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
11
2009.03

ディペンダビリティ

英国のディペンダビリティ研究サイトを幾つか訪ねた。英国のサイトに集中して訪問したのには理由がある。システムのディペンダビリティについての議論は二十年以上前からなされているが、情報技術の分野で昨今のように頻繁に用いられ始めたのは、英国のDIRC (The Dependability Interdisciplinary Research Collaboration) プロジェクトに始まるように思われるからだ。これは五大学 (Newcastle, Edinburgh, Lancaster, York, City University London) で計算機科学を中心に心理学や社会学からの参加も得て学際的に進められた。

ともあれ今回は、このDIRC参加サイトを中心に訪問した。NewcastleとYorkをたずねて心強かったのは、我々がfieldworkと名づけて行っているのと同様の活動を形式手法(数理的技法)に関して行っていたことである。これは企業の開発過程を変えて新技術を導入していくという仕事である。研究なのかコンサルテーションなのか境目がよくわからず、研究論文にはなりにくい仕事なので、日本国内ではあまり盛んではないが、NewcastleやYorkでは、我々と同様のスタンスに立って共通する技法を独立に開発している場合もあり、大変興味深かった。

City University London の Centre for Software Reliabilityでは、システムのディペンダビリティ評価技術の重要性を再認識した。我々は評価結果に客観性を持たせるためにも、まず規格策定からはじめようとしていた。しかし評価技術は当初の予想よりもはるかに複雑な様相を呈しており、むしろ評価技術確立が先であって、標準はその後にできるべきものかもしれない。

BathのPraxis社ではTokeneerプロジェクトで形式手法のベストプラクティスを提供した成果を紹介してもらった。彼らはCbyC (Correctness by Construction) と称してHoare論理に基づく検証を行いながらコーディングを進める手法を確立している。実用化寸前にきている形式手法の様子を如実に示す一例であろう。

2009年３月
システム検証研究センター
研究センター長　木下 佳樹

＜ＣＶＳニュースレター 11 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
●関西センター：〒 563-8577　大阪府池田市緑丘 1-8-31

●トピックス 1

産総研オープンラボ 開催

2008 年 10 月 21、22 日、産業技術総合研究所のつくばセンターで「産総研オープンラボ」が開催されました。産総研オープンラボは、産総研がこれまで行ってきた研究の成果や研究リソースを、企業の経営層、研究者・技術者、大学・公的研究機関の方々へ広くご覧いただくために、今回初めて実施されました。特に、本拠地のつくば地区の研究室等 250 箇所を公開、各地域センター展示、全体および、ライフサイエンス、情報通信・エレクトロニクス、ナノテクノロジー・材料・製造、環境・エネルギー、地質、標準・計測の産総研の六研究各分野の技術講演会がありました。

情報通信・エレクトロニクス分野主催の技術講演会「ディペンダブルな情報システムを目指して」では、ディペンダビリティに関連する五つの講演がありました。このうち CVS 研究センター長木下の講演では、情報処理システムの不具合事故の事例、それらを報じる新聞記事に見られた的外れな批判事例、今後の見通しなどを紹介しました。

各方面から非常に注目を集め、両日あわせて、延べ 3500 人を超える多数の方々に来場いただき、大盛況のうちに終了しました。

我々 CVS は、つくば本部情報棟 1 階に設けられた地域センター展示室へパネルを五枚展示しました。「システムの不具合防止とバグ検知 形式手法で安心安全」をテーマに、連携検証施設、システム検証研究センターの研究活動の取組みなどを紹介しました。会場では、関西産学官連携コーディネータ 奥野、組込みシステム技術連携研究体 尾崎、システム検証研究センター 渡邊の 3 名が説明を担当しました。

各パネルのタイトルと内容は次の通りです。

1. システムの不具合防止とバグ検知　形式手法で安心安全
   システム検証研究センターの活動紹介
2. ソフトウェア信頼性技術の研究開発・人材養成の産学官 連携活動を強化 ～ソフトウェア信頼性技術の中核施設～
   整備中の連携検証施設と組込みシステム技術連携研究体の活動紹介
3. 事例 8 アセンブラで記述された組込みシステムのモデル検査による検証事例
   「システム検証の事例報告集」掲載事例のダイジェスト
4. Agda
   Agda 言語と Agda システムの紹介
5. 統合検証環境
   統合検証環境の概略と Schorr-Waite マーキングアルゴリズムのハイブリッド検証の事例

期間中およそ５０人の方に我々の展示へ立ち寄っていただきました。普段出展する組込みシステムの展示会などと異なり、バイオ系、マテリアル系など情報系以外を専門とする方々とも交流できました。携帯電話など組込みシステムは我々の身の回りに遍在しますが、「組込みシステム」という言葉ですらまだ一般的に認知されているわけではないようです。

展示説明では、連携検証施設ならびに組込み適塾の紹介など注目を集めました。ロボット系分野の方からいろいろと質問いただいた印象があります。形式技法やモデル検査は「どこで教えてもらえるのか？」という質問もあり、これについては組込み適塾、研修コース、初級コーステキストなどを紹介できました。わずかながら、数理的技法の普及につながるものと確信しています。

オープンラボというとおり、やはり今回の目玉は研究室公開でした。つくばに研究室を持たない我々はスペースの限られたパネル展示だけしかできず、研究室公開ができなかったことがとても残念でした。また、オープンラボの現場を訪れ、パネルだけの展示は少し地味すぎたと反省しました。セラピー効果のあるアザラシ型ロボ「パロ」展示の人気に勝てるような素敵なデモの開発は今後の課題です。

ご来場いただいた方、お立ち寄りいただいた方、どうもありがとうございました。

当日の様子などは下記 [1,2] に報告されています。

[1]. 産総研オープンラボ－盛況のうちに終了－ . 産総研 Today, 2008, 8 (12), P34. http://www.aist.go.jp/aist_j/aistinfo/aist_today/vol08_12/network/p32.html#g
[2]. 産総研オープンラボへのご参加御礼 . http://www.aist.go.jp/aist_j/openlab/2008/au1024.html

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
●関西センター：〒 563-8577　大阪府池田市緑丘 1-8-31

●トピックス 2

国際シンポジウム AIM9 開催

国際シンポジウム Agda Intensive Meeting 9 (AIM9) を昨年 11 月 27 日から一週間、仙台市で開催しました。ニュースレター第 10 号でもお伝えした国際研究集会シリーズ Agda Impelentors' Meeting (AIM) の第九回目にあたります。

Agda は CVS がスウェーデンの Chalmers 工科大と共同で開発している対話型証明支援系で、人間が出す指示と計算機の応答の対話で正しいプログラムと証明を構成していくソフトウェアシステムです（ニュースレター第 7 号）。

CVS はこの対話型支援の柔軟さと自動証明ツールの馬力を統合する「統合検証環境」の考えを提唱し、Agda を拡張した統合検証環境 Agda-IVE の研究開発を実施しました。これは JST CREST プロジェクトの研究課題「検証における記述量爆発問題の構造変換による解決」（2002 年～ 2008 年）の一部として行われ、以降 CVS の中核的基盤技術として CVS 企業共同研究等に応用されています。

今回の AIM9 は、この成果を発信する目的をもって JST 国際強化支援策のシンポジウム支援をうけ、これまでより多くの海外研究者の参加を得ました。（参加者内訳：外国研究者 8 名・国内研究者 15 名）これに併せて、集中合宿的 AIM の特徴「コードスプリント」（ミニプロジェクト作業）もますます活発に行われた結果、AIM9 は Agda コミュニティーの拡充と国際連携強化の点で大変有益な活動となりました。

セミナー部分では、上記 CREST 成果に関する発表 3 件に加え、プログラム導出、"codata" 型関連技術、基礎理論、対話システムモデル、など幅広い話題が提供され、統合検証環境と Agda の現在と将来について、開発者と利用者の間で共通の理解が深まりました。

コードスプリントでは、ドキュメンテーション拡充、Agda コンパイラを用いた統合検証の新方式、実装の最適化、仕様記述事例、一階様相 μ 論理形式化、サイズつき型、依存型／ codata 型プログラミング実験、他支援系ユーザによる Agda 評価、など多彩なプロジェクトが実施されました。

それぞれの具体的成果に加えて、様々な立場・スキルの研究者達が緊密な共同作業を通じて交流を深めた効果も大きなものでした。

最終日の総括では、統合検証と Agda の将来が話し合われました。位置づけ・他システムからの差別化について、システムに関する検証支援だけでなく、システム自体を correct by construction で実現するプログラミング環境として優れている、という Agda の利点をより強化していく方針が確認されました（依存型プログラミングの新しいスタイル等）。

今回 AIM9 のコードスプリントではじめて Agda を体得した他支援系の専門家からは、Agda の利点を高く評価する意見がありました。また体制について、メジャーバージョンアップ、正式な研究協力覚書交換他が話し合われました。

次回 AIM10 は 9 月に一週間、スウェーデンで開催される予定です。ご興味をお持ちの方は CVS までご連絡ください。

シャルマース工科大と招聘講演者の講義中の様子

ミニプロジェクト作業中の様子

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
●関西センター：〒 563-8577　大阪府池田市緑丘 1-8-31

● CVS ニュース 1

第五回システム検証の科学技術シンポジウム 開催

2008 年 11 月 17 日から 19 日まで、筑波大学にて、第五回システム検証の科学技術シンポジウムが開催されました。本シンポジウムは、第三回まではシステム検証研究センターが主催していたものです。前回からは、ソフトウェア科学会ディペンダブルシステム研究会の主催となり、システム検証研究センターは共催いたしました。今回は、77 名の方に参加していただき、システム検証および関連する以下のようなテーマで 3 日間にわたり発表および質疑応答しました。参加者の内訳は、24 名が産業界から、28 名が大学関係者、25 名が大学以外の公共機関からとなっており、産業界と学界の交流の場を提供できたのではないかと考えております。

■ 11 月 17 日 (月) ■

初日の招待講演は、ソニーコンピュータサイエンス研究所の 真理雄様に「オープンシステムとディペンダビリティ」というタイトルで講演して頂き、新しい研究の方向性を含む非常に画期的な内容でした。

最後はポスターセッションで、参加者はそれぞれのポスターの説明を熱心に聞き入っていました。この日は、ポスターセッションの会場をそのまま利用して懇親会を行い、ポスターの話題やその他の話題で大いに盛り上がりました。

■ 11 月 18 日 (火) ■

二日目の最初の招待講演は、ダイキン工業の二宮 清様の講演で、「システムモデリングによるソリューションの創出」でした。近年の高度化した空調システムの紹介からはじまり、システムの運用時のディペンダビリティを確保する実社会での最新事例をお話しいただき、大変参考になりました。

午後の招待講演では、楽天株式会社の千田孝由起様から、「楽天のＷｅｂサービスを支えるインフラ技術と信頼性向上のためのしかけ ～止まらないサービスを目指して ～」というタイトルでお話していただきました。巨大な Web サービスを内側から見せていただき、大変興味深く聞くことができました。

■ 11 月 19 日 (水) ■

最終日の招待講演は、筑波大学大学院の加藤 和彦先生の講演「仮想計算機技術の動向」でした。1 時間という講演時間が短く感じるほど、内容の濃いお話しでした。

また、初日と 2 日目にそれぞれ一件ずつ、函館ワークショップ特別講演として日産自動車の渡邉 晃様と国立情報学研究所の中島 震先生に講演して頂きました。函館で開催された 2008 年度のディペンダブルシステムワークショップの発表から興味深いものを再発表していただいたものです。

今回のシンポジウムでは、ソフトウェア開発時における検証技術に関する発表だけでなく、ソフトウェアライフサイクル全般にわたってソフトウェアのディペンダビリティ向上を目指す研究や発表が多くなったと感じました。今後のこの分野の研究の方向性を示していると思います。

有意義なシンポジウムを滞りなく開催することができましたことに対し、関係者および参加者の方々に深く感謝いたします。

予稿集をご希望の方は下記 URL より入手できます。
http://unit.aist.go.jp/cvs/symposium/sympo-top.html

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
●関西センター：〒 563-8577　大阪府池田市緑丘 1-8-31

● CVS ニュース 2

ET2008 出展

産業技術総合研究所システム検証研究センター（以下 CVS） は Embedded Technology 2008 ／ 組 込 み総合技術展（主催：社団法人 組込みシステム技術協会（JASA)、会場：パシフィコ横浜、日程：2008 年 11 月 19 日（水）～ 21 日（金)、略称：ET2008）に出展しました。Embedded Technology は旧名称 MST として開始してから今年で 22 回目を数え、今回の ET2008 では来場者が 3 日間で延べ 26000 人に上りました。その会場で CVS は 2m × 2m のブースを設け、次の 5 枚のパネルを展示・解説を行いました。

◆システム検証研究センター概要
◆連携検証施設概要
◆定理証明支援系 Agda
◆ Agda を中心とする統合検証環境
◆フィールドワーク事例

CVS のブースの来訪者の多くは数理的技法を既に承知されており、導入方法や適用方法、また最新の事例などについて多くの質問がありました。その中で、導入や適用の方法に関して「モデル検査器 SPIN を勉強したが、実務ではまだ使えない」「定理証明支援器 Coq を使ってみたが、証明の書き方が分からなかった」などの声が寄せられました。

モデル検査については比較的広く知られてきており、SPIN などのモデル検査器を独学しているという声はこれまでもいろいろな場所で数多く寄せられていましたが、今回の展示では、モデル検査よりも比較的難しいとされる定理証明についても独学で使用を試みたという声もありました。

定理証明の普及はまだこれから先のことであろうと考えていた我々は、少々の驚きとともに、モデル検査や定理証明を含む数理的技法がネットワーク機器産業、自動車産業、電機産業の大手を中心に着実に認められつつあることを実感しました。

一方、数理的技法の開発現場への本格的な導入について、既に実施されているという声は聞かれませんでした。来訪者の多くは現場の技術者の方々であり、経営者や管理職の方はそれほど多くないという状況でしたが、来訪者からは、数理的技法を開発現場に導入するために、経営者や上司を説得する材料がほしいという要望もありました。つまり、その方自身は数理的技法の導入を試みたいと考える一方で、経営者や管理職はそれをなかなか採用しないという状況があると思われます。

数理的技法の導入について、開発現場の技術者はその必要性も感じながらも、経営側はそれに伴うリスクやコストを許容できないと判断している現実があるということを窺い知ることができました。

CVS は過去に Embedded Technology の関西版である Embedded Technology West/ 組込み総合技術展　関西（主催：社団法人 組込みシステム技術協会 (JASA)、略称：ET West）に 2 回出展し、それを踏まえて全国版である Embedded Technology に出展いたしました。

これまでの出展内容は、すでに述べた CVS が行ってきた数理的技法の研究やその数理的技法の適用事例研究などであり、今回の ET2008 では研究のより詳しい解説や適用事例集の配布などを行いました。

今後、さらに開発中の検証ツール Agda 体験コーナーなど、数理的技法の効果を実感できる展示を行い、数理的技法の普及に貢献していきたいと考えています。

ET2008 に出展の様子

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
●関西センター：〒 563-8577　大阪府池田市緑丘 1-8-31

●イベント・講演会・出版

2008年7月～2009年3月

イベント開催報告

◆計算機言語談話会(CLC)　毎週木曜日開催

7/23　大崎 人士（産総研 システム検証研究センター）
8/28　吉田 聡（産総研 システム検証研究センター）
10/9　高橋 孝一（産総研 システム検証研究センター）
10/30 高橋 和子（関西学院大学 理工学部）
11/12 Gyesik Lee（産総研 情報セキュリティ研究センター）
12/11 横山 哲郎（名古屋大学大学院 情報科学研究科 附属組込み SRC）
12/18 Anthony John Power（University of Bath）
1/29　Jean-Pierre Jouannaud (INRIA-LIAMA &Tsinghua University)
3/4　上田 和紀（早稲田大学 理工学術院情報理工学科）

〔開催場所：産業技術総合研究所 システム検証研究センター
千里オフィス6F会議室〕

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（産総研コンソーシアム）

第２回講演会　2008年9月18日開催
演　題：「最近の検証ツールおよびその実装の動向」
講演者：小川 瑞史氏 北陸先端科学技術大学院大学情報科学研究科教授
第３回講演会　2008年10月23日開催
演　題：「国内外におけるフォーマルメソッドの産業応用動向」
講演者：粂野 文洋氏 株式会社三菱総合研究所情報技術研究センター主任研究員・国立情報学研究所特任准教授
第４回講演会　2008年12月05日開催
演　題：「モデル検査支援ツールとその導入事例の紹介」
講演者：小池 隆氏　富士ソフト株式会社 技術本部研究開発センター生産技術研究室室長
第５回講演会　2008年12月19日開催
演　題：「VDMによる実システム開発」
講演者：佐原 伸氏 株式会社CSKシステムズ理事製造グループ VDM推進課
第６回講演会　2009年01月29日開催
演　題：「フォールトプローンなソフトウェアモジュールのスパムフィルタを利用した検出手法」
講演者：水野 修氏 大阪大学大学院情報科学研究科
第７回講演会　2009年02月06日開催
演　題：「Bメソッドの概要と開発現場への技術導入」
講演者：堀 武司氏 北海道立工業試験場 情報システム部情報通信科

〔開催場所：産業技術総合研究所システム検証研究センター
千里オフィス 6F会議室〕

会員募集中　詳細はこちらからどうぞ▼

システム設計検証技術研究会のURL：
http://unit.aist.go.jp/cvs/con-top.html

出版

◆テクニカルレポート

8 月発行

PS-2008-011,　Hiroki Takamura, Powers of positive elements in constructive C *-algebras

PS-2008-012, 青木利晃 , 粂野文洋 , 木下佳樹 , 篠崎孝一 , 高木理 , 高村博紀 , 田口研治 , 中原早生 , 西原秀明 , 早水公二 , 本位田真一 , 渡邊宏 , モデル検査の教育プログラム構築に向けて

PS-2008-013, Hideaki Nishihara, Koichi Shinozaki, Koji Hayamizu, Toshiaki Aoki, Kenji Taguchi, Fumihiro Kumeno, Model checking education for software engineers in Japan (Preliminary Version)

9 月発行

PS-2008-014, 木下佳樹 , Agda 言語について

11 月発行

PS-2008-015, システム検証研究センター , モデル検査研修コース中級編

12 月発行

PS-2008-016,　システム検証研究センター, 第6回ディペンダブルシステムワークショップ(DSW2008)論文集

PS-2008-017, Satoru Yoshida, Sequential continuity and boundedness of generalized functions in constructive mathematics (Preliminary Version)

2 月発行

PS-2009-001, システム検証研究センター , 第五回システム検証の科学技術シンポジウム (SSV2008) 講演論文集

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

禁無断転載
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