Research Center for Verification and Semantics
産業技術総合研究所 システム検証研究センター
News Letter
2
2005.11

社会の中のシステム検証技術

以下は第二回システム検証の科学技術シンポジウムにおける講演からの抜粋である。

システム検証の科学技術が社会に貢献する形に大きく分けて二つあると私どもは考えております。一つは、バグ検出の技術、あるいはそもそもバグの出来ないような開発技術を提供して、システム開発の生産性や信頼性を向上させる、というもので、開発者のための側面といえましょう。もう一つは、利用者のための側面で、情報処理システムの品質保証のための基準認証のためにシステム検証の技術を使おう、というものです。

◆開発者のための検証技術

バグ検出の技術としての側面では、数理的技法による検証法がバグの早期発見を可能にすることが重要です。バグ検出の時期が、仕様作成、詳細設計、コーディング、テスト、出荷という一連のシステム開発過程の後になればなるほど、手戻りのコストが高くなるのはご承知のとおりです。

我々は、システム開発の現場に参加して、開発中のシステムのバグ検出を、モデル検査などの数理的技法を用いて試みる、という活動を行っております。そこでは、数理的技法による検証を用いて反例が出ても、すぐにバグが見つかったと結論するわけにはいきません。誤解などのせいで、数理モデルが対象システムを正しく反映しているとは限らないからです。そこで、反例がでたら、それがバグを示しているのかどうかを設計者に判定してもらうことになります。設計者はそれをバグだという場合もありますし、数理モデル構築の際の誤解を指摘する場合もあります。このように、数理モデルを作ってはモデル検査などで反例を出してバグかどうかを判定する、という作業を繰り返して、出来るだけ多くのバグを検出しようとするのが数理的技法によるシステム検証です。

インパクトがあるのは、組み込みソフトウェアの検証で、ハードウェアの実機が出来上がってくる前に、かなり複雑な割り込み事象列を含んだ反例を出して、それがバグだとわかるような場合です。「実機がないのに、どうしてそんなややこしい事象列がみつかるのだ？！」と技術者に驚かれたことが何度かあります。

◆利用者のための検証技術

情報化が進むにつれ、情報処理システムの品質を何らかの方法で保証してほしい、認証してほしいという要求が出てくるのは自然でしょう。一次産業の JAS マーク、二次産業の JIS マークにあたるお墨付きが三次産業あるいは情報産業にもほしいというわけです。
ソフトウェアの品質にはいろいろな側面があります。 セキュリティ、安全性、信頼性、公平性などなど。システム検証研究センターでは現在、ソフトウェアの安全性や信頼性に関する基準認証の基盤研究をおこなっています。

システムの安全性に関しては、機能安全の考え方に基づく規格 IEC61508 が既に定められており、英国の UKAS やドイツの TUEV といった民間機関が、これに基づく認証活動を既に始めています。わが国のメーカがヨーロッパへの輸出をするにあたって認証が必要になる場合がでてきています。

また、型式承認などが要求される特定計量器に関しても、その制御ソフトウェアの不当な改竄を検出し、信頼性を保つように、ソフトウェアの認証を始めようという動きが欧州からはじまっております。昨 2004 年には欧州の計量法にあたる MID (Measurement Instruments Directive) が欧州議会を通過し、2006 年 10 月 30 日に発効しますが、これに計量器組込ソフトウェアの認証に関する条項がはいっています。こちらも、わが国のメーカといえども、輸出のためには認証が必要で、対岸の火事とはいっておられません。

ソフトウェアの認証活動は、究極的には、ソフトウェアがそれぞれの意味で「一定水準に達している」のを検証する、ということです。ここでは、システム検証技術は鍵となる技術です。例えば IEC61508 規格のソフトウェアに関する部分を見ると、システムに要求される安全性の度合いにしたがって四段階の SIL(Safety Integrity Level) を設定しているのですが、高い安全性を要求されるレベル（SIL3, SIL4）ではシステム検証の数理的技法を用いて安全性を検証することを求めています。

私どもシステム検証研究センターは、わが国の NMI（National Metrological Institute）である産総研計測標準研究部門と協力して、特定計量器制御ソフトウェアの認証に関する研究を進めてきましたが、今年度になって、IEC61508 に基づく認証活動のための調査研究および基盤研究を開始しました。ソフトウェアに関する認証活動の開始は、ただ便利なもの面白いものを追求するだけではすまなくなったことを意味しています。ソフトウェアの世界が成熟してきたことを象徴しているのではないでしょうか。

システム検証研究センター長　木下佳樹

＜ＣＶＳニュースレター　２号＞

産業技術総合研究所　システム検証研究センター http://unit.aist.go.jp/cvs/
●千里サイト：〒 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
●尼崎サイト：〒 661-0974　兵庫県尼崎市若王寺（なこうじ）3-11-46

●トピックス１

第二回 システム検証の科学技術シンポジウム開催報告

システム検証研究センターは科学技術振興機構と共催で第２回のシステム検証の科学技術シンポジウムを 2005 年 10 月 20 日および 20 日に大阪府豊中市の「千里ライフサイエンスセンター」にて開催しました。初日に 146 名、２日目に 112 名の皆様にご参加いただきました。

このシンポジウムは、情報処理システムのディペンダビリティ（信頼性・安全性・セキュリティ）、情報処理システム開発の生産性、数理的技法（モデル検査・定理証明）、数理的技法周辺の理論（算譜意味論・プログラミング理論・書き換え系）、情報処理システムのテスト、品質保証、開発方法論、検証手法の導入事例研究などをテーマとしています。このシンポジウムの特徴は基礎理論から実際のソフトウェア開発の現場まで幅広いシステム検証に関する第一線の研究発表が一堂に会することです。

今回シンポジウムへの参加者（初日 146 名、２日目 112 名）の内訳をみますと、産学の比率がほぼ１：１と、予想以上に多くの産業界の方々にご参加いただきました。前回にもまして、産学官の交流の場として貴重なものになったと思います。

今回のシンポジウムでは、３件の招待講演と１件のチュートリアル、基調講演、また一般講演は、２日間で 16 件、ポスターセッション９件となり、講演総数は 30 件となりました。
当初は、講演のみの開催とする予定でしたが、予想以上にお申し込を多数いただき、２日間で全てを発表していただくことが時間的に難しくなってしまったため、急遽ポスターセッション枠を設け、できるだけ多くの発表をしていただけるようプログラムを修正いたしました。かなりタイトなプログラムとなりましたが、大変充実した２日間となりました。

シンポジウム会場
千里ライフサイエンスセンターの５Ｆ
サイエンスホールで
開催されました。

会場：サイエンスホール

会場：ホール前受付

様々な視点から検証を俯瞰する
基調講演・招待講演・チュートリアル

◆基調講演

「システム検証の科学研究とフィールドワーク」

シンポジウムは、当研究センター長の木下佳樹による基調講演でスタートしました。本基調講演では、統合検証環境の構築を柱とした科学研究、および、技術移転と同時に社会への応用を観察することから、新しい科学を生み出すことを目的としたフィールドワークの紹介など、システム検証研究センターの活動を概観しました。

◆チュートリアル

「計算と論理をコンピュータ上に実現するための自然枠組」

チュートリアルでは、佐藤雅彦教授（京都大学）に「計算と論理をコンピュータ上に実現するための自然枠組」というタイトルで講演をしていただきました。講演の前半では、自然演繹の理論的背景の 100 年の歴史を約 30 年ごとに「論理の時代」「計算の時代」「計算と論理の融合の時代」の３つの時代に分割してお話していただいた上で、そこから未来の姿の展望を語っていただきました。後半では、佐藤教授が現在取組まれているシステムのデモを行っていただきました。

産業技術総合研究所　システム検証研究センター　http://unit.aist.go.jp/cvs/
●千里サイト：〒 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
●尼崎サイト：〒 661-0974　兵庫県尼崎市若王寺（なこうじ）3-11-46

◆招待講演 1「組込みシステム開発の課題と検証技術」

初日の最初の招待講演では、高田広章教授（名古屋大学）に「組込みシステム開発の課題と検証技術」というタイトルで講演していただきました。最初に組込みシステムの開発の現状と課題、そして、その特徴についてわかりやすく整理しながら、組込みシステムにおけるシステム検証の重要性を解説していただきました。後半では、その例として、リアルタイムスケジューリング理論に基づいたリアルタイム性検証技術の概要と、自動車制御システムとネットワークへの適用事例までお話くださいました。社会の中で遍在する組込みシステムにおけるシステム検証は今後ますます発展が求められる分野であることを改めて感じました。

基調講演：木下佳樹

チュートリアル：
佐藤雅彦教授

◆招待講演 2「システム検証とは？」

二日目は岸田孝一氏（SRA 先端技術研究所）による招待講演「システム検証とは？」でスタートしました。この講演では、「正しさ」とは何か、「検証」とはいかなる作業かについてお話ししていただきました。外国の哲学者や日本の江戸時代の哲学者の話も交え、広い視野からみた検証というものに対する様々な考えを紹介いただきました。検証の原点について改めて考えさせられた講演でした。

◆招待講演 3「論理的方法と代数的方法」

午後からの本シンポジウム最後の招待講演では、小野寛晰教授（北陸先端科学技術大学院大学）に「論理的方法と代数的方法」というタイトルで、論理学における代数的方法を歴史を振り返りながら、その概要をお話いただきました。ここで講演された内容は、当センターでも行われている意味論の研究と非常に関連が深いものであり、今後も小野先生、そして北陸先端科学技術大学院大学（JAIST）とも研究交流を積極的に行っていく予定です。

招待講演：高田広章教授

招待講演：小野寛晰教授

数理的技法
モデル検査がキーワードに
一般講演・ポスターセッション

◆数理的検証法の実用化へ

一般講演では、やはり、今話題のモデル検査をキーワードにした発表が多く、一般講演とポスターセッション全体の約３割強を占めました。モデル検査は数理的技法の一つですが、近年、理論的研究から実際の検証への応用がすすみつつあります。本シンポジウムでも、モデル検査の実用化のためのツール開発や事例報告（「状態遷移表のモデル検査」「鉄道信号システムの連動図表と連動装置のモデル検査」「モデル検査の実用化に向けた取り組みと事例報告」「モデル作成にもとづくレビュー手法の提案」）など、数理的技法の実用化への大きな動きが直接感

会場：　一般講演

会場：　総合司会

産業技術総合研究所　システム検証研究センター http://unit.aist.go.jp/cvs/
●千里サイト：〒 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
●尼崎サイト：〒 661-0974　兵庫県尼崎市若王寺（なこうじ）3-11-46

じられる講演が多数ありました。また、情報処理システムの不具合による世界的な社会問題の深刻度が増すなか、ソフトウエアの安全性の国際規格に関連した講演が２件（「ISO/IEC15408に基づく定理証明とモデル検査による情報セキュリティ使用の検証技法」「ソフトウェアの安全性／機能安全規格に基づくソフトウェアの設計と認証」）あり、システム検証と国際規格との関係という新しい流れを捉えることができました。

ポスターセッションでも、モデル検査をキーとした発表が多くあり、ここでも、実用面でのモデル検査への関心の高さが伺えました。

◆学術的研究成果も充実

学術的研究成果に関しては、リアクティブシステムの仕様検証法（「Muller オートマトンを用いたリアクティブシステムの仕様検証法とその完全性」「時間論理タブロー証明器のＭＰＩによる実装」「リアクティブシステムを対象とした様々な実行時検証概念の形式化とその判定アルゴリズムの完全性」）、セキュリティ関係（「A Static Analysis using Tree Automata for XML Access Control」「Formal Modeling and Verification of Workflows with Security Considerations」）や、項書き換え系（「モジュラーな代数仕様言語のための項書き換えシステム」「高階書換えシステムのモジュラ性」）、意味論（「Kleene category as a model of calculation」） といった分野で発表が行われました。

◆次回シンポジウムへの始動

今回のシンポジウムでは、参加者の数もさることながら、企業からも一般講演の申し込みが複数あったこと、また、関西に限

ポスターセッション会場風景１

ポスターセッション会場風景２

らず、遠方からも多くご参加いただいたことは、システム検証の科学技術に対する関心の高さを実感するものでした。当研究センターがこの分野の拠点になるように活動を進めて行きたいと思います。最後になりましたが、前回のシンポジウムに引き続き、機関誌「コンピュータソフトウェア誌」（岩波書店）に特集号を組み、希望する講演者の投稿を可能としていただき、単なる後援以上の支援をいただいた日本ソフトウェア科学会、また協賛いただいた情報処理学会、電子情報通信学会、関西ＩＴ共同体、日本数理科学協会（現:国際数理科学協会）の諸組織、招待講演、チュートリアルの講演者の皆様、また、一般講演やポスターセッションの講演者の皆様に厚くお礼申し上げます。

2005 年 10 月
第二回システム検証の科学技術シンポジウム事務局

シンポジウムの詳しいプログラムはシステム検証研究センター（ＣＶＳ）のＷＥＢサイトよりご覧いただけます。
また、シンポジウムでの講演内容を掲載した、予稿集を発行しております。ご希望の方は、下記までお申込ください。

ＷＥＢサイトには、ＣＶＳの活動内容、これからの講演会やワークショップの予定などを随時掲載しておりますので、是非お立ち寄りください。
CVS WEB サイト URL： http://unit.aist.go.jp/cvs/

予稿集のお問合せは：
メールにて、ご住所 / 所属 / お名前を明記の上
第二回システム検証の科学技術シンポジウム
事務局宛にお申込ください。
Email： verification2005@m.aist.go.jp

産業技術総合研究所　システム検証研究センター http://unit.aist.go.jp/cvs/
●千里サイト：〒 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
●尼崎サイト：〒 661-0974　兵庫県尼崎市若王寺（なこうじ）3-11-46

●トピックス 2

AIM3 開催報告

４月に開催した AIM2 に引き続き、AIM3 を共同開発先の Chalmers University of Technology（スウェーデン イェテボリ市）で開催しました。

創刊号でも紹介しましたが、CVS は、対話型証明支援系 Agda をスウェーデンの Chalmers 工科大学と共同開発しています。この研究協力の中心となるのが AIM(Agda Implementors Meeting) で、年二回のペースで双方の研究者が一堂に会し、互いの進捗の共有に加えて集中合宿的に研究活動を進めています。今回、第三回目となる AIM3 が 8 月 30、31 日の 2 日間、Chalmers 工科大学において行われ、双方から約十名ずつが参加しました。

主要テーマは次世代の支援系 Agda2 の方式策定でした。理論的な裏付けとなる型理論の「コア」言語を、純粋な計算体系の上の推論規則としてデザインし、また実用にむけた機能強化を計る「フル」言語について、そのモジュール化機構やパターンマッチングでの関数定義方式などを定めました。これらに基づく Agda2 実装作業は、現在 Chalmers と CVS の分担のもとに進行中です。
技術交流として、CVS 側からサブタイピング実装、プラグイン機構、Agda 言語コンパイラー、Chalmers 側からプログラム停止性検査の新方式、Haskell プログラムの検証法などについて報告がありました。ここでの重要な成果の一つは、現行 Agda の配布について合意が形成できたことです。

AIM3 の直前の二週間、Chalmers 工科大学ではプログラミングおよび数学での対話型証明構成に関する百名規模のサマースクールが、第一線でご活躍の研究者の方々を講師として開催されました。CVS からは 9 名がこれにもフル参加し、Agda 実習のインストラクター役などとして運営に協力しました。CVS には、開発する技法を Agda 上の統合検証環境としてまとめて提供する長期計画があります。計画が、多くの研究員の作業を要する段階に具体化されつつあるいま、スクールへの参加によって CVS 全体の技量が向上し、計画が実現へむけて大きく加速しています。

●お知らせ

10/14 プレスリリース

対話型検証研修コース（初級編）新設のお知らせ（新設記念 無料開催中）

CVS では、モデル検査研修コースに加えて対話型検証研修コース（初級編）を新設いたしました。第一回目は 11/28 ～ 12/1 に開催しました。

「対話型検証研修コース（初級編）」は定理証明に興味を持つ方々のための研修コースです。
本コースでは、定理証明支援系 Agda を使ってさまざまな定理とその証明を扱い、形式的に証明することがどういうことなのかを実感していただきます。
Agda は関数型プログラミング言語としても機能します。研修コースでは初めに、いくつかの関数やデータを定義し、プログラムを実行することで Agda で使われる言語とシステムの操作になれていただきます。
その後に定理証明を扱います。ある問題（ソート関数が正しく機能しているか？など）を Agda を用いて考える場合、一つの方法として (1) 問題を数理的に（述語論理などを用いて）定式化する (2) 定式化されたものを Agda が取り扱える形で記述する (3)Agda を操作して問題を解決する、と作業を分けることができます。
初級コースでは主に (2) と (3) にあたる部分を扱います。また、演習の時間を多くとり、実例と経験から Agda と定理証明を理解していただけるようにしています。

■目　標

1. Agda を使ってプログラム（関数）をかけるようになる。
2. Agda を使って定理や証明をかけるようになる。
3. 型理論の上で命題や証明がどう表現されているかを知る。

■前提条件

述語論理、型付きラムダ計算、関数型プログラミングを学んだことがあり、Emacs を使って文章作成ができる方を対象としています。

開催予定の確認と、参加お申込は HP から。
URL：http://unit.aist.go.jp/cvs/

産業技術総合研究所　システム検証研究センター http://unit.aist.go.jp/cvs/
●千里サイト：〒 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
●尼崎サイト：〒 661-0974　兵庫県尼崎市若王寺（なこうじ）3-11-46

●イベント・講演会

2005 年 9 月～ 11 月
イベント開催報告

◆計算機言語談話会（CLC） 毎週木曜日定期開催中

場所：システム検証研究センター千里サイト

日付　　講演者（所属）

09/08　池上大介、岡本圭史、高井利憲、古澤仁（CVS）
09/29　竹内泉（CVS）
10/06　西澤弘毅（CVS）
10/13　Till Plewe（筑波大学）
10/27　西澤弘毅（CVS）
11/04　Paul Pettersson（Uppsala Univ. Sweden）

直近のスケジュールはこちらから▼
CLC の URL：http://unit.aist.go.jp/cvs/CLC/

◆システム設計検証技術研究会 2 ヶ月毎に開催中（産総研コンソーシアム）

場所：システム検証研究センター千里サイト

第三回　9 月 7 日開催

講演者　関　浩之（奈良先端科学技術大学院大学）
演　題　「無限状態モデル検査ー概要と事例報告ー」

直近のスケジュールはこちらから▼
コンソーシアムの URL：http://unit.aist.go.jp/cvs/consortium/

◆ワークショップ 随時開催中

場所：北陸先端科学技術大学院大学

第一回 JAIST/TRUST-AIST/CVS Joint Workshop on Verification Technology(VERITE)9 月 21 日 22 日

講演者（所属）※講演順

《9 月 21 日》

1. Yoshiki Kinoshita (AIST)
2. Takuya Katayama (JAIST)
3. Kokichi Futatsugi (JAIST)
4. Weiqiang Kon, Kazuhiro Ogata, Kokichi Futatsugi (JAIST)
5. Kenro Yatake, Toshiaki Aoki, Takuya Katayama (JAIST)
6. Eun-Hye Choi (AIST)
7. Sathawornwichit Chaiwat, Takuya Katayama (JAIST)
8. Nguyen Truong Thang, Takuya Katayama(JAIST)
9. Hitoshi Ohsaki (AIST)
10. Kunihiko Hiraishi (JAIST)

《9 月 22 日》

1. Peter Dybjer(Chalmers Univ. of Technology)
2. Makoto Takeyama (AIST)
3. Takahiro Seino, Kokichi Futatsugi (JAIST)
4. Koichi Takahashi (AIST)
5. Toshinori Takai, Daisuke Ikegami (AIST)
6. Mizuhito Ogawa (JAIST), Eiichi Horita (NTT)
   Satoshi Ono (Kogakuin)

◆研修コース

11 月 4 日　特別講座：モデル検査研究コースお試し版
場所：梅田スカイタワーウェスト 23F
11 月 7 日～ 10 日　第 9 回モデル検査研修コース初級編（Spin）
場所：システム検証研究センター千里サイト
11 月 28 日～ 12 月 1 日　第 1 回対話型検査研修コース初級編
場所：システム検証研究センター千里サイト

直近のスケジュールはこちらから▼
研修コースの URL：
http//unit.aist.go.jp/cvs/training-course/training-course-top.html

出版

◆テクニカルレポート

8 月発行

PS-2005-013　Joe Hendrix, Hitoshi Ohsaki, and José Meseguer
" Sufficient Completeness Checking with Propositional Tree Automata"
PS-2005-014　高橋孝一、田辺良則、関澤俊弦
" 一次元セルオートマトンの有限近似解析 (Preliminary Version)"

9 月発行

PS-2005-015　関澤俊弦、田辺良則、高橋孝一
" 時相論理の充足可能性判定器のためのベンチマーク用論理式生成法 (Preliminary Version)"

10 月発行

PS-2005-017
" 第二回システム検証の科学技術シンポジウム予稿集 "

※全てのテクニカルレポートは HP からも入手可能です。
URL：http://unit.aist.go.jp/cvs/techrep.html

プレスリリース

10/03　第二回システム検証の科学技術シンポジウム
　　プログラム発表
10/14　対話型検証研究コース（初級編）新設のお知らせ

※リリースの詳細は、HP からご覧ください。
URL：http://unit.aist.go.jp/cvs/press_release.html

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
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
Email：informatics-inquiry@aist.go.jp