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
6
2007.02

モデル検査の利用

数理的技法とは無縁のシステム開発現場が、まだまだあちこちにある一方で、CVS のまわりでは、モデル検査の知識が確実にいきわたりつつあるようだ。数理的技法には、モデル検査以外にもいろいろな手法があるとはいえ、数理的技法普及をミッションとする我々にとっては、一歩前進といえる状況がえられつつあるようにおもわれる。今回は、モデル検査がシステム検証にどのように利用されるかを概観し、次の一歩をどのように進めるべきかを考えてみたい。モデル検査をしることの次は、それを使うことだろうというのである。

モデル検査利用の概観　モデル検査を情報処理システムの検証に用いる場合、まず、システムの動作仕様を手にいれて（実はこれがなかなかの難題だが、それはさておく）、それをあらわす遷移系を定式化し、さらにモデル検査器が定めた Promela などの記述言語によってかきおろす。並行して、そのシステムに求めたい性質、つまり検証項目を CTL あるいは LTL などの特別な論理式でかく。
遷移系と検証項目をかいたら、それらをモデル検査器に入力してモデル検査する。その結果には次の三通りがある：（1）遷移系が検証項目をみたす；（2）みたさない（どんな実行系列の場合にみたさないかの反例がつく）；（3）モデル検査の異常終了（記憶領域があふれたり、いつまでたっても答をかえさないなど）。

検証項目をみたす場合　この場合でも、システムが検証項目をみたしているとはいえない。遷移系がシステムを正しく反映しているとはかぎらないからである。この場合、理屈では、「これだけの検証作業をしたが不具合はみつからなかった」ということがいえるだけである。

検証項目をみたさない場合　この場合でも、前項と同じ理由で、システムに不具合があるとはかぎらない。そこで、反例を解析して検証担当者とシステムの設計者がともに検討し、その反例がシステムの不具合を示しているのかどうかを設計者が判定する。誤解のために遷移系がシステムをうまく反映していない場合もあるし、仕様上はたしかにおこりえるけれども、周囲の条件から、滅多におこらないといえるので、問題にしなくてもよい、という場合もある。いずれにしても反例が不具合をしめしていない場合には、状況は前項と同じであり、あまりはっきりしたことはいえない。いっぽう、反例が不具合をしめしている場合には、設計者が不具合を修正し、その修正を遷移系に反映させて、モデル検査をはじめからやりなおす。

異常終了する場合　この場合、異常終了の原因は必要な記憶領域あるいは計算時間がおおすぎることだから、遷移系のつくりをもっと小さなものに変更してモデル検査をやりなおす。いうまでもなく、ただ小さくしさえすればいいというわけではなく、「検証項目を確かめる」という観点からはシステムの本質をかえずに、小さくするのである。遷移系を改良してモデル検査をやり直すという点では、（2）で反例が不具合をしめすと判定した場合と同じである。

以上でモデル検査器の利用を概観したが、ここには少なくとも二つの課題があるとおもわれる。

課題 1：正しく反映しているか？　一つめの課題は検証対象システムを遷移系が正しく反映していることをどのようにしてたしかめるのか、という問題である。上にしるしたように、遷移系がシステムをうまく反映していることをしめさないと、不

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

具合のあることはしめせても、システムが不具合なくうごくことを保証することはできない。モデル検査の検証対象はシステム自身ではなく、あくまでも遷移系だからである。

課題 2：利用サイクルの支援　もう一つの課題は、遷移系を改良してはモデル検査する、というモデル検査利用サイクルの支援である。このようなサイクルは検証項目がみたされず、しかも、反例が不具合をしめすと判定した場合や異常終了の場合にあらわれる。モデル検査器は遷移系を検査するものであって、遷移系の改良を支援するものではないから、改良の支援は他の方法によらなければならない。例えば遷移系の記述言語の入力・更新を支援するツールや、モデル検査が出す反例を解析するツールがのぞまれる。

我々 CVS の周辺でも、この方向の研究開発がおこなわれている。CVS では、これらの問題を個別に解決するだけではなく、対話型定理証明支援系の上の統合検証環境をもちいて系統的に行おうとしている。これについては、別の機会に詳しくしるしたい。

システム検証研究センター
センター長　木下　佳樹

●活動紹介

計算機言語談話会（CLC）
（Computer Language Colloquium）

CVS/AIST では、毎週木曜日、国内外の研究者をお招きして講演会を開催しています。もちろん当研究センターの研究者も講演者として登場しています。今回は、具体的にどのような活動を行なっているかをご紹介いたします。

■ CVS/AIST の共通知識基盤

CLC は、前身の電子技術総合研究所時代を経て、研究ラボから研究センターに発展し今日にいたるまで、継続して行なわれている研究セミナーであり、CVS/AIST の研究活動の中心的な役割を持っています。また同時に、様々な背景を持つ CVS/AIST の研究メンバー全体に共通する知識を形成していくための場であります。CLC は、もう一つの CVS/AIST の活動である「システム設計検証技術研究会」とは若干趣を異にし、より学術分野に重きをおいた講演内容となっております。

■国際会議レベルの講演も聞ける CLC

例えば、2006 年 10 月 11 日に開催いたしました第 173 回計算機言語談話会では、モデル検査の教科書「Model Checking」の著者として知られる、カーネギーメロン大学の Edmund Clarke 教授をお招きし、「Model Checking: From Hardware to Software and Back Again」と題してモデル検査の最新研究について講演していただきました。モデル検査は、最初はハードウェアの検証技法として成功しました。その後、ソフトウェアの検証への応用を目指し、多くの研究者が述語抽象化などのさまざまな応用研究を行いました。その結果、モデル検査はソフトウェアの検証技法としても有効性が認められてきました。しかし最近では、その応用研究の成果がハードウェア検証の研究にフィードバックされることにより、モデル検査はハードウェアのより高度な検証技法としても発展しつつあるとのことです。このような最新の研究状況を知ることができる計算機言語談話会は、ある意味で国際会議以上に貴重な存在といえます。

■リラックスした雰囲気の中での自由な議論

この活動は、研究センター内だけにとどめるのではなく、外部にも公開しており、ここで取り上げる研究に興味をお持ちの方々でしたらどなたでも無料で、そして気軽に参加いただけます。CLC は CVS/AIST の千里サイト（大阪府豊中市）の会議室で開催されています。リラックスした雰囲気のなか自由な議論が交わされ、様々な人や研究が邂逅し、新たな研究が自然発生的に生まれる場となっています。

CLC のスケジュールおよび参加申込はこちらから：
http://unit.aist.go.jp/cvs/CLC/

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

●会員募集

産総研コンソーシアム

システム設計検証技術研究会 平成１９年度会員募集

システム検証研究センター（CVS/AIST）では、システム設計および開発に資する検証 技術の普及を活動目的として、産総研コンソーシアム・システム設計検証技術研究会を開催しています。ここでは、数理的技法にもとづく検証についての講演や、世の中で広く使われている検証ツールの紹介を行なっています。

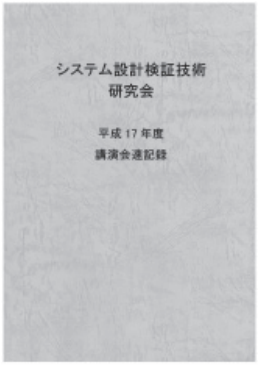
■平成１８年度（２００６年度）活動内容

本研究会は会員制で、平成１８年度会員数は組織として 16 団体、個人では 12 名でした。本年度は、講演会を中心に活動いたしました。主に国内の大学や企業から講師をお招きし、７回の講演会を開催いたしました。
※講演内容は速記録としてまとめられ、会員限定で配布しております。

各講演会の後は、講師を囲んで、講演中に出来なかった質問や、普段では聞けない苦労話から、この分野のトレンドにいたるまで様々なお話ができる場を提供しております。会員の皆様には、講演とともに、交流会での収穫も多い機会です。

■平成１９年度会員募集

現在、平成 19 年度の会員を募集しています。
本研究会は会員制です。法人会員（企業、学会、研究機関など）と個人会員がありますが、いずれも産総研（AIST）の承認が必要です。



システム設計検証技術研究会
速記録

速記録には、講演で使用した発表資料とともに、講演内容だけでなく、質疑応答までも忠実に再現し、掲載しております。レファレンスに最適な一冊です。

年会費：

法人会員　１０万円　　個人会員　無料

注）１ 法人会員の場合、1 団体で何名様でも講演会にご参加いただけます。
注）２ 企業在籍の方は原則として法人会員としてのご参加をお願いいたします。

お申込の詳細は、CVS/AIST のホームページ（URL: http://unit.aist.go.jp/cvs/conso-top.html）をご覧の上、事務局にメールにてお申込ください。

システム設計検証技術研究会の会員は、システム検証研究センターが主催する講演会やその他イベントへ優先的に参加することができます。また、速記録も配布されます。平成１８年度の速記録は、３月下旬に発行予定です。

◆シリーズ「システム検証技法」

モデル検査法③（最終回）「モデル検査による検証の落とし穴」

計算機の高速化とモデル検査ツールの発達によって、モデル検査によるシステムの振る舞い検証は有望になっている。しかし、モデル検査は万能ではなく、使い方にも注意を要する。今回はそのようなモデル検査にまつわる落とし穴を紹介する。

前回の記事で書いたように状態爆発問題を回避する方法がいくつも提案されているが、システムの全状態を全てそのまま扱うことは不可能である。結局は何らかの方法で状態数の比較的少ないモデルを作成しないと、モデル検査では結果を得ることはできない。ここで一つの問題が発生する。即ち、作成されたモデルは元のシステムに対して妥当であることをどうやって保証したらよいか、という問題である。システムの信頼性を確保するためには、検証 (verification) だけでなく、このような妥当性 (validation) も重要となる。ソフトウェア工学では二つをまとめて Verification and Validation(V&V) と呼ぶことがしばしばある。妥当性は最終的には人間の判断が必要となる。従って、妥当性の確保のためには、システムに関して詳しく理解している人と、その人が誤解なく正確に振る舞いを把握できるモデルの表記法が必要となる。

例えば、複数のシステムが並行に動作する並行システムの場合、一つ一つのシステムの振る舞いは理解できるが、全体の振る舞いは人間の理解を超えてしまう。従って、システム全体の振る舞いをモデル化した場合、妥当性の確保は難しい。そこで、モデル検査ツール

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

平成１９年度も、国内外から著名な講師を招聘し、これまで以上に有益な講演会を開催してまいります。そのほか、テーマ別の討論会や技術研修会なども企画し、産総研コンソーシアムとして活動の幅を広げてまいりたいと存じます。
活動内容に関しまして、皆様からのご意見ご要望がございましたら、事務局にメールにてご連絡ください。

今後とも、システム設計検証技術研究会の活動にご支援賜りますようお願い申し上げます。

平成 19 年２月
システム設計検証技術研究会　事務局

【平成 18 年度実施講演会一覧】

第１回講演会　平成 18 年７月６日開催
「次世代組込みシステムのためのソフトウェアプラットフォーム」
講演者：早稲田大学理工学術院コンピュータ・ネットワーク工学科
　　教授　中島　達夫氏

第２回講演会　平成 18 年７月 27 日開催
「モデル検査技術に基づく UML 設計検証ツールの紹介」
講演者：北陸先端科学技術大学院大学　情報科学研究科
　　特任教授　岸　知二氏

第３回講演会　平成 18 年８月 21 日開催
「組込みソフトウェア検証における組合せテスト設計の戦略と技術」
講演者：バルテス株式会社　技術部　マネージャー　石原　一宏氏

第４回講演会　平成 18 年 10 月６日開催
「ディペンダブルシステム ― 高信頼システム実現のための耐故障技術」
講演者：国立情報学研究所 アーキテクチャ科学研究系
　　教授　米田　友洋氏

第５回講演会　平成 18 年 11 月 16 日開催
「エンピリカルソフトウェア工学と EASE プロジェクト」
講演者：奈良先端科学技術大学院大学　情報科学研究科
　　ソフトウェア工学講座　教授　松本　健一氏

第６回講演会　平成 18 年 12 月 21 日開催
「航空機開発で採用されているモデル検証ツールとデモ」
講演者：富士設備工業株式会社　電子機器事業部
　　取締役事業部長　浅野　義雄氏

第７回講演会　平成 18 年１月 26 日開催
「Real World of Software Testing」
講演者：「知識ゼロから学ぶソフトウェアテスト」の著者
　　高橋　寿一氏

では、一つ一つのシステムのモデルを入力すると、全体は機械的に合成され全体の検証が行われる。各々のモデルの妥当性は確保しやすく、それによって、全体の妥当性も確保されるのである。

妥当と判断されたモデルが存在したとしても、それが状態爆発を起こしてしまう場合は、モデル検査を行うためにはモデルの修正が必要になる。そこで、妥当性を確保したまま状態数の少ないモデルに変形する方法が必要となる。当センターは、このような抽象化技法を重要と捉え研究を行っている。

モデルの妥当性は重要だが、実は妥当性というのは検証したい性質に依存する。例えば、デッドロックが起こらないことを検証したい時は、デッドロックを引き起こすリソースの競合だけが問題で、詳細なデータの値を省略しても妥当性は満たされる。しかし、データの値が問題になる場合には、省略することができない。従って、妥当なモデルは一つだけ存在するといったものではなく、検証事項に応じたモデルが必要になる。極端に言い換えると、検証事項が決まらない限りモデルは作成できず、モデル検査もできない。

モデル検査はあくまで道具であって、まずは検証したい事項をよく検討しておくことの方がより重要である。検証事項ごとに見通しのよいモデルを作成することは、モデル検査で検証できる可能性もあるし、モデル検査不能であっても開発の手助けにもなると思われる。

副研究センター長　高橋　孝一

■シリーズ・システム検証技法 " モデル検査法 " は今回で最終回です。ご愛読ありがとうございました。

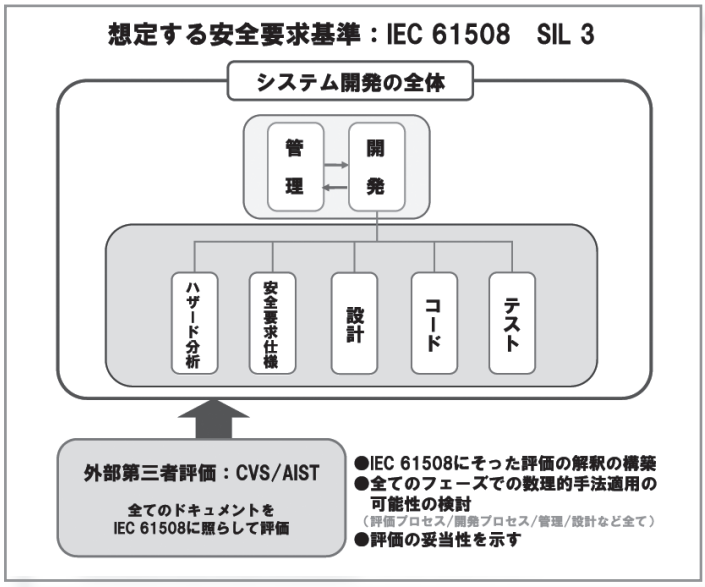
産業技術総合研究所　システム検証研究センター http://unit.aist.go.jp/cvs/
●千里サイト　：〒 560-0083　大阪府豊中市新千里西町 1-2-14　三井住友海上千里ビル 5F
●関西センター：〒 563-8577　大阪府池田市緑丘 1-8-31

● CVS ニュース

ソフトウェア認証にむけて

CVS/AIST は機能安全対応自動車制御用プラットフォーム開発プロジェクトに参画しています

CVS/AIST は、株式会社ヴィッツと名古屋大学大学院情報科学研究科附属組込みシステム研究センターを中心とした、機能安全規格 IEC 61508 の SIL 3 への適合を想定した機能安全対応自動車制御用プラットフォーム開発プロジェクトに参画しています。この開発プロジェクトは、経済産業省の平成 18 年度戦略基盤技術高度化支援事業（中小企業基盤整備機構）に採択されました。



このプロジェクトは、IEC 61508 SIL 3 に対応する自動車制御システム向けプラットフォームの開発とその標準化を目指します。さらに、プロジェクトに参加する企業や団体だけでなく、中小企業全体に機能安全に対応するスキルを広めることを目指しています。

※今回のプロジェクトで開発された OS、ミドルウェア、アプリケーション、ドキュメントはすべて無償公開される予定です。

■ CVS/AIST の役割

CVS/AIST は、このプロジェクトの研究実施者の一組織として全体に関わっていきますが、主な役割としては、「ソフトウェア開発における安全性分析手法の確立」、および開発されたソフトウェアに対する「第三者評価の実施と評価レポートの作成」の二つがあげられます。

プロジェクト全体の具体的な目標：

1. 安全機能 OS の開発：
これまでバラバラで管理されていた各アプリケーション等の運用状況や動作の確認などを、一括で動的に管理する機能をもつ OS の開発

2. 通信ミドルウェアの開発：
自動車の制御を通信で行なうアプリケーションの開発

3. 次世代例示アプリケーションおよび対象サンプル車輌製作

4. 機能安全対応ドキュメント作り：
開発プロセスからプログラムを含む、開発に関わる全てのドキュメント作り

「ソフトウェア開発における安全性分析手法の確立」

CVS/AIST は、ソフトウェアの安全性分析手法を、IEC 61508 で推奨されている手法に基づき、他の研究実施者と共同して確立していきます。各ソフトウェア開発の根幹となる安全要求仕様はこの安全性分析手法により決定されます。

「第三者評価の実施と評価レポートの作成」

このプロジェクトでは、各種ソフトウェアが開発されていきますが、CVS/AIST では、このソフトウェア開発について IEC 61508 の要求事項に則した第三者評価を行ないます。
IEC 61508 は機能安全の一般的な枠組みですので、実際にソフトウェアを開発する際には、これを具体的な対象にあわせたものに落とし込む必要があります。CVS/AIST では、この落とし込み作業が妥当かどうかを第三者として評価していきます。

■プロジェクトを通じての活動

今回のプロジェクトで CVS/AIST は、ソフトウェアにおける機能安全を確保していくための様々なプロセスに取り組んでいきますが、全てのプロセスにおいて数理的技法の適用の可能性を合わせて検討していく予定です。

CVS/AIST は、フィールドワークの一環としてこのプロジェクトに取り組み、数理的手法適用範囲拡大の可能性を追求するとともに、ソフトウェア認証を行なっていくための枠組みの基礎を構築していくことを目指しています。これを継続し発展させ、CVS/AIST の目標でもある、本格的なソフトウェア認証枠組み構築につなげ、安全で信頼できる社会への貢献を目指していきたいと考えています。

プロジェクトの詳細はこちらから：http://www.toppers.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
●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

2006 年 12 月～ 2007 年 02 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

日付　　講演者（所属）

2006 年

12/07　新田　直也 (甲南大学)
12/14　Jacques Garrigue（名古屋大学）

2007 年

01/11　Tadeusz Litak（北陸先端科学技術大学院大学）
01/18　結縁　祥治 (名古屋大学)
01/25　一杉　裕志（産業技術総合研究所)
02/01　Bengt Nordström（シャルマース工科大学）
02/08　Bengt Nordström（シャルマース工科大学）
02/15　Bengt Nordström（シャルマース工科大学）
　　安部　達也 (東京大学)
02/16　中野　昌弘（北陸先端科学技術大学院大学)
　　小西　善二郎（東京女子大学）
02/22　Peter Ölveczky(Univ. Oslo)
02/23　矢田部　俊介（神戸大学）
　　Bengt Nordström（シャルマース工科大学）
03/01　Bengt Nordström（シャルマース工科大学）

※今回シャルマース工科大学の Bengt Nordström 教授が CVS/AIST に 5 週間滞在されるのを機に「構成的型理論」について 2 月から 3 月初旬にかけて連続 5 回講義をしていただきました。

（開催場所：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▼
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）

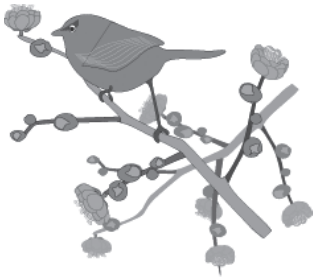
第六回　2006 年 12 月 21 日開催
講演者　浅野　義雄（富士設備工業株式会社）
演　題　「航空機開発で採用されているモデル検証ツールとデモ」

第七回　2007 年 01 月 26 日開催
講演者　高橋　寿一（「知識ゼロから学ぶソフトウェアテスト」著者）
演　題　「Real World Software Testing」

※平成 1 8 年度は 1/26 の第七回講演会で終了し、当日総会も実施しました。現在平成 1 9 年度会員を募集中です。

（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▼
コンソーシアムの URL：http://unit.aist.go.jp/cvs/consortium/



出版

◆テクニカルレポート

2007 年
2 月発行

PS-2007-001
Satoru Yoshida
"A note on the weak topology for the constructive completion of the space D(R)"

PS-2007-002
Hiroki Takamura
"Semisimplicity, EDPC and discriminator varieties of modal FLew-algebras (Preliminary Version)"

PS-2007-003
Toshifusa Sekizawa, Toshinori Takai, Yoshinori Tanabe, and Koichi Takahashi
"A Method to Generate Formulae for Temporal Logic Satisfiability Checkers"

PS-2007-004
Toshifusa Sekizawa, Yoshinori Tanabe, Yoshifumi Yuasa, and Koichi Takahashi
"MLAT: Modal Logic Abstraction Tool"

※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

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