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
7
2007.09

巻頭に寄せて

夏休み、参観にいった子供の特別授業で、正多面体がおしえられていたのをみて、小学生のとき、父に正十二面体や正二十面体の展開図をおしえてもらい、「バフンシでつくってみよ」といわれたのをおもいだした。バフンシとは何かいな、馬糞紙？ それはまたなんと品のない表現であることよ、馬糞なんぞみたことがないが、あれはボール紙のような色をしているのか、などと感心しながら、近所の文房具屋へいってバフンシをくださいといったら、やはりちょっとびっくりされ、しかし意味はちゃんとつうじて、それをつかって、父に教えてもらいながら正多面体を五種類つくったのをおぼえている。正五角形の定規とコンパスによる作図法はややこしかった。後に中学生になってから、学校の技術家庭でもならった覚えがあるが、今はまったくわすれてしまった。正多面体が五種類しかないというのはずっと覚えている。今回初めて納得できる理由をみつけた。

厚紙をはりあわせるのではなく、折り紙で多面体をつくっている人たちもいるらしい。一枚の紙でつくるとはかぎらず、部品を折り紙でつくって、それをくみあわせて、正多面体や準正多面体、星形などどんどんつくる場合もあるのだそうだ。ユニット折り紙という言葉もしった。いろいろな多面体をひたすら折り紙で折った結果をみると迫力をかんじる。

折り紙の幾何学的な取り扱いへの興味は大きいらしく、既に何人かの方々によってまとまった仕事がなされているようだ。伏見康治満枝夫妻の著書がパイオニアの一つのようだ。計算機に関係する仕事もある。ちょうど一年ばかり前、井田哲雄さんが「計算折り紙(Computational Origami)」のお話を千里で講演してくださった。はじめに聴衆に出された課題が、正方形に内接する正三角形を折り紙で折ってみよ、というものだった。お話の内容は折り紙による作図を公理化し、作図の正しさの証明を計算機でおこなう、というものだったと記憶する。なるほど、折り紙は検証の実演の題材によさそうだ、と思ったものだ。

以上を書いている最中に出席した研究会で、フラクタル立体図形についての立木秀樹さんのお話をきいた。模型を作って京都大学の博物館に展示もしているとのこと。ホームページでも、いろいろあそべる。このような図形と計算機の多様な関わりに、システム検証がどう関係するだろうか？ 折りにふれてかんがえている。

2007 年 9 月

システム検証研究センター
センター長　木下　佳樹

＜ＣＶＳニュースレター　７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

２００６年度 システム検証研究センター 研究成果報告会

システム検証研究センター (CVS) では、３月 15 日に 2006 年度に当研究センターで行われた研究についての成果報告会を開催いたしました。

本レターでは、発表された１７の研究項目について、概要をご紹介いたします。発表内容の全容はテクニカルレポートにまとめ冊子として発行いたしました。ご希望の方は、当センターホームページよりお申込ください。また、ホームページより直接 PDF ファイルでダウンロードも可能です。

http://unit.aist.go.jp/cvs/techrep.html

２００６年度システム検証研究センター 研究成果報告 全１７研究項目概要

1. フィールドワーク１

班長：大崎人士
班員：石田麻紀　尾崎弘幸　高井利憲　松本利雅　吉田聡　（小池憲史）

計５件のモデル検査実験を行い、従来手法では発見困難なバグの発見、リセット機構の効果的なモデル化、２種類のモデル検査ツールの有効性などの評価などの成果があった。昨年度の実験からの知見も含めた今年度の具体的な成果は、モデル化支援ツールである C2Promela コンバータ と Promela スライサーの開発、図示記法とスペックパターン辞書（LTL 検査式用例集）、環境ドライバやスケルトンをはじめとするモデル検査ノウハウに関する技術文書などがある。図示記法は、企業からの研究参加者と産総研研究員との共同研究作業の過程で生まれた成果で、モデル検査の現場導入に大きく貢献した。

2. フィールドワーク２

班長：高橋孝一
班員：清野貴博　髙木理　竹内泉　和泉憲明

本年度では、産総研次期イントラシステム開発の要件定義において、実際に使用されているドキュメント（業務フロー図）を対象とし、数理的技法の導入を試みた。この結果、数理的解析に用いることができるドキュメントが実際の開発の中で記述され、そのドキュメントを元に我々の手で解析を行うことができた。これらの成果によって、ドキュメントの質が向上した。数理的技法の導入にあたっては、次期イントラシステムの開発部隊との折衝を行ったが、その際に旧来用いられていた記法では数理的解析を行うために不足していた情報の追加記述を依頼し、受け入れられた。

3. フィールドワーク４

班長：湯浅能史
班員：水口大知　渡邊宏

車載ソフトウェアの対話的検証法：年度初めより夏までの間、大学や自動車関連企業と共同で、車載ソフトウェアの検証方法に関する研究会を数回行った。我々システム検証研究センターからは、ソフトウェアの正しさを、証明支援ツールＡｇｄａとの対話的な証明構築で保証する方法を提案した。題材として車間距離や運行速度を自動的に一定に保つ「オートクルーズコントロールシステム」を取り上げ、自動車の制動装置や路面状況等を含む物理環境と制御ソフトウェアが、相互に関係をしあう状況を数学的にモデル化した。

4. フィールドワーク５

班長：渡邊宏
班員：清野貴博　髙村博紀

モデル検査法を用いた通信プロトコル設計支援の研究を行った。これは企業の数理的技法導入に向けた検証試供品を開発することを目的とした活動で、設計段階でのモデル検査の有効性を実際に企業との共同研究の中で確かめ、企業にその有効性を納得させ、開発の場に導入させることが目標である。具体的には、双方向にデータの送受をし、データ送信がウォッチドッグ機能の役割を担うなど現実的でかつ一般的な通信プロトコルの設計段階にモデル検査器 UPPAAL を適用する事例研究を行った。

5. 研修コース開発

班長：西原秀明
班員：池上大介　上出哲広　木下佳樹　崔銀恵　中原早生　水口大知　渡邊宏　宮原則子

「モデル検査初級」の研修コーステキストを「四日で学ぶモデル検査初級編」というタイトルで出版した。前年度末にパッケージ化した「研修コース講師用手引き」と共に、モデル検査の普及教育体制のひとつが定まったことになる。続いて「モデル検査中級」の開発を行った。教材作成 (カリキュラムに沿った研修内容の詳細化、受講者 (技術者) にあった実例や演習の作成)、試行開催を行った。センターに蓄えられたモデル検査に関する知見・経験が、例や演習の作成時に大いに役に立ったことを特に指摘しておく。中級編の教材は初級編と同様にテキストなどの形でパッケージ化される予定である。

6．ソフトウェア認証研究

班長：松岡聡
班員：木下佳樹　長谷部浩二　水口大知

昨年度に引き続き、計量器および機能安全系におけるソフトウェア認証技術についての調査・研究を行った。計量器については、タクシーメータの改竄検出に必要となる機能要件をまとめて、メーカーに実施させるとともに、その認証を型式承認の一部として開始した。また、法定計量におけるソフトウェア認証についての解説書の執筆を開始した。機能安全系については、国際規格 IEC 61508 に関する国内外委員会出席および様々な動向調査に加えて、戦略的基盤技術高度化支援事業に採択されたプロジェクト「機能安全対応自動車制御用プラットフォームの開発」を名古屋大学らと開始した。今年度はまず IEC 61508 準拠のために必要となるソフトウェア安全性分析手法の開発に着手した。なお８月にはカナダにて、計量器および機能安全系におけるソフトウェア認証の国内動向について発表した。

7．抽象化ツール研究開発

班長：高橋孝一
班員：関澤俊弦　高井利憲　田辺良則　湯浅能史

ポインタを操作するプログラムのソースコードを網羅的に検証するためには、抽象化が必須である。我々は、ポインタ操作をするソースコードから、抽象化された状態遷移系を自動生成する MLAT ツールを作成した。生成された状態遷移系を全数探索することによって検証が可能になる。また、MLAT の一部を対話型検証器 Agda と連携させた。

8．数理モデル研究

班長：木下佳樹
班員：岡本圭史　高井利憲　髙村博紀　竹内泉　武山誠　中原早生　西澤弘毅

プログラミング意味論の研究を行うことを目的としている。第一に一階様相 μ 計算によって並行システムが竦合に陥るための Coffman 条件を定式化して事例を与え、一階様相 μ 計算から函数記号を除去する手法を与えた。第二に重みつきクリプキ構造を用いて多値モデル検査における抽象化の意味論を与え、模倣定理などを証明して日本ソフトウェア科学会高橋奨励賞を受賞した。第三に正則木言語の部分集合の代数的特徴づけを試みたが、これはさらに検討が必要である。

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

９．対話型検証研究

班長：武山誠

班員：池上大介　尾崎弘幸（10 月～）　加藤紀夫　清野隆博　西原秀明　宮原則子　山下伸夫（10 月～）

対話型定理証明支援系 Agda の研究開発および普及を行うことを目的として、本年度は Agda1 の簡易マニュアル整備とコード例の集積を行なって Agda ホームページを本格稼動させ、Agda1 の配布パッケージを提供した。また第 4 回 AIM ― (Agda Implementors Meeting) を開催した。Agda2 核言語の設計も進めている。

１０．依存型付作譜言語研究

班長：尾崎弘幸

班員：加藤紀夫　武山誠　山下伸夫

Agda の記述言語は証明記述言語であるのと同時に、依存型を持つプログラミング言語でもある。我々は、Agda の記述言語をプログラミング言語とみなした開発環境を構築した。具体的には、コンパイラ Agate とライブラリを開発した。実用化を視野に入れ、コンパイラの最適化処理も実現した。

１１．MPI ライブラリ検証研究

班長：山形賴之

班員：斎藤正也　高橋孝一　水口大知　湯浅能史　加藤紀夫　西澤弘毅

MPI 仕様ライブラリ YAMPII を、モデル検査器 SPIN を用いて検証した。今回の検証の目的は、分割され非同期に送信されるデータが適切に受信・再構成されることによって、送信内容と受信内容の一致が達成されることである。検証対象となるモデルは、特に重要な通信管理部と通信実行部のソースコードをもとに作成した。検証可能な範囲では、反例は発見されなかった。

１２．木構造オートマトン

大崎人士

等式付ツリーオートマトン理論に基づく自動検証ツール (ACTAS) の開発を中心に研究を実施した。イリノイ大学 (Jose Meseguer 教授他) と共同開発している検証用ライブラリ CETA の機能向上により、検証エンジンの基本性能の向上が得られた。また, これまでの等式付ツリーオートマトンの研究成果に対し『平成 18 年度文部科学大臣表彰 若手科学者賞』が授与された。

１３．π計算の論理

竹内泉

本研究の目的は、業務システムの仕様記述に適した代数付きπ計算、及び、それによって記述された仕様の性質を証明する論理体系を設計することである。論理体系について、カット除去によって証明探査と反例構成の手続を同時に進めることが目標であったが、カット除去に対する本質的な困難が見つかった。

１４．空間表現意味論に関する研究

竹内泉（関西学院大学教授高橋和子氏との共同研究）

本研究の目的は、二次元ユークリット空間、即ち平面上の図形に対して機械的な推論や操作をする為の形式的表現を提案することである。本研究では位相的性質を処理する為の表現方法を提案する。2006 年度の研究成果は、ある PLCA 表現が確かに何かの平面図形を表していることの必要十分条件を与えたことである。

１５．PML 意味論の研究

班長：木下佳樹

班員：高橋孝一　田辺良則　湯浅能史

抽象化ツールの研究では、研究対象としてポインタを処理するための言語 PML (Pointer Manipulation Language) を導入している。本研究項目では，PML の操作的意味論を定義した。その上で、PML プログラムに対する検証が行えるように、Hoare 流の証明を行うために必要な公理を導入し、定義した意味論のもとで、体系の健全性を証明した。

１６．形式仕様開発支援環境の研究

清野貴博　武山誠

本研究では、代数仕様言語 CafeOBJ を対象とした形式仕様開発支援環境の構築を目的としている。CafeOBJ では記述した仕様を項書換え系とみなすことで、項書換えによる等式推論を行うことができる。年度進捗としては、Agda から CafeOBJ を呼び出すための Agda プラグインを開発した。

１７．フォールトトレラント分散アルゴリズムの検証

班長：崔 銀恵

班員：岡本圭史　竹内泉　土屋達弘　菊野亨（大阪大学）Moonzoo Kim (KAIST)

近年、いくつかの重要な耐故障分散アルゴリズムは、合意アルゴリズムと故障検出機構に基づくモジュラー構造に分解できることが示された。この構造に従い，耐故障分散アルゴリズムの自動検証法確立を目指し、次の研究を行った。1) 分散システム上の故障の分類毎のモデル化手法を開発。商用機器組込の耐故障分散グループマネジメントプロトコルの検証に適用し、不具合を検出。2) 上記モジュラー構造耐故障分散アルゴリズムのモデル検査法の枠組みを考案し、非ブロッキング原子コミットプロトコルの検証に適用。

◆シリーズコラム

機能安全（第 1 回）「機能安全と IEC 61508」

「機能安全」という言葉が、ここ数年の間でよく聞かれるようになった。産総研 CVS では、その国際規格である IEC 61508 の適合認証に関する研究を進めている。
そこで、今回の連載では、機能安全と IEC 61508 について、少しまとめて紹介したい。

機能安全とは、標語的に言えば、「安全関連系を用いて危険源を制御することにより確保される安全」のことである。こういうと難しく感じられるかもしれないが、例えば踏切において遮断機や警報機によって確保される安全がその代表である。

このように機能安全は、随所で活用されてきたものだが、その形態はコンピュータ技術を用いたものへと発展してきている。これを受けて、“Functional safety of electrical/electronic/programmable electronic safety-related systems” と題した国際規格 IEC 61508 が、2000 年迄に制定され、その JIS 化の際、「機能安全」という邦訳語が誕生した。昨今、国内において IEC 61508 が大きく注目されている理由を、以下に挙げてみたい。

①包括的な規格：従来の製品安全規格とは違い、IEC 61508 はコンピュータ技術による安全関連系の、ライフサイクル全体にわたって要求事項を定めている。さらに組織の機能安全管理や監査、従事者の適性についても述べており、新たなタイプの総合的な規格となっている。

② SIL の導入：IEC 61508 では、安全関連系の性能をリスク軽減の度合いに応じて 4 つの水準に区分しており、これを「安全度水準」(Safety Integrity Level; SIL) と呼んでいる。これにより、ランダムハードウェア故障の世界と、決定論的

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

定理証明支援系 Agda とは

定理証明の技術はシステム検証のための基本的な道具の一つですが、人間が紙と鉛筆だけを使って証明を記述するのは手間がかかり、間違ってしまうこともあります。実は、コンピュータを使って定理証明を行うための便利なツールが存在します。Agda はそのようなツールの一つです。Agda は Martin-Löf 型理論に基づく対話型の定理証明支援系であり、証明が関数型プログラムとして得られるという特徴を持っています。今回は定理証明支援系と Agda の特徴について紹介します。

■ 定理証明支援系とは

定理証明支援系は、コンピュータを使って問題を記述し、その問題の正しい答え（証明）を得るためのコンピュータソフトウェアです。定理証明支援系を使うと、答えが正しいかどうかを機械の力を使って誤りなく検査できるので、答えの正しさについて絶対的な信頼性を得ることができます。定理証明支援系では「このシステムにおいてこの性質が成り立つことを証明せよ」という形で問題を記述します。例えば、情報処理システムの持つ性質の検証や、論理的な推論などがこの形で記述できます。正しさが証明された性質を定理と言います。

定理証明支援系を使うには、問題を厳密に記述する必要があります。対象のシステムをコンピュータ上で記述する作業をモデル化といいます。適切でないモデル化をすると元のシステムと無関係なシステムを検証することになってしまうため、モデル化の誤りが起こらないように注意する必要があります。

定理証明支援系はすべての問題を自動的に解いてくれるわけではありません。難しい問題については人間が解き方を指示し、コンピュータがその正しさを検査するという協調作業によって答えを見つけるのが標準的な使い方です。とはいえ、多くの定理証明支援系は、簡単な問題ならば自動的に解く能力を持っています。どのような問題が自動的に解けるかは個々の支援系によって異なりますが、その能力は自動定理証明やモデル検査と本質的に同じです。つまり、コンピュータが解き方を知っている形式で記述された問題しか自動的に解けないのです。この制限のため、難しい問題を無理に自動的に解こうとすると、問題の記述が不自然になり、モデル化の誤りが起こる可能性が高くなってしまいます。定理証明支援系を対話的に使えばこのような制限がないため、より自然な形で問題を記述することができ、モデル化の誤りを減らすことができます。

■ Agda の特徴

定理証明支援系 Agda は、対話型であることのほかに、一般的な関数型プログラミング言語と同等な構文を持つことを特徴としています。これは、プログラムを証明と見なす Curry-Howard の対応によって実現されています。このため Agda では、システムの記述、性質の記述、そして証明の記述の３つを１つの言語で行うことができます。また、関数型プログラムを対象とした検証においては、プログラムがそのままシステムの記述になるためモデル化が不要となり、モデル化の誤りを完全に無くすことができます。Agda のプログラムは関数型プログラムとして実行することも可能です。

現在新しいバージョンの Agda の開発が進行中であり、これから普及していくことが期待されています。システム検証研究センターでは、Agda から対話的に自動検証器を呼び出すことができる統合検証環境の構築を目指して研究開発をおこなっています。

システム検証研究センター　加藤 紀夫

故障の世界が統一的に扱われている。

③ソフトウェアの重視：IEC 61508 では、安全関連系を構成するソフトウェアの開発プロセス全体にわたって要求事項が述べられている。SIL 毎に用いるべき手法・技法のパッケージを規定している点が特徴的である。

④形式手法の推奨：特に SIL 4 の安全関連系を構成するソフトウェアについては、形式手法の使用を「強く推奨」している。

⑤広範な対象：規格の対象は、コンピュータ技術による安全関連系を用いる全ての分野であり、プロセス産業、鉄道、自動車、原子力、産業機械など広範囲にわたる。また、コンポーネント機器や、各種ツール等も規格に沿った開発が求められる。

⑥自動車分野への適用：現在 ISO において、IEC 61508 に基づく自動車の機能安全規格が策定中であり、国内ではその動向が注視されている。

⑦適合認証への需要：特に欧州市場では、センサーや PLC 等の安全関連系の構成機器に対して、IEC 61508 への適合認証取得が求められており、国内メーカーも対応を進めている。その対象範囲は拡大しつつある。

⑧欧州主導：IEC 61508 は、英国とドイツの主導によりまとめられた規格であり、国内の慣行にそぐわない面もある。また、適合認証もこの２ヶ国の企業が主に実施しているため、認証取得を目指す国内企業にとっては負担が大きい。

⑨ソフトウェア安全性への期待：ソフトウェアの不具合によって、製品の安全性が損なわれる事例が多数報告されている現状にあって、IEC 61508 の考え方が様々なソフトウェアシステムの安全性確保に有効であると期待されている。

次回以降は、IEC 61508 に述べられている機能安全の方法論、および、適合認証の課題について記したい。

システム検証研究センター　水口 大知

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

モデル検査研修コース中級編の完成へ

CVS ではモデル検査法の普及を目指してモデル検査研修コースを開発していますが、中級編の完成が目前となりましたので御紹介します。

中級編は、初級編を修了してモデル検査の基本を理解した方々が、モデル検査の標準的な技術を身につけるためのコースです。中級編の修了によって、開発現場で直面する課題の幾つかを独力で解決できる程度の能力を身につけることができます。

中級編は「モデルの合成」「モデルの抽象化」「CTL」の三章から成ります。

■モデルの合成

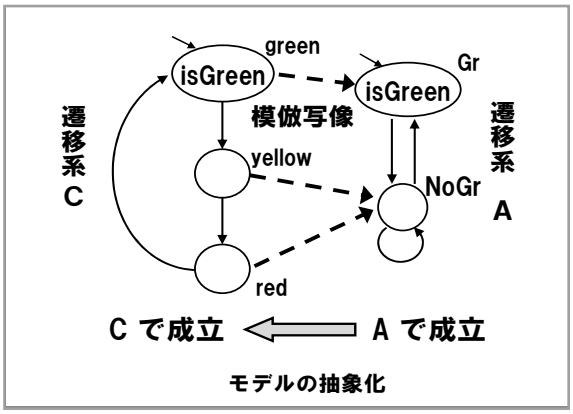
初級編では、検査対象のシステム全体をそのまま遷移系に書き下していました。しかし通常行われているシステム設計を考えると、機能や動作で分割したモジュール毎にモデル化し、それを組み合わせて全体のモデルをつくるほうが自然です。この「モデルを組み合わせる」ことをモデルの「合成」と呼びます。各モジュールが同期して動作しているか、変数を共有しているか、などの状況によって複数の合成手段があり、またモデル検査ツールによっても使える合成は異なってきます。

中級編の「合成」の章では重要な四種類の合成を説明し、具体的な使用例を紹介します。特に演習として三つの排他制御アルゴリズムを合成を使ってモデル化し、その安全性などを検証します。

■モデルの抽象化

さて、モデル検査には状態爆発問題という本質的な問題があります。これは巨大なモデルに対して起こり、なんとかしてモデルを縮める以外に解決策はありません。しかしモデルの性質が変わってしまうほど縮めてしまっては意味がありません。モデルの性質を変えないように小さなモデルをつくる手段の一つを「抽象化」といいます。

中級編の「抽象化」の章では、状態をまとめる写像である「模倣写像」を説明します。「モデルを縮める」＝「状態数を減らす」＝「複数の状態をまとめる」と考えると、模倣写像は一つの抽象化を与えます。次に LTL 式の保存定理を紹介します。これは中級編で扱う抽象化の中心となる定理で、模倣写像で縮めたモデル M' で検査式が成り立てば、縮める前のモデル M でも同じ検査式が成り立つことを保証します。章の後半では保存定理を応用したより具体的な抽象化 (データ抽象化、述語抽象化) を説明します。



モデルの抽象化

■ CTL

初級編では LTL (Linear Temporal Logic) という論理を使って検査式を記述しましたが、他にも「CTL」(Computational Tree Logic) という論理がモデル検査に使われています。これらの論理は記述できる性質に差があり、互いに補完的なものになっています。中級編の「CTL」の章では、CTL の特徴やその定義を紹介し、 LTL との違いも説明します。

システム検証研究センター　西原 秀明

モデル検査研修コースの詳細はこちらから：
http://unit.aist.go.jp/cvs/kyotei/index.html

第四回システム検証の科学技術シンポジウムのお知らせ

開　　催　　日：２００７年１１月５日（月）～７日（水）
場　　所：名古屋大学 野依記念学術交流館

主　　催：日本ソフトウェア科学会ディペンダブルシステム研究会
講演者募集締切：２００７年　９月２１日（金）
原　稿　締　切：２００７年１０月１２日（金）

本シンポジウムでは、システム検証に関する研究発表、事例発表、ポスター発表、ソフトウエアデモ、解説講演を行います。

基調講演：木下　佳樹（産業技術総合研究所）
招待講演：石川　裕　（東京大学大学院 教授）
　　鈴村　延保（アイシン精機株式会社）
　　高浜　盛雄（名古屋大学大学院 教授）
　　林　　春男（京都大学 教授）

詳しくは、当研究センターホームページをご覧ください。
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

●イベント・講演会

2007 年 3 月～ 2007 年 10 月
イベント開催報告

◆計算機言語談話会（CLC） 原則毎週木曜日 定期開催中

日付	講演者（所属）
03/16	宮崎 裕（北海道大学）
03/16	加藤 和彦（筑波大学）
03/22	上出 哲広（CVS）
03/22	吉田 聡（CVS）
04/05	松本 眞（広島大学）
04/12	Armin Lawi（九州工業大学）
04/19	鹿島 亮（東京工業大学）
05/10	竹内 泉（CVS）、安部 達也（東京大学）
05/10	吉田 聡（CVS）
05/31	Michael Winter（Department of Computer Science, Brock University, Canada）
06/28	長谷部 浩二（CVS）
07/05	Li Xin（Japan Advanced Institute of Science and Technology）
07/12	長谷部 浩二（CVS）
07/26	高井 利憲（CVS）
07/31	松岡 聡（産総研　計測標準研究部門）
09/25	Jiri Adamek（Institute of Theoretical Computer Science, Technical University of Braunschweig, Germany）
10/04	武山 誠（CVS）
10/11	吉田 聡（CVS）
10/18	田辺 良則（CVS）、木下佳樹（CVS）
10/25	髙木 理（CVS）

（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）

第一回　2007 年 7 月 20 日 開催
講演者　山本 訓稔氏、服部 彰宏氏（富士ゼロックス株式会社オフィスプロダクト事業本部コントローラーソフトウェア開発部）
演　題　「Model Checking を適用した実践的非同期制御検証 」

第二回　2007 年 9 月 27 日 開催
講演者　中本 孝一氏（兵庫県立大学大学院教授）
演　題　「組込みソフトウェアの高信頼化開発手法」

第三回　2007 年 10 月 26 日 開催
講演者　栗田 太郎氏（フェリカネットワークス:モバイル FeliCa 開発）
演　題　「モバイル FeliCa IC チップ開発における形式仕様記述手法の導入」

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

一般公開　開催報告

2007 年 7 月 27 日産総研尼崎事業所において、「一般公開」を開催しました。当研究センターでは、***LEGO*** を用いた簡易プログラムの体験コーナーや夏休み算数教室「たし算のルール」と題して講義を行いました。来場者は４５４名にのぼり、盛況のうちに終了いたしました。

出版

◆テクニカルレポート

4 月発行
PS-2007-005
Koki Nishizawa, Yukiyoshi Kameyama, and Yoshiki Kinoshita
"Simulations of Multi-Valued Models for Modal μ -Calculus"

6 月発行
PS-2007-006
Satoru Yoshida, Yoriyuki Yamagata
" ソフトウェア更新システムプロトコルの BAN Logic による安全性検証 (Preliminary Version)"

7 月発行
PS-2007-007
システム検証研究センター
"2006 年度（平成 18 年度）研究報告集 "

PS-2007-008
Yoriyuki Yamagata, Masaya Saito
" ソフトウェア更新システムのモデル検査によるセキュリティ"

PS-2007-009
Koki Nishizawa
"Algebraic Structure for a modal fixed point logic and abstract interpretation"

※全てのテクニカルレポートは HP から入手可能です。
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