guideline itself took ca. a year and a half. Development methodology is rather difficult to make shape, but a guideline or manual seems to be one of the technically useful as well as persuading form to give shape to it.

6.2.2. Model Checking Training Course. Experimental introductions of model checking to industry necessarily involved tranferring model checking practice to engineers. This ended up with creating CVS training courses. Currently CVS has two model checking courses; the first course teaches the basic use of model checkers[15], while the second course involves abstraction as well as various tehcniques for composing transition systems, which is necessary for the use of model checking in industrial setting[16]. In preparing these courses, care was taken so that the students would not be dependent of the particular model checking tool they use, according to the thought that the students' knowledge should be classified into two: tool dependent knowledge and tool independent understanding of the idea of model checking.

CVS training courses is not limited to model checking, but a course for proof assistants is now being started, as proof assistants are becoming more and more important as tools which support the early stages of system development.

6.2.3. Model-based testing. In collaboration with Renesas Inc., and with the funding of JST, CVS conducted a research project of applying Agda, proof assistant based on intuitionistic type theory, to model-based testing[17].

Renesas has its own know-how to generate test cases for LSI, where one writes a list of boundary conditions and there is a program which, given a list of boundary conditions, generates a set of test cases, ready to be input to the test harness (a software which executes the testing job). It is a fairly automated scenario, yet one has to squeeze manually a list of boundary conditions out of a specification of instructions. This step being manually done, there is naturally a room for error to be introduced at this step, and one omission of a small boundary condition may cause hundreds of thousands of test cases, hence the test may become incomplete.

In this project, a machine-readable, executable specificaiton of instructions of an LSI in Agda was first developed. Then, a program which generates boundary conditions, given an executable specification and a description of 'know-how' of how to squeeze a list of boundary conditions out of a specification of instructions. So, the task of squeezing a list of boundary conditions out of a specification of instruction is replaced by the task of writing down those know-how in our new scenario. We expect the reduction of man power to be one fifth of what was necessary in the old scenario.

References

[1] AIST, "A new methodology for research—type 2 basic research and full research," 2002. [Online]. Available: http://www.aist.go.jp/

[2] U. Flick, *An Introduction to Qualitative Resaerch*, ser. Cram101 Textbook Outlines. Academic Internet Publishers, 2006.

[3] "Agda wiki." [Online]. Available: http://appserv.cs.chalmers.se/users/ulfn/wiki/agda.php

[4] Y. Tanabe, T. Takai, T. Sekizawa, and K. Takahashi, "Preconditions of properties described in ctl for statements manipulating pointers," in *Supplemental Volume of the 2005 International Conference on Dependable Systems and Networks (DSN-2005)*, 2005, pp. 228–234.

[5] Y. Tanabe, K. Takahashi, and M. Hagiya, "A decision procedure for alternation-free modal μ-calculi," in *Advances in Modal Logic*, vol. 7, 2008, pp. 341–362.

[6] T. Sekizawa, Y. Tanabe, Y. Yuasa, , and K. Takahashi, "Mlat: A tool for heap analysis based on predicate abstraction by modal logic," in *Proceedings of the IASTED International Conference on Software Engineering (SE 2008)*, 2008, pp. 310–362.

[7] Y. Yuasa, Y. Tanabe, T. Sekizawa, , and K. Takahashi, "Verification of the deutsh-schorr-waite marking algorithm with modal logic," in *Second IFIP Working Conference on Verified Software: Theories, Tools, and Experiments (VSTTE'08)*, ser. Springer Lecture Notes in Computer Science, vol. 5295. Springer-Verlag, 2008, pp. 115–129.

[8] H. Ohsaki, "Beyond regularity: Equational tree automata for associative and commutative theories," in *Proceedings of 15th CSL, Paris (France)*, ser. Springer Lecture Notes in Computer Science, vol. 2142. Springer-Verlag, 2001, pp. 539–553.

[9] H. Ohsaki, J.-M. Talbot, S. Tison, and Y. Roos, "Monotone ac-tree automata," in *Proceedings of 12th LPAR, Montego Bay (Jamaica)*, ser. Springer Lecture Notes in Artificial Intelligence, vol. 3855. Springer-Verlag, 2005, pp. 337–351.

[10] J. Hendrix, H. Ohsaki, and M. Viswanathan, "Propositional tree automata," in *Proceedings of 17th RTA, Seattle (Washington)*, ser. Springer Lecture Notes in Computer Science, vol. 4098. Springer-Verlag, 2006, pp. 50–65.

[11] H. Ohsaki and H. Seki, "Languages modulo normalization," in *Proceedings of 6th FroCoS, Liverpool (England)*, ser. Springer Lecture Notes in Artificial Intelligence, vol. 4720. Springer-Verlag, 2007, pp. 221–236.

[12] N. Kobayashi and H. Ohsaki, "Tree automata for non-linear arithmetic," in *Proceedings of 19th RTA, Hagenberg (Austria)*, ser. Springer Lecture Notes in Computer Science, vol. 5117. Springer-Verlag, 2008, pp. 291–305.

[13] K. Okamoto, "Formal verification in a first-order extension of modal mu-calculus," to appear in Computer Software.

[14] R. Kashima and K. Okamoto, "General models and completeness of first-order modal mu-calculus," *Journal of Logic and Computation*, vol. 18, no. 4, pp. 497–507, 2008.

[15] R. C. for Verification and Semantics, *Model Checking in four days, Elementary Level (in Japanese)*. NTS, 2006.

[16] ——, "Model checking, middle level (in japanese)," Research Center for Verification and Semantics, AIST, Tech. Rep., 2008.

[17] T. Abe, T. Higuchi, R. Imai, Y. Kinoshita, S. Nakano, K. Okamoto, M. Saito, and M. Takeyama, "Formalization of system lsi specification and automatic generation of verification items," in *Supplementary Proceedings of TESTCOM/FATES 2008*, 2008, pp. 75–76.

フィールドワークと四分六の原則 - システム検証研究センター紹介　(in English)
(算譜科学研究速報)
発行日：2009 年 6 月 8 日
編集・発行：独立行政法人 産業技術総合研究所 (システム検証研究センター)
同連絡先：〒560-0083 大阪府豊中市新千里西町 1-2-14 三井住友海上千里ビル 5F
TEL：06-4863-5025
e-mail：informatics-inquiry@m.aist.go.jp

Fieldwork and the 4:6 Principle - Introduction to the Research Center
for Verification and Semantics, AIST
(Programming Science Technical Report)
8 June 2009
(Research Center for Verification and Semantics (CVS))
National Institute of Advanced Industrial Science and Technology (AIST)
5F Mitsui Sumitomo Kaijo Senri Bldg., 1-2-14, Shinsenrinishi-machi, Toyonaka,
Osaka 560-0083 Japan
TEL：+81-6-4863-5025
e-mail：informatics-inquiry@m.aist.go.jp

AIST01-J00022-95