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
1
2005.08

数理的技法により安全で信頼できるシステムを！

◆ニュースレター創刊にあたって

産業技術総合研究所システム検証研究センター (AIST/CVS) は 2004 平成 16 年 4 月に設立された。一年余をへて、学術研究とフィールドワークを中心とする CVS の活動を様々な形で開始したのを機会にニュースレターを定期的に刊行することとした。

◆システムの開発技法と認証技法

ソフトウェアを含む情報処理システムの安全性、信頼性向上への要求は、いや増すばかりである。欧米では IEC61508 に基づく安全性認証や MID による法定計量ソフトウェア認証なども既にはじまっており、わが国の産業界、行政における関心も、たかくなってきた。欧米への機器輸出にあたって認証がもとめられるからである。

安全性、信頼性への要求が利用者の立場からだとすれば、開発者の立場からの情報処理システムに対する要求は、生産性にあるだろう。テストによる検証法では、実機がないと検証できず、したがって、不具合を見つけたときの手戻りもおおきい。バグの早期発見がもとめられる。

CVS の研究対象の中心は、情報処理システムの不具合をみつけ、システムの安全性や信頼性を主張するための数理的技法 (Formal Methods, 形式的技法) である。数理論理学や代数学を用いてソフトウェアのモデルを構築し、数学にもとづいた検証法をあたえようとするこの技法は、設計段階での検証を可能とするため、システムの開発技術として有効である。さらに、安全性やセキュリティ、信頼性、公平性などに関する認証をあたえるための基盤技術としてもかかせない。

◆職人芸か科学技術か

欧米では数理的技法の研究者の層もあつく、実用化されるにいたっている。しかし、わが国ではこれまで、数理的技法の研究、教育をおこなうまとまった場所がなく、必要な訓練を受けた研究者や技術者が十分にそだってこなかった。わが国の技術者の間では数理的技法は広くしられておらず、数学的訓練の不足による誤解もすくなくない。数理論理学にもとづく開発手法などというものは、何か特別のものであるかのようにみなされているのではないか。

実は数学をもちいることに特殊なところは、何もない。航空機、橋梁といったものが数学によらずに作られるときくと、誰もがおどろくのではないか。なのに、情報処理システム開発では、数学をつかわなくて当然とされている。職人芸に昇華していればまだよい。かぎられた経験だけが頼りの闇雲なプログラミングが、わが国ではまだまだ横行している。

システム検証研究センター
センター長　木下佳樹

しかし、開発されるシステムの規模がおおきくなり、その数がふえるにつれ、職人芸の限界があきらかになった。職人芸ではなく、数理的技法をはじめとする科学技術が、大規模情報処理システム開発の現状を打開する可能性をもつ唯一のアプローチといってよいであろう。

◆我々の研究観

我々は、職人芸ではなく、科学技術としてのシステム開発技術提供に貢献したい。科学的知識やディシプリンの科学の外における活用を研究することによって、職業としての研究がなりたつのだとかんがえる。しかし、それを場当たりで解決するだけでは満足しない。科学を技術に応用する過程を観察し、そこから新たな科学をつくりだしたい。

我々は科学のための科学の素晴しさをおおいに賛美する。では科学至上主義に安住するのか。否、科学の価値観だけにとじこもっていては、袋小路におちいるのではないかと危惧する。科学と外界との相互作用なしには、科学の健全な発展はありえないだろう。科学の活用を考えることが、科学自身にとってもよい効果をもたらすと信ずる。

このような考えに基づく CVS の事業が、わが国の情報学研究に積極的影響をあたえ、数理的技法が当然のように産業界でもちいられる日がくることをねがっている。

2005 年 8 月吉日
産業技術総合研究所システム検証研究センター
センター長　木下佳樹

＜創刊号　目次＞

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

●研究テーマ

システム検証研究センター(CVS)研究テーマ

システム検証研究センター（CVS）の目標は、システム検証の数理的科学技法が情報処理システム開発における生産性および信頼性の向上に有効であることを広く知らしめ、数理的技法を産業界の標準技術の一つとして普及させることです。

◆目標へのアプローチ

科学研究とフィールドワークのインタラクション

この目標を達成させるために、CVS は「**科学研究**」と「**フィールドワーク**」の二つのアプローチによって算譜科学に関する研究活動を展開しています。

■科学研究
　システム検証およびその周辺の現象に対する学術的興味に基づいて展開する研究活動をいいます。
■フィールドワーク
　企業などにおけるシステム開発の現状を踏まえつつ、算譜科学の研究成果を、開発現場における問題解決に役立てていく活動をいいます。

CVS の研究活動は、この二方向の活動を通じて行われ、学界と産業界の双方向のインタラクションで研究を深化させていきます。

◆研究体制

研究員が構成する CVS 研究ネットワーク「班」構造

CVS では、この研究目標を達成するために、さまざまな側面から研究すべきテーマを取り上げ、個別に研究が行われます。この研究テーマにそって、CVS 研究員は「班」を構成します。ユニークなのは、１人の研究者が１つの班に所属するのではなく、複数の班に所属し、それぞれの研究を行うということです。研究のネットワーク化ともいえるでしょう。研究員という人を媒介として、それぞれの研究テーマが相互に有機的に連携しています。CVS は、この体制から、研究者がより柔軟で幅広い視野をもって課題に取り組む土壌を醸成し、より良い研究成果につながることを期待しています。

また、それぞれの班は必要に応じていつでも新しくはじめることができ、また終わることも可能です。CVS では、このように組織の硬直化を徹底的に排除し、積極的に目標達成にむけて前進しています。

◆ 2005 年度の研究テーマ

2005 年度スタート時の研究テーマ

今年度は昨年度から継続分とあわせて 15 の研究テーマが設定されました。
必要に応じて新たなテーマが加わる可能性がありますので、随時、このニュースレターの紙面で報告してまいります。

科学研究

科学研究の具体的目的は、情報処理システムの規模の拡大にともない仕様やプログラムの記述の量が人間の能力を超えてしまうことで、見直しや検証が不完全になり不具合がでる問題を解決し、より正確で効率的な検証を可能にしていくことです。研究テーマを絞り込むキーワードを設定、細分化して研究を進めています。

キーワード：「**リアクティブシステム**」と「**抽象化**」
重点分野：「**対話型検証**」「**算譜意味論**」「**自動検証**」

＜**研究テーマ**＞
- 算譜意味論
  - 代数構造による抽象化・詳細化の意味論
  - 述語様相 μ 計算
  - π 計算の論理
  - 正則表現、正則 ω 表現の代数。Kleene 代数など。
- 自動検証
  - PML（Pointer Manipulation Language）の自動抽象化
  - ACTAS- 等式付木構造自動機械に基づく自動検証器
- 対話型検証
  - Agda - Martin-Löf 型理論に基づく対話型証明器
  - Mendori - 超変数を持つ対話型証明器
  - Agate - 依存型を持つ函数型作譜言語

フィールドワーク

CVS では外部の皆様との共同研究を積極的に行っております。フィールドワークでは、具体的成果をあげていくだけを研究テーマとするのではなく、得られた成果を広く一般にも応用するための手法の研究も重要なテーマの一つとしております。

1. 共同研究
- 業務 WEB システム動作検証　「模倣に基づく検証法」
- 組込みソフトウェアの検証　「環境ドライバ法」の考案
- 図書管理システム試験開発
  - Empirical Data の取得
  - 模倣に基づく検証法の試用
- 遠隔ソフトウェア更新システム信頼性

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

2. ノウハウ体系化プロジェクト
個別の共同研究で得たノウハウを抽象化することで、個々の企業のプライベートに触れることなく他の開発にも応用できるようにし、広く一般に提供することを目的としています。その一環として、フィールドワーク手法研究セミナーをセンター内で開催し、知識の共有を図っています。

3. 評価法の研究
評価の方法を研究することで、数理的技法の有効性を客観的に評価できるようにし、他の検証手法や開発手法との比較をより科学的に行う基礎作りをテーマとしています。

◆研究成果の形

色々な形で表される研究成果

CVS での研究成果は主には次の 4 つの形をとって、学術界や産業界に寄与していきます。

1. セミナー
計算機言語談話会（CLC）を中心に、システム設計検証技術研究会、AIST/CVS ワークショップ、シンポジウムなどさまざまなセミナー・講義などで研究成果を共有していきます。

2. 論文執筆
学術論文の執筆は、CVS におけるもっとも重要な研究活動であり、論文は学術界や産業界に広く提供しております。

3. 先端的ソフトウェアの開発
理論研究の成果を反映した先端的ソフトウェアの試作や開発を行います。

4. 研修コース
CVS での研究を進める中で蓄積していく技術や理論のノウハウを内部に留めてしまうのではなく、外部向けの研修コースとして提供しております。

数理的技法（Formal Methods）とは？
数理的技法とは、情報処理システムの開発手法を科学的根拠に基づいてあたえようとする試みの総称です。ソフトウェアおよびハードウェアシステムの開発や検証、仕様の作成など様々な開発工程で応用することが可能です。

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

AIM2 開催報告

昨年度からスタートした AIM（Agda Implementor's Meeting: Agda 開発者の会）の 2 回目となる AIM2 が 4 月 14 日から 20 日までの間、CVS 千里サイトで開催されました。

AIM は、CVS とスウェーデンのイェーテボリにある Chalmers University of Technology の研究者による、定理証明支援系 Agda システムの開発と保守をテーマにした集中合宿形式の定期研究集会です。通常、研究者は電話会議などを通じて研究を進めていますが、半年に 1 度のペースで AIM を開催し、集中して研究を行っています。1 回目の AIM1 は、昨年秋にスウェーデンで開催され、今回は日本の CVS 千里サイトで開催されました。Chalmers 工科大学から 8 名、CVS から 9 名の研究者が参加し、連日早朝から深夜にわたって共同研究がおこなわれました。

◆ Agda とは？

Agda とは、Martin-Löf 型理論に基づく「対話型証明支援系」です。これは問題の厳密な記述、正しいプログラムや証明の構成を、コンピュータとの対話を通して効率よく行うためにもちいるソフトウェアシステムです。プログラム開発用の構造エディターを「字面」だけでなく意味についても取り扱えるように高度化したものと考えることができます。

◆ AIM2 の内容

AIM2 では、次の 3 つの活動が行われました。

1. AIM1 以降の相互の活動報告
2. コードスプリント
3. 今後の活動計画

コードスプリントとは、3～4 名くらいのグループに分かれて集中して実際にコードを書く活動をいい、あまり他では見られない手法です。

・AIM2 参加者

今回のコードスプリントは 5 つのグループに分かれて行われました。

① TYPES サマースクール（Chalmers 主催）のチュートリアルテキスト
② 次世代 Agda に向けた Prototype のコーディング
③ 現在の Agda 改良プログラミング
④ Agda による代数構造 KAT とそれを用いたプログラム意味論の形式化
⑤ Agda の新機能をテストするための圏論の形式化

◆交流

その 1・・・研究交流イベント（ワークショップ）

多くの研究者が一同に会するこの機会を利用して、AIST/CVS ワークショップを開催しました。ここでは、AIM 参加者だけでなく、他の研究者も参加。AIM の枠を超えた研究発表が行われました。

・ワークショップ風景

その 2・・・文化交流

AIM2 開催期間中、相互の研究者はほぼ寝食をともにしたといってもいいくらいの密度の高い研究活動を行っておりましたが、週末のつかの間、桜で有名な奈良県吉野郡や京都の嵐山などに出かけ、日本の春を満喫しました。

・桜の木の下で

・京都嵐山にて

◆今後の予定

次回、AIM3 は 8 月にスウェーデンの Chalmers University of Technology 主催でひらかれる TYPES サマースクールに引き続いて開催されます。

※ TYPES サマースクールは、EU で行われている The TYPES project の活動の一環です。このプロジェクトの目的は型理論に基づくコンピュータプログラミングと形式推論の技術開発を研究することです。

産業技術総合研究所　システム検証研究センター　http://unit.asit.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

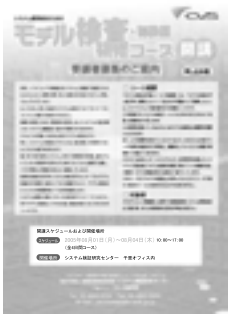
●お知らせ 1

好評！無料開催中 モデル検査研修コース初級編

モデル検査研修コース（初級編）は「モデル検査を手っ取り早く理解したい！」「自分の手を動かして理解したい」というソフトウェア技術者向けの研修コースです。2004 年度より開始しましたが、大変好評をいただいております。

現在のソフトウェアや情報処理システムは、複雑で規模の大きなものとなり、開発の際に高い信頼性を保証することが難しくなっています。というのも、多くの場合システムは限られたテストケースについてしか動作を確認できないからです。障害の原因となる「開発者の意図しないシステムの振る舞い」はシステム稼動後に漸く発見されるのです。このため、まだ記憶に新しいシステムに絡む様々な不具合は、実際に使ってみて初めてその姿を現すのです。これでは遅すぎます。モデル検査とは、この「意図しないシステムの振る舞い」を発見することに大きな威力を持つ手法なのです。
CVS では、このモデル検査を実際にさまざまな事例に適用し、

●紹介ホームページ


●開講ちらし

そこで蓄積したノウハウを応用してこの研修コースを開発し、システム開発に実際に携わっておられる技術者やマネージャの方々に提供しております。開発側の方々だけでなく、企業においてシステムを導入される側の技術者や開発者、設計者の皆様、また、それらを目指す学生の皆様など、幅広い層の方々にご受講いただきたいコースです。
本コースは、全 4 日間の集中コースですが、現在、無料で開講しております。この機会に是非お申込ください。

開講スケジュール詳細 URL：http://www.unit.aist.go.jp/cvs/

●お知らせ 2

第二回 システム検証の科学技術 シンポジウム開催 （参加費無料）

昨年 2 月に第一回目を開催。初回にもかかわらず、延べ 200 名の皆様にご参加いただきました。第二回目は、10 月 20 日～ 21 日の 2 日間の予定で、大阪府豊中市の「千里ライフサイエンスセンタービル」にて開催いたします。多数の皆様のご参加をお待ちしております。

主　催：科学技術振興機構
　　産業技術総合研究所 システム検証研究センター
協　賛：日本ソフトウェア科学会、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
会　場：千里ライフサイエンスセンタービル（大阪府豊中市）

最新の情報は下記 URL をご覧ください。
シンポジウムの詳細 URL：
http://unit.aist.go.jp/cvs/symposium/verification2005/

テーマ：
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「Formal Methods」（モデル検査 / 定理証明）
数理的技法周辺の理論（算譜意味論 / プログラミング論理 / 書換系）
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

参加ご希望の方は、事務局宛にメールでお申込ください。
シンポジウム事務局 Email：verification2005@m.aist.go.jp

プログラム概要：
基調講演：木下佳樹（CVS）
招待講演：
小野寛晰（北陸先端科学技術大学院大学）
高田広章（名古屋大学）
岸田孝一（株式会社 SRA 先端技術研究所）

←シンポジウム案内ちらし

産業技術総合研究所　システム検証研究センター http://unit.asit.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 4 月～ 8 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）

4/7　池上大介（CVS）
5/11　Ralph-Johan Back（Abo Akademi Univ. & TUCS）
5/12　戸沢晶彦 (日本 IBM 東京基礎研究所）
5/19　竹内泉、尾崎弘幸（CVS）
5/24　Bernard Dion（Esterel Technologies）
6/2　竹内泉（CVS）
6/3　Don Sannella（Univ. of Edinburgh）
6/16　高橋孝一（CVS）
6/23　石濱直樹、片平真史（宇宙航空研究開発機構　JAXA）
6/30　Nicolas Marti（Univ. of Tokyo)
7/4　Pawel T. Wojciechowski
（School of Computer and Communication Sciences,
Ecole Polytechnique Fe'de'rale de Lausanne（EPFL））
7/7　佐藤憲太郎（ミシガン大学）

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

第一回　4 月 25 日開催

講演者　青木利晃（北陸先端科学技術大学院大学）
演　題「定理証明システムとソフトウェアの検証への応用」

第二回　7 月 25 日開催

講演者　小西晃輔（株式会社シーディー・アダプコ・ジャパン）
演　題「形式手法・形式検証を適用したセーフティークリティカルな組込み制御アプリケーションの開発事例紹介」

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/

◆ AIST/CVS ワークショップ 随時開催中

場所：システム検証研究センター千里サイト

第三回 AIST/CVS ワークショップ 4 月 18 日開催
"Workshop on Automatic and Interactive verification"

講演者（所属）※講演順

1. José Meseguer (Univ. of Illinois)
2. Peter Dybjer (Chalmers Univ. of Technology)
3. Thierry Coquand (Chalmers Univ. of Technology)
4. 大崎人士 (CVS)
5. 田辺良則 (CVS)
6. 木下佳樹 (CVS)
7. Bengt Nordström (Chalmers Univ.of Technology)

随時開催いたします。直近のスケジュールはこちらから▼
ワークショップ URL：
http://unit.aist.go.jp/cvs/workshop/Workshop-top.html

◆研修コース

場所：システム検証研究センター千里サイト

5 月 16 日～ 19 日　第 6 回モデル検査研修コース初級編（NuSMV）
7 月 4 日～ 7 日　第 7 回モデル検査研修コース初級編（NuSMV）
8 月 1 日～ 4 日　第 8 回モデル検査研修コース初級編（NuSMV）

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

研究発表

◆テクニカルレポート

4 月発行

PS-2005-009　高木理、渡邊宏、武山誠
"PVS の紹介 "

6 月発行

PS-2005-010　竹内泉
"Kleene Category as a Model of Calculation (Preliminary Version)"
PS-2005-011　田辺良則、高橋孝一他
"A decision Procedure for Alternation-free Two-way Modal mu-Calculus"
PS-2005-012　西澤弘毅、武山誠
"Algebraic Structure for a Fixed Point Logic and Abstract Interpretation"

※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.asit.go.jp/cvs/techrep.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