戦略的創造研究推進事業 CREST

研究領域「情報社会を支える新しい高性能情報処理技術」

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」

研究終了報告書

研究期間　平成 14 年 11 月～平成 20 年 3 月

研究代表者：木　下　佳　樹

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
研究センター長

1　研究実施の概要

情報処理システムの遍在化に伴い、組込システムをはじめとする情報処理システムの誤動作の影響が大きくなり、システムの検証技術がにわかに注目されている。 抽象化とよばれる手法によって膨大な記述量を持つシステムの検証を可能にし、ソフトウェアの信頼性を抜本的に向上させることが本計画の目的である。

プログラムの数学的モデルを与えるプログラム意味論が 1960 年代以来研究され続けており、これに基づくプログラムの検証法が一応の体系化をみせたのは 1970 年代初頭である。三十年以上にわたる研究の歴史を持つにもかかわらず、ソフトウェアの数理的検証法が、ソフトウェア開発の現場で用いられることは、いまだに稀である。 その最も大きな原因の一つは、検証の記述が膨大になって人間や自動検証器の理解の能力を超えたものになってしまうことにある。

システム検証での大きな課題の一つにスケーラビリティを得ること、つまりシステムやその性質の記述の量が爆発的に増えても、とり扱うことができる原理を与えることがある。 スケーラビリティを得るための有力な手法が抽象化である。 一般に、具体的なシステムの性質のうち、注目したい性質を保つが、他の性質は保つとは限らないようなシステムを、元のシステムを抽象化したものという。 逆に、抽象的なシステムからはじめて、その性質をすべて保つような具体化を行ったシステムを得ることを、詳細化といっている。 抽象化と詳細化は、たがいに逆の関係にある。

1990 年代に、研究代表者らは、詳細化(refinement)の一般的な意味論（数理的モデル）を、圏論における函手意味論の手法を用いて与えた。 ここでは、函手的意味論の常套手段に従って、情報処理システムのモデルを函手によって与え、詳細化は二つのモデルの間に与えられるものとして、函手の間の緩変換(lax transformation)として定式化される。 詳細化の函手的意味論は、システムを記述する言語（プログラミング言語）によってパラメータ化された形であたえられており、その意味で極めて一般的なものである。 研究代表者ら

は、プログラミング言語としてwhile命令を採用した場合を調べ、一般的な意味論を入力出力型システムに適用して具体化した。

ところで詳細化と抽象化は上述のように表裏一体の関係にある。 意味論は、システムを求める算法までは規定せず、算法が展開される数学的世界を記述するものだから、詳細化の意味論と抽象化の意味論は一致する。 つまり詳細化の函手的意味論はそのまま、抽象化の函手的意味論でもある。

本計画では、抽象化の函手的意味論の適用範囲を、入力出力型システムから刺激応答型システムに拡大するための意味論研究を行った。 命題様相μ計算の部分体系ではあるがCTLを含む体系Rμの構築とそこで抽象化の意味論構築と自由生成の存在証明がその内容である。 いっぽう、既に具体的な理論が立てられている入力出力型システムについては、研究代表者らの意味論が示す方向で、抽象化支援システムを試作することとした。 抽象化支援ツール周辺の文献調査を経て、ポインタ処理を行うwhile命令に関する抽象化を支援するシステムMLATを試作し、これを用いてDeutsch-Schorr-Waiteマーキング算法の正当性を検証してそのフィージビリティを示した。 一方で、定理証明支援系を作業台(workbench)として用いながら抽象化の正当性を検証する統合検証環境Agda-IVEを研究開発した。 われわれはMLATをAgda-IVEに組込み、研究計画の最終段階において、Agda-IVEのフィージビリティを確かめるために、実問題の検証を試みた。MPIの実装のひとつであるYAMPIIの開発者の協力を得て、そのなかから、ポインタ操作に問題が起こり得る部分を抽出し、その部分の正当性をAgda-IVEを用いて行なうという作業を行なった。 その結果、Agda-IVEにおける、AgdaとMLATの相互作用が、システムの検証対象を確定する試行錯誤の段階において極めて有用であることがわかった。

2 研究構想及び実施体制

(1) 研究構想

本研究は

抽象化シナリオ　与えられた具象システムの検証が記述量爆発によって困難であるため、より検証しやすい抽象システム、およびそれと具象システムとの間の関係を設定し、その関係が、抽象化関係:「抽象システムでの検証が具象システムでの検証を導く」を満たすことを前提として、抽象システムの検証に具象システムの検証を帰着させる。

に関する研究である。理論研究を行なう一方で、このような検証手法を支援するツールを研究試作した。

本研究の背景を提供するのは、1990 年代に研究代表者らが展開した、詳細化の極めて一般的な理論である。 詳細化 (refinement) とは、システムの抽象的な仕様記述から、その性質を保ちつつ、より具体的でプログラムに近い仕様記述に書き換える操作である。操作を逆向きに考えると、システムの具体的な記述から、その(重要な)一部の性質を保ちつつ、より抽象的な記述に書き換える、抽象化とよばれる操作となる。 所与のシステムを検証する立場からは、抽象化の操作が重要で、システムを構築する立場からは詳細化が大切であるが、これらは互いに逆の関係で、本質的には同じものである。

研究代表者らの先行研究の成果である入力出力型システムの抽象化の函手意味論では、while 命令の性質を過不足なく表す(圏の上の)代数的構造(以下ではWと記す)を設定し、システムを基本データ型を対象とし基本命令を射とする圏 S によって記述する。 記述の意味は任意に与えられたW代数Dにおいて、解釈される: W代数の全体がなす圏 W-Alg から Cat への忘却函手を U とすると、S から U(D)への函手(解釈函手)を与えることによって、記述の意味が確定する。 詳細化においては、具体的な解釈 C と抽象的な解釈 A の二つの解釈函手があると考える。 詳細化の関係を、C から A への緩変換(lax transformation)によって表現する。 関係を逆にみれば抽象化の関係が得られる。

本計画では、同様の手法で、刺激応答型システムの抽象化をモデル化する計画を立てた。これが、本計画の理論研究の骨子をなす。 刺激応答型システムを表す命題様相論理のうち最も一般的な命題様相 μ 計算に関する抽象化を考察した。 この体系の代数構造を

与えることには集合論的な問題があるので、命題様相 μ 計算の部分体系ではあるが、実用上問題のない程度に一般的な体系 Rμ を設定し、これに関する考察を展開した。

いっぽう、先行研究に基づいて、既に具体的な理論が立てられている入力出力型システムの抽象化については、この理論が導く方向で、抽象化を支援する検証システムを試作することとした。 抽象化においては、二つの数理モデルが関係するので、正確な理論だてなしには混乱が生じがちであった。 我々は、一般論から厳格な意味論を入出力システムの抽象化に対して与え、これに基づいて試作システムを考察した。

文献調査の結果、入出力システムのうち、とくにポインタを操作するシステムの抽象化を考察することとした。 ポインタ処理命令を基本命令としてもつ while 命令を設定して PML（Pointer Manipulation Language）と名づけ、PML の状態を記述するための様相論理 2CTLN（2 way CTL with Nominals）を構築し、これに関する抽象化を支援するシステム MLAT（Modal Logic Abstraction Tool）を試作した。 これは、高橋孝一らによって以前からなされてきた、ポインタの参照関係に関する考察の発展でもあった。

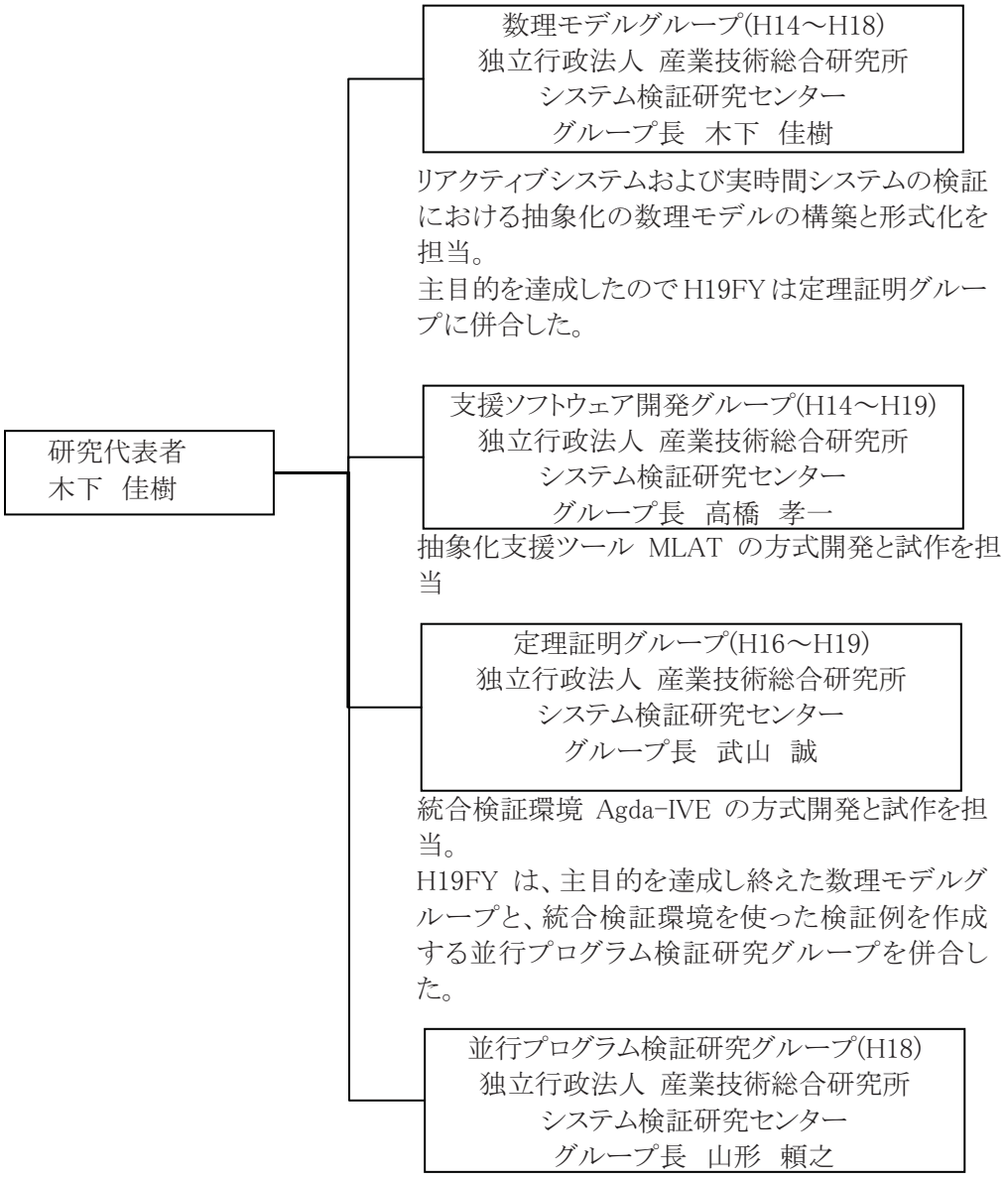
高橋らの研究は、自動検証を指向するものである。 しかしながら、われわれは計画当初より、計算機による対話的な検証支援の重要さも研究活動の視野に入れていた。 計画二年目に定理証明支援系研究を専門とする武山誠が参加したのを機会に、統合検証環境の研究を題目に加えた。

自動検証システムを使って検証する場合にでも定理証明支援系を、複数の自動検証系の作業台として用いて、与えられた検証課題を、定理証明支援系によって分解、加工し、自動検証系に処理させ、得られた結果をさらに定理証明支援系によって処理していく、という検証方法を統合検証環境と呼んでいる。 我々は定理証明支援系 Agda を土台にして、その内部構造を変更して SMV や Gandalf（一階述語論理自動検証系）さらに pfvalid（2CTLN の充足可能性判定器。MLAT の部分システムである）などの plug-in を付加した Agda-IVE の上での検証手法を開発した。

計画の最後一年半を費やして、Agda-IVE における検証事例を実問題にもとづいて提示

した。 MPI (Message Passing Interface)の実装の一つである YAMPII システムの開発に参加して、開発者にとって心配な検証課題を抽出し、ある性質が繰り返しによっても不変であることの検証を Agda-IVE によって行なった。 いっぽう、Deutsch-Schorr-Waite の印付け算法の正当性検証を Agda-IVE において行い、MLAT のスケーラビリティを示した。

(2)実施体制


研究代表者
木下 佳樹
数理モデルグループ(H14～H18)
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
グループ長 木下 佳樹
リアクティブシステムおよび実時間システムの検証における抽象化の数理モデルの構築と形式化を担当。
主目的を達成したのでH19FYは定理証明グループに併合した。
支援ソフトウェア開発グループ(H14～H19)
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
グループ長 高橋 孝一
抽象化支援ツール MLAT の方式開発と試作を担当
定理証明グループ(H16～H19)
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
グループ長 武山 誠
統合検証環境 Agda-IVE の方式開発と試作を担当。
H19FY は、主目的を達成し終えた数理モデルグループと、統合検証環境を使った検証例を作成する並行プログラム検証研究グループを併合した。
並行プログラム検証研究グループ(H18)
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
グループ長 山形 頼之
YAMPIIの検証実験を担当

3 研究実施内容及び成果

3．1リアクティブシステムおよび実時間システムの検証における抽象化の数理モデルの構築と形式化

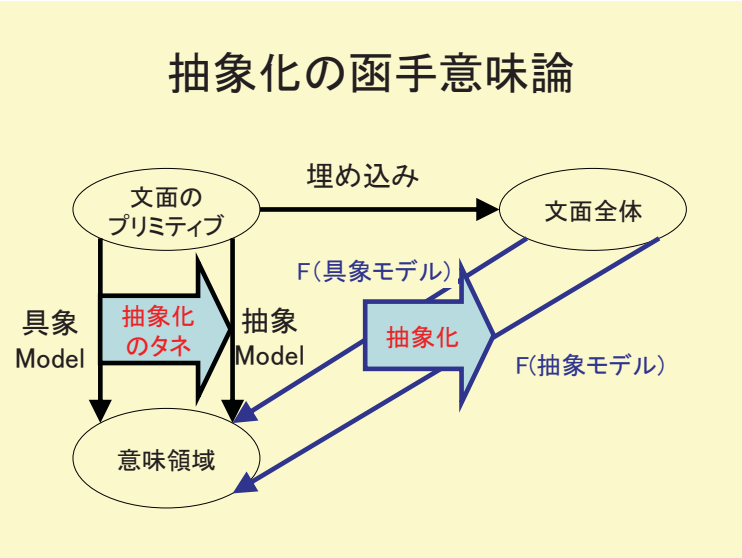
（産業技術総合研究所　システム検証研究センター　数理モデルグループ　）

(1)研究実施内容及び成果

Rμ

刺激応答系の抽象化シナリオを緩変換の枠組みによって実現することを目標に、様相μ計算の部分系Rμを構築して、そこでの抽象化シナリオの数理モデルを研究した。

抽象化の定式化のために、本研究では、代数構造の概念を用いたアプローチをとっている。 刺激応答系のモデル検査のための論理として、最も強い記述力を持つのは命題様相μ計算である。 これを函手意味論で扱うには、古典命題論理でのブール代数のような、命題様相μ計算のモデルがもつ代数構造を確定する必要がある。 しかし、不動点演算子が集合論的な問題を引き起こす（自由代数が存在しない）ため、集合の上の代数構造で、様相μ計算に対応するものはないことが知られている。 そこで、様相μ計算の部分系 Rμ でそのような問題を起こさないようなものを構築し、Rμ および Rμ における抽象化過程の数理モデルを、Lawvere A-理論[21]を用いて与え、解釈の定義、健全性定理と完全性定理、抽象化の定義、論理式保存の定理などの間の関係を函手意味論の常套手段を用いて記述した[28,36]。 Rμ は様相μ計算の部分系ではあるが、刺激応答系の性質記述に広く用いられる CTL を部分系として含み、刺激応答系の仕様記述言語としても十分実用に耐える記述力を持っている。 このRμの理論は研究代表者らによる抽象化の函手意味論を刺激応答系に具体化したものと考えることができる。



ところで抽象化の数理的定式化として Cousot らによる抽象解釈の概念が有名である。研究代表者らの函手意味論は抽象解釈を特別の場合として含むものであるが、まず、抽象解釈に必要な圏論的構成を明確にした。 抽象解釈におけるガロア接続の構成が,「冪集合が自由完備上半束であること」にもとづく自由生成と Kan extension に基づいていることが明らかになった[57]。 また, よく知られている「与えられた遷移系を模倣する遷移系は ACTL 式を保存する」という事実も, 同じ枠組みで理解されることが明らかになった。

FOM μ

刺激応答システムの検証には現在、命題様相 μ 計算およびその部分系が用いられることが殆どである。 モデル検査のような自動検証法を適用する立場からは、命題論理の範囲にとどまることが重要であるが、定理証明支援系による検証法の立場からは、命題論理の範囲にとどまる必要はなく、むしろ量化記号(quantifier)がないための記述力の低さが注目される。 そこで、命題様相 μ 計算の一階拡張に取り組んだ。 まず、刺激応答システムの論理体系として様相 μ 計算の自然な拡張である一階様相 μ 計算 FOM μ を提示した[30,79,83]。 命題様相 μ 計算の一階拡張にはいろいろのやり方、程度があるが、我々は最も保守的なやり方をえらび、不動点をとるときの述語変数には、引数が 0 個のもの(命題変数)だけを許すことにした。 この体系について健全性を示したが、通常のモデルの定

義では論理的公理が帰納的枚挙不能になり、完全性が決して得られないことも同時に判明した。 そこで高階論理における Henkin モデル(generalised model)に準ずる方法でモデルの定義を変更し、この定義のもとでの完全性を示した[20]。

また、体系 FOMμ による記述実験も行い、次のような命題様相μ計算では記述できないような仕様記述を示した。 (1)実行途中にプロセスの個数が増減し、不定個数のプロセスが走る環境での相互排除問題[85]。 (2)刺激応答システムのデッドロック発生可能性の条件(Coffman 条件)の検証[31]。

以上の結果により、論理 FOMμ は確立されたと考えられるが、代数的モデル、圏論的モデルをあたえることが課題として残っている。

多値モデル検査の意味論

Rμ の手法を用いて多値モデル検査における抽象化の研究を行った。 辰巳と亀山による、ドモルガン代数を真偽値とする多値モデル検査を利用したモデル化の誤りを発見手法に関する先行研究の上にたち、真偽値の構造や模倣関係の条件に関する詳細な考察を行なった。 具体的には、完備ハイティング代数(cHa)を真偽値とする多値モデルと、その間の模倣関係を定式化し、cHa を真偽値の全体とする様相μ計算の状態意味論と経路意味論を与え、多値模倣関係がこれらの論理のモデル検査に対して健全な抽象化になることを証明した[35,80]。 この際、2値の場合では模倣関係は状態意味論でも経路意味論でも健全な抽象化になるにもかかわらず、cHa の場合に経路意味論に関して健全な抽象化にならない例があることを発見し、さらに、経路意味論に関しても健全な抽象化になるために、真偽値の cHa が満たすべき十分条件も与えた。

この成果は、多値モデルの抽象化を一般的に扱うための基礎理論と位置づけられる。ドモルガン代数、ファジー論理、確率モデル、などを用いた多値モデルに関する類似研究との比較は今後の課題である。 なお、この研究の一部の西澤弘毅による口頭発表[80]が、平成 19 年ソフトウェア科学会高橋奨励賞を受賞した。

(2)研究成果の今後期待される効果

近い将来、後述する MLAT と同様の抽象化ツールが作られると見られるが、抽象化は複数のモデルが交錯する数理現象であるため、抽象化自体の数理的モデルが確立されないことには、抽象化の正当性を明確に示すことは困難であった。 抽象化による検証のアプローチは、抽象化という操作の正当性を前提として巨大システムの正当性を示そうとするものであるから、抽象化の正当性は、本質的に重要である。 本項目のうち、Rμの研究は、抽象化の数理的モデルを、刺激応答システムに関して与えて、そこでの抽象化の正当性を定式化するものであり、大規模システムの検証における記述量爆発問題への、抽象化によるアプローチの正当性の根拠を与えた。 文献[88]は、MLAT の正当性を、Rμの意味論を用いて示したものであり、これと同様にして、いろいろな抽象化ツールの正当性を定式化し、示すことができる。

また、Rμ研究の一般性のおかげで、この枠組で多値モデル検査の意味論とその解析をすすめることができた。 多値モデル検査によって、差分の少ないモデルに関するモデル検査を一度に行なう可能性が既に示唆されている。 また、多値モデル検査は、確率モデル検査や重み付モデル検査など、用途にあったモデル検査の発展をうながすものと期待される。

最後に、われわれが与えた多値モデルに関する抽象化の定式化に従って、多値モデル検査のアルゴリズムや抽象化のアルゴリズムが与えられ、効率的なモデル検査が可能になることや、モデル化の誤りが発見できるようになることが期待される。 これにより、モデル検査が専門家の間だけでなく、企業の技術者を含む、より広い利用者の間に広まることが期待される。

3．2抽象化支援ソフトウェアの方式開発と試作
（産業技術総合研究所 システム検証研究センター 支援ソフトウェア開発グループ ）

(1)研究実施内容及び成果

抽象化支援ツール MLAT

まず「既存抽象化算法の調査」の題目で抽象化支援系技術の動向を、自動化の観点から調査することからはじめた。 抽象解釈、データマッピング、述語抽象など、支援系作成の分野において広く知られている抽象化の技法を調べるとともに、既存もしくは開発中の抽象化を利用している検証ツール、SLAM、BLAST、Bandera、JPF、ESC/Java、FeaVer、SPIN、STeP、PAX の九つの検証系における抽象化技術を調べた[2,5,54,56]。 この調査結果をまとめた解説論文[5]は、抽象化についてのまとまった邦文文献がなかったこともあって、国内で広く読まれ、平成 19 年日本ソフトウェア学会解説論文賞も受賞した。

いっぽう、既存抽象化算法の調査によって、既存の抽象化は数値データを扱うものがほとんどであり、ポインタ構造の抽象化についての先行研究が殆どないことがわかった。 そこで、高橋-萩谷による並列ゴミ集めの抽象化算法を一般のポインタ処理システムに適用できるよう、一般化を試みることとし、ポインタ処理システムの抽象化算法の研究を平成 15 年度より開始した。 我々は、ポインタシステムの性質を時相論理で記述して検証するアプローチを開拓したが、そのために必要な時相論理(2CTL、2CTLN および alternation free μ calculus)を次々に定式化し、おのおのでの論理式の充足可能性判定算法を考案し、これに基づいた充足可能性判定器を試作していった[8,9,12,14,70]。 また、ポインタシステムの本質を抽出した算譜言語 PML (Pointer Manipulation Language) を設定[72]、その性質を時相論理式で記述し、これに関して述語抽象化を行う支援ツール MLAT (Modal Logic Abstraction Tool) を試作した[34,73,74,84,87]。 支援ツールの試用によって、システムの記述のために時相論理により大きな記述力が必要なことがわかり、時相論理の定式化からやりなおす、という作業を繰り返した。

MLAT は PML の抽象化を自動的に行うシステムである。PML のプログラムの状態は、ポインタで指されるセルの集まり(ヒープ)である。 若干設定を単純化してセルの内容は他のセルを指すポインタだけだとすると、ヒープは、セルの集合 X とその上の二項関係 R によって表現することができる。 x R y のときに、セル x の内容が y を指していると考えるのである。(X,R) がつくる Kripke 構造の性質を様相論理によって記述することとした。 R(ポイン

タが「指す」関係)と共にその逆関係 R° (ポインタに「指される」関係)を考える様相論理 2CTL (2 way CTL) をまず定義し、その基本的な性質と充足可能性判定算法を考察した。しかし、後に述べるDSWマーキング算法の仕様記述には2CTLでは記述力が不足することがわかり、CTLの部分を一般の命題様相μ計算で置き換えたalternation free μ計算を設定し、この計算に関する充足可能性判定算法などをすべて考察しなおし、かつ MLATの実装にも変更を加えた。

ヒープを操作するプログラムは、状態をヒープとする遷移系である。 したがって、我々の体系には、様相が二つある。「ポインタで指す」ことの様相と「プログラムの1ステップの実行」の様相である。 このような枠組に、述語抽象化の技法を適用した。

抽象化のアルゴリズムがEXPTIME完全なので、「よくある場合について、実用に耐える応答性能を得る」ことが本研究において重要であった。 高速化の尺度が必要なので、DSW (Deutch-Schorr-Waitマーキング算法)をMLATによって行なうことを目的にtune upを行なった。 到達不能な状態に関する遷移関係の計算を省き、計算途中に到達可能性を判定していく、事後条件の計算もとりいれて状態数を減らす、などの実装上の工夫を凝らした。

DSW 算法検証への適用、という目標は、高速化のみならず、仕様の記述力強化も導いた。既に述べたように、状態記述のための論理を2CTLNからalternation-free μ計算に拡張したのはこの目的のためであった。 例えばalternation-free μ計算の論理式

$\mu X[p \vee \langle l \rangle(\neg s \wedge X) \vee \langle r \rangle(s \wedge X)]$

は2CTLNでは記述できないが、DSWの検証に必要である。

Agda-IVEにMLATを組込んだ。 MLATの一部であるpfvalid(Hoare tripleの恒真性判定器)を Agda から呼べるようにし、さらに Agda 上に PML の Hoare 論理を定義した。Agda-IVEによってPMLの基本命令やその列に関するHoare式を自動証明することができるようになった[81]。 この機能の有効性を調べるためAgda-IVEによってポインタ操作プログラムの検証実験を行い、さらにDSW算法の正当性検証を行い、本手法で中規模の検

証が可能であることを実証した[88]。

ポインタを扱うプログラムの検証は重要だが、非常に困難であり、このテーマの歴史は古い。 最近では John Reynolds による separation logic が有名である。 Separation logic と MLAT によるアプローチとの違いは、まだ詳細に検討できていないが、記述のしやすさに関しては、局所的な性質の記述では separation logic による記述が優る一方、shape analysis などの大域的性質では、MLAT によるアプローチが優るように思われる。

(2)研究成果の今後期待される効果

本項目で開発した MLAT によって、ポインタ処理に関する形式的検証をおこなえるようになった。 一般にポインタ処理は、バグが発生しやすい上、テストもコードレビューなどの伝統的検証法もあまり効果を発揮しないので、MLAT の意義は大きい。 MLAT を利用するには、現在のところ特別なノウハウが必要で、誰でもこのツールを使えるという状態ではないものの、言語処理系や OS など、利用頻度の高いソフトウェアの正当性検証に MLAT を用いてシステムの信頼性の飛躍的な向上に貢献することができる。 たとえば、Lisp や Haskell をはじめとする函数型プログラミング言語や Java など、動的なメモリ管理を必要とするプログラミング言語が主流になりつつあるが、これらの言語処理系の、メモリ管理の正当性を Agda-IVE をとおした MLAT によって検証することにより、これらの言語でかかれたプログラムすべての動作の信頼性を上げることができる。 実際、ある Lisp 処理系の開発グループからの興味を呼び、MLAT を用いて彼らの処理系のごみ集め算法の正当性検証を行なうプロジェクトを、本計画のあとに始めつつある。

3．3 抽象化シナリオ摘要のための統合検証環境の構築
（産業技術総合研究所 システム検証研究センター 定理証明グループ ）

(1)研究実施内容及び成果

統合検証環境 Agda-IVE

第三年次から設けた定理証明研究グループでは、さまざまな検証方式を適材適所に適用し結果を統合するための統合検証環境 Agda-IVE (Agda Integrated Verification Environment) の研究開発を行なった[4,6,65,66,70,81]。 Agda-IVE は、Martin-Löf 型理論に基づく対話型証明支援系 Agda の上に構成したもので、モデル検査器 SMV、一階述語論理自動証明器 Gandalf や本計画で研究開発した抽象化支援系 MLAT などを Agda から呼び出し、これらの自動検証器による検証の結果を再び Agda に取り込んで検証を続ける、という検証スタイルを支援するものである。 Agda と諸自動検証器は、(1) 自動検証器が支援する論理の Agda 上の実装と、(2) Agda からの自動検証器への呼び出しを自動化するプラグイン機構によって接続される。

統合検証環境によって、さまざまな検証問題の記述、小問題への論理的分解、各種自動ツール呼び出し等を、共通の記述言語とユーザーインターフェースによって行なえる。 その過程の整合性が保証される形で半自動化されるため、各種ツールを手動で組み合わせるのに比べて、より確実で、より便利である。

Martin-Löf-型理論は、論理とプログラミングを統一する基礎理論である。 論理式に対する証明の構成と、プログラム仕様 (型) に対するプログラムの構成とは同一の原理で基礎付けられるという、Curry-Howard 同型の考えに基づく。 型理論は、証明をプログラムとして書ける汎用プログラミング言語の理論と言える。 論理としては直観主義高階論理を含む。システム検証の基盤として型理論が優れているのは、システムのモデルとなるプログラム、検証したい性質を表す論理式、モデルが性質を満たすことの証明をひとつの体系で扱えるためである。

対話型証明支援系 Agda は、型理論でのプログラミング[32,77]と証明の構成を支援するソフトウェアシステムである。 スウェーデンの Chalmers 工科大学で 1997 年ごろに開発が始められ、2004 年からは CVS も開発に加わっている。 一般のプログラム開発における統合開発環境ないし構造エディタと同様の役割を果たす。 最も基本的な機能は、与えられたプログラムが与えられた型に対して正しいか、証明が論理式に対して正しいか、を機械的

に検査する型検査である。 編集途中で未完成の部分が残るプログラムに対しても、完成部分の整合性を型検査できる。 編集の各ステップでこれを行うため、プログラムが完成できれば、その型に対する正しさが保証されていることになる。 編集に関する支援には、未完成部分の型から次に取り得る正しいステップの候補を示す、候補がひとつの場合は自動的に適用する、漏れのない場合分けを生成する、などがある。 型情報を用いることで、文法のみしか考慮しない構造エディタより高度な支援がなされる。

Agda-IVE の中核は、外部の自動検証器を Agda から呼び出す plug-in の一般機構である[71]。 この plug-in 機構を用いて SMV や FOL（Gandalf)、それに我々が試作した抽象化支援ツール MLAT などのシステムを Agda から呼び出せるようにし、対話型検証と自動検証を局面に応じて使い分けることを可能にした。

本題目では、Agda-IVE の試作に並行して、様相 μ 計算の Agda 上での実装 μ NK を試作し、これを用いて抽象化シナリオの雛形となる形式化実験を行った。 プログラムの無限状態具体解釈と有限状態抽象解釈を定理証明で結び、後者を SMV で検証した。

また依存レコード型とサブタイピングおよび超変数をもつ入力言語を対象とした型検査器 Mendori を実装して Agda の拡張改良にむけた実験をおこない、これで得られた知見を活かして次世代言語の核を設計した。

さらに、Agda 言語を入出力等の機能と実用的な速度をもつ依存型付作譜言語として用いることを可能にするべく、Agda を Haskell に翻訳するコンパイラ Agate を試作した。 Agate によるオーバヘッドは数十％程度であり、依存型を用いた作譜実験を十分に可能とする環境を提供することができた。 さらに Agate への Haskell 関数の埋め込みを一般的に行う機能拡張を施し、また翻訳で生じる無駄なコードを取り除く最適化機能をもつ第二版を公開した。 ライブラリ強化に向けた依存型プログラミングの実験も進め、構文解析組合せ子ライブラリなどを提供することができた。

なお、Agda-IVE の普及のため、手引などのドキュメントを整備する一方で、公式ホームページ http://unit.aist.go.jp/cvs/Agda/ を新設し、one-click installer などを提供して配布

体制を強化した。

構成的型理論や高階論理などに基づく証明支援系の研究は 1980 年代に始まり、現在では Agda をふくめて多数の実験システムが構築され、一部は、銀行オンラインシステムの検証などの実用に供されている。 しかしながら、証明支援系を他のシステムの作業台(workbench)として用いる発想は、一部に萌芽がみられたものの、Agda-IVE が初めてこの発想を明確にし、実装してみせた。

いっぽう、Agda-IVE 開発の副作用として作成した Agda 言語のコンパイラ Agate は、それ自身、依存型を用いた函数型プログラミングのスタイルを promote するものである。 依存型プログラミングのための処理系は、過去にも存在し、現在も項の値の評価器の形で与えられているものがあるが、入出力機構を備え、本格的なプログラミングを可能にするのは Agate が初めてである。

(2)研究成果の今後期待される効果

モデル検査などの自動検証システムは、自動とはいうものの、状態爆発などの記述量爆発を起こさないよう、trial and error で検証対象となるシステムの記述を調整する必要がある。 この記述調整のための手法の一つが、抽象化であるが、他にも slicing など、いろいろな形の調整がありうる。 Agda-IVE は、記述調整の支援を Agda によって行なう道を拓くものである。 その結果、自動検証システムの利用範囲を拡大し、情報処理システムの信頼性向上に寄与することができる。

いっぽう Agda 言語をプログラミング言語として扱ってコンパイルする Agate は、依存型プログラミングという新しいプログラミングスタイルの実験環境を用意しており、プログラムの整合性の強力な静的検査を備えたプログラミング言語構築の可能性を示唆している。

3．4 スレッドとポインタを扱うプログラムの自動検証システムの研究開発
（産業技術総合研究所　システム検証研究センター　並行プログラム検証研究グループ ）

(1)研究実施内容及び成果

Agda-IVE の実問題への適用

Agda-IVE を用いた検証の適用可能性を調べるため、計画の最後の一年半を用いて、実問題への適用を試みた。

実問題として MPI (Message Passing Interface)の石川裕らによる実装である YAMPII の検証をとりあげることにした。 このシステムを取り上げた理由は、メッセージ交換は刺激応答型システムの例になっていること、ポインタ処理が含まれていそうなことなどもさることながら、開発者のグループが検証実験に極めて協力的であったことも影響が大きい。

はじめの半年程度を用いて、YAMPII ソースコードの排他制御の正当性の完全自動検証機能を、既存のモデル検査器などのツールを組み合わせて提供する可能性を探った[86]。これは MPI 開発者グループにとってもっとも望ましい支援ツールであったが、半年にわたる調査の結果、完全自動検証機能の提供は短期間では困難という結論に達した。 そこで、Agda-IVE を用いた、半自動検証を行うこととした。

YAMPII は、通常の通信システムと同じく、いくつかの層に分けてメッセージを処理する。最上位層の API 層は、仕様で定められた関数名を提供する。 その関数名はたいてい、SENDRECV 層への転送関数である。 SENDRECV 層では、引数の内容に応じて要求オブジェクトが発行され、REQUEST 層が管理する待ち行列に投函される。 通信の処理は、REQUEST 層が提供するポーリング関数を繰り返し呼ばれることによって進行する。REQUEST 層のポーリング関数から P2P 層のポーリング関数が呼ばれ、あとはそれぞれの通信手段に依存する定められた方法で通信がすすむ。

YAMPII のような巨大なシステムを限られた期間とマンパワーで検証する場合には、システム全体の完全な検証は不可能であるから、検証項目に優先順位をつける必要がある。優先順位は、いろいろな価値観で決定されうるが、今回は、開発者にとって、もっともバグが出やすそうに思われるのはシステムのどの部分のどんな性質に関してか、ということを聞

き取りで調査した。 開発の途中で過去に実際に生じたバグと同じパターンの検証項目も重視した。 その結果、YAMPII が通信要求を管理するときに使う待ち行列が正しく実装され、かつ正しく使われていることの検証を行なうことにした。 ポインタ操作と微妙な割り込みが絡むため、バグが入る可能性が他の部分よりも大きそうだったからである。

```
issued.val := FALSE
insert(sQ,req)
req.val := SENDING
while (req.val != DONE)
  if (*) if (issued.val == FALSE)
             issued.val := TRUE
              req.val := CANCEL
  if (*) if (e1 <- sQ.top)
              remove(sQ,e1)
              if (e1.val == CANCEL)
                    insert(cQ,e1)
                    e1.val := WAIT
              else e1.val := DONE
  if (*) if (e2 <- choose(cQ))
              remove(cQ,e2)
              e2.val := DONE
```

- insert/remove/choose は別途定義された関数
- if (*) *B* は *B* の非決定的実行
- sQ (sendQueue): 送信要求の待ち行列
- cQ (cancelQueue): キャンセル応答の待ち行列

図 1 検証対象 PML プログラム

そこで、図 1 に記すようなプログラムに関して、Agda-IVE による検証を行なった。

この遷移系に関して、「q ではじまる二重リストが良形(well-formed)である」が while 文の不変条件(invariant)であることを、Agda-IVE を用いて検証した。 二重リストが良形であることを記す論理式は、命題論理の表現力に限界があるために、非常に長くなった(二十以上のリテラルの連言)が、2 名で 3.5 ヶ月程度かけて記述することができ、これを 5 名で約 1 ヶ月かけて検証することができた。 検証そのものよりも、その前段階である、検証すべき部分をうまく切り出して適当な検証項目を設定する作業に、より多くの手間がかかっていることに注意すべきである。 また、この前段階では、不変式を発見するために試行錯誤するが、この作業のために、Agda-IVE の対話環境と MLAT の最弱事前条件計算器が極めて有効に働いた。

(2)研究成果の今後期待される効果

本項目によって、統合検証環境 Agda-IVE を用いた検証手法が確立し、そのフィージビリティを確かめることができた。 今後、Agda-IVE の適用実験をさらに何度か行い、改良をすすめることによって、大規模システムに対して、妥当な形で形式的検証法を適用するこ

とが可能になる。

4 研究参加者

(1)「数理モデル研究」グループ(リアクティブシステムおよび実時間システムの検証における抽象化の数理モデルの構築と形式化の研究)

氏名	所属	役職	研究項目	参加時期
木下 佳樹	(独)産業技術総合研究所 システム検証研究センター	研究センター長	検証における抽象化の数理モデルの構築	H14.11～H19.3
渡邊 宏	(独)産業技術総合研究所 システム検証研究センター	研究員	検証における抽象化の数理モデルの構築	H14.11～H19.3
古澤 仁	鹿児島大学 理学部 数理情報科学科	准教授	検証における抽象化の数理モデルの構築	H14.11～H19.3
武山 誠	(独)産業技術総合研究所 システム検証研究センター	招聘研究員	検証における抽象化の数理モデルの構築	H15.9～H19.3
中原 早生	(独)産業技術総合研究所 システム検証研究センター	研究チーム長	検証における抽象化の数理モデルの構築	H16.4～H19.3
竹内 泉	(独)産業技術総合研究所 システム検証研究センター	研究チーム長	検証における抽象化の数理モデルの構築	H16.8～H19.3
清野 貴博	(独)産業技術総合研究所 システム検証研究センター	産総研特別研究員	検証における抽象化の数理モデルの構築	H17.10～H18.3
高村 博紀	(独)産業技術総合研究所 システム検証研究センター	産総研特別研究員	検証における抽象化の数理モデルの構築	H17.4～H18.12
西澤 弘毅	東北大学大学院情報科学 研究科 情報基礎科学専攻	研究員	検証における抽象化の数理モデルの構築	H15.4～H19.3
佐藤憲太郎	(独)産業技術総合研究所 システム検証研究センター	テクニカルスタッフ	検証における抽象化の数理モデルの構築	H16.4～H17.1
岡本 圭史	(独)産業技術総合研究所 システム検証研究センター	テクニカルスタッフ	検証における抽象化の数理モデルの構築	H18.4～H19.3
高井 利憲	(独)産業技術総合研究所 システム検証研究センター	研究チーム長	検証における抽象化の数理モデルの構築	H17.6～H19.3
齊藤 紀子	(独)産業技術総合研究所 システム検証研究センター	CREST 技術員	検証における抽象化の数理モデルの構築	H14.12～H16.6
冨松美知子	(独)産業技術総合研究所 システム検証研究センター	テクニカルスタッフ	CREST 事務	H16.7～H19.3

(2)「支援ソフトウェア研究開発」グループ(抽象化支援ソフトウェアの方式開発と試作の研究)

氏名	所属	役職	研究項目	参加時期
高橋 孝一	(独)産業技術総合研究所 システム検証研究センター	副研究センター長	抽象化ソフトウェアの方式と試作	H14.11～H20.3
大崎 人士	(独)産業技術総合研究所 システム検証研究センター	主任研究員	抽象化ソフトウェアの方式と試作	H16.1～H20.3
田辺 良則	(独)産業技術総合研究所 システム検証研究センター	招聘研究員	抽象化ソフトウェアの方式と試作	H15.2～H20.3
高井 利憲	(独)産業技術総合研究所 システム検証研究センター	研究チーム長	抽象化ソフトウェアの方式と試作	H15.4～H17.5
関澤 俊弦	(独)産業技術総合研究所 システム検証研究センター	テクニカルスタッフ	抽象化ソフトウェアの方式と試作	H16.4～H20.3
湯浅 能史	東京工業大学 大学院情報理工学研究科	特任 准教授	抽象化ソフトウェアの方式と試作	H17.4～H20.3

(3)「定理証明研究」グループ(①抽象化シナリオ摘要のための統合検証環境の構築②多値クリプキ構造に基づく意味論と抽象化の研究)

氏名	所属	役職	研究項目	参加時期
武山　誠	(独)産業技術総合研究所 システム検証研究センター	招聘研究員	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H15.9～H19.11
永山　操	(独)産業技術総合研究所 システム検証研究センター	CREST研究員	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H15.2～H18.3
池上　大介	(独)産業技術総合研究所 システム検証研究センター	研究員	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H15.4～H20.3
Jeffrey Brian Polakow	(独)産業技術総合研究所 システム検証研究センター	招聘研究員	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H16.11～H17.10
尾崎　弘幸	(独)産業技術総合研究所 システム検証研究センター	研究員	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H16.11～H20.3
西原　秀明	(独)産業技術総合研究所 システム検証研究センター	研究員	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H15.4～H16.10 H18.4～H20.3
加藤　紀夫	(独)産業技術総合研究所 システム検証研究センター	産総研特別研究員	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H17.4～H20.3
清野　貴博	(独)産業技術総合研究所 情報技術研究部門 知的コンテンツグループ	産総研特別研究員	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H18.4～H20.3
山下　伸夫	(独)産業技術総合研究所 システム検証研究センター	テクニカルスタッフ	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H18.4～H19.9
湯浅　能史	東京工業大学 大学院情報理工学研究科	特任准教授	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H19.4～H20.3
齋藤　正也	(独)産業技術総合研究所 システム検証研究センター	産総研特別研究員	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H19.4～H19.11
水口　大知	(独)産業技術総合研究所 システム検証研究センター	研究員	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H19.4～H20.3
木下　佳樹	(独)産業技術総合研究所 システム検証研究センター	研究センター長	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H19.4～H20.3
渡邊　宏	(独)産業技術総合研究所 システム検証研究センター	研究チーム長	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H19.4～H20.3
古澤　仁	鹿児島大学 理学部 数理情報科学科	准教授	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H19.4～H20.3
中原　早生	(独)産業技術総合研究所 システム検証研究センター	研究チーム長	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H19.4～H20.3

竹内　泉	(独)産業技術総合研究所 システム検証研究センター	研究チーム長	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H19.4～H20.3
西澤　弘毅	東北大学大学院情報科学研究科 情報基礎科学専攻	研究員	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H19.4～H20.3
岡本　圭史	(独)産業技術総合研究所 システム検証研究センター	テクニカルスタッフ	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H19.4～H19.11
高井　利憲	(独)産業技術総合研究所 システム検証研究センター	研究チーム長	構成的型理論に基づいたリアクティブシステムの検証と抽象化	H19.4～H20.3
亀山　幸義	筑波大学大学院 システム情報工学研究科	准教授	多値クリプキ構造に基づく意味論と抽象化の研究	H19.4～H20.3
冨松　美知子	(独)産業技術総合研究所 システム検証研究センター	テクニカルスタッフ	CREST 事務	H19.4～H20.3

(4)「並行プログラム検証研究」グループ(スレッドとポインタを扱うプログラムの自動検証システムの研究開発の研究)

氏名	所属	役職	研究項目	参加時期
山形　頼之	(独)産業技術総合研究所 システム検証研究センター	研究員	スレッドとポインタを扱うプログラムの自動検証システムの研究開発	H18.4～H19.3
齋藤　正也	(独)産業技術総合研究所 システム検証研究センター	研究員	スレッドとポインタを扱うプログラムの自動検証システムの研究開発	H18.4～H19.3
水口　大知	(独)産業技術総合研究所 システム検証研究センター	研究員	スレッドとポインタを扱うプログラムの自動検証システムの研究開発	H18.4～H19.3

5　招聘した研究者等

氏　名(所属、役職)	招聘の目的	滞在先	滞在期間
Wolfram Kahl MacMaster University	Workshop での講演 “Compositional Syntax and Semantics of Tables”	兵庫県尼崎市	2004.4.12 ～4.23
John Hughes Chalmers University	Workshop “Types for Verification” での講演	兵庫県尼崎市	2004.5.5 ～ 5.14
Peter Dybjer Chalmers University	Workshop “Types for Verification” での講演	兵庫県尼崎市	2004.5.5 ～ 5.14
Anthony　John Power Edinburgh University Laboratory for the Foundation of Computer Science Senior Research Fellow	抽象化の函手意味論に用いる台数構造論(enriched category の代数構造)に関する議論。 また、刺激応答系の余代数意味論に関する議論。今後の研究交流体制についての打合せ。	大阪府豊中市	2005.11.20 ～12.22
Mooly (Shmuel) Sagiv Professor, University of Tel Aviv	シェープ解析に関する研究討論。招聘を機に、CLC での講演も依頼。	大阪府豊中市	2006.4.2 ～ 4.9

Anthony John Power Research Fellow, Dept of Computer Science, University of Edinburgh	情報処理システムの精製法や抽象化の数理モデルの圏論を用いた研究を行う。	大阪府豊中市	2006.11.19 ～12.28
Bengt Nordstroem Professor, Chalmers University of Technology	Agda2 の型理論を紹介する講義を依頼。型理論一般の講義を周辺分野の研究者向けに行う。	大阪府豊中市	2007.1.26 ～3.7
Michael Winter; Associate professor, Dpt. of Computer Science, Brock University	CLC 講師（演題：Ordered Categories of Processes）	大阪府豊中市	2007.5.31 ～6.2

6 成果発表等

(1)原著論文発表 （国内誌 7 件、国際誌 16 件）

[1] Masami Hagiya, Koichi Takahashi, Mitsuharu Yamamoto, and Takahiro Sato, Analysis of Synchronous and Asynchronous Cellular Automata using Abstraction by Temporal Logic, Proceeding of International Symposium on Functional and Logic Programming (FLOPS2004), LNCS2998, 2004.

[2] Toshinori Takai, A Verification Technique Using Term Rewriting Systems and Abstract Interpretation, LNCS, Rewriting Techniques and Applications, Vol.3091, pp.119-133, 2004. (Draft: Toshinori Takai. A Verification Technique Using Term Rewriting Systems and Abstract Interpretation, Programming Science Technical Report, AIST, PS-2004-006, 2004.)

[3] Hitoshi Furusawa, A free construction of Kleene algebras with tests, Proceedings of Seventh International Conference on Mathematics of Program Construction, 12-14 July, 2004, Stirling, Scotland, UK, in a volume of Springer-Verlag Lecture Notes in Computer Science, Vol. 3125, pp.129-141, 2004.

[4] Peter Dybjer, Qiao Haiyan, Makoto Takeyama, Verifying Haskell Programs by Combining Testing, Model Checking and Interactive Theorem Proving, INFORMATION AND SOFTWARE TECHNOLOGY, Vol.46, No.15, pp.1011-1025, 2004.

[5] 田辺 良則, 高井 利憲, 高橋 孝一, 抽象化を用いた検証ツール, コンピュータソフトウェア, Vol. 22, No. 1, pp. 2-44, 2005. (草稿:田辺良則,高井利憲,高橋孝一, 抽象化を用いた検証ツールの調査, 産業技術総合研究所算譜科学グループ研究速報, AIST, PS-2003-007, 2003.)

[6] Peter Dybjer, Qiao Haiyan and Makoto Takeyama, Rondom Generators for Dependent Types, Theoretical Aspects of Computing - ICTAC 2004, Revised Selected Papers, Lecture Notes in Computer Science, vol. 3407, pp 341—355, 2005.

[7] Hitoshi Osaki, Toshinori Takai, ACTAS: A System Design for Associative and Commutative Tree Automata Theory, ENTCS, Vol. 124, pp. 97-111, 2005.

[8] Yoshinori Tanabe, Toshinori Takai, Toshifusa Sekizawa and Koichi Takahashi, Preconditions of properties described in CTL for statements manipulating pointers, Supplemental Volume of the 2005 International Conference on Dependable Systems and Networks, pp.228-234, 2005.

[9] 田辺良則, 高橋孝一, 山本光晴, 佐藤貴洋, 萩谷昌己, BDD を用いた 2 方向 CTL 論理式充足可能性決定手続きの実装, コンピュータソフトウェア, Vol.22 No.3, pp.154-166, 2005.

[10] 高木理, 武山誠, 渡邊宏, 対話型証明支援ツールPVSの紹介, コンピュータソフトウェ

ア, Vol. 22, No. 3, pp. 37-57, 2005.
[11] 高木理, 武山誠, 渡邊宏, Verification of Transition System Reduction via PVS, コンピュータソフトウェア, Vol. 22, No. 3, pp. 134-145, 2005.
[12] Yoshinori Tanabe, Koichi Takahashi, Mitsuharu Yamamoto, Akihiko Tozawa and Masami Hagiya, A Decision Procedure for the Alternation-Free Two-Way Modal μ-Calculus, LNAI, Automated Reasoning with Analytic Tableaux and Related Methods (TABLEAUX 2005), Vol. 3702, pp. 277-291, 2005.
[13] Koki Nishizawa, ″Algebraic Structures for Cocomplete Fibrations and Fibred CCCs″. In Peter Mosses, John Power, and Monika Seisenberger, editors, Selected Papers from the First Conference on Algebra and Coalgebra in Computer Science Young Researchers Workshop (CALCO-jnr 2005), University of Wales Swansea Computer Science Report Series CSR 18-2005, pp. 55-69, 2005.
[14] 関澤俊弦, 高井利憲, 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論理式生成法, 電子情報通信学会論文誌 D-I, J89-D 巻 4 号 642 頁～650 頁, 2006.
[15] Toshinori Takai, Hitoshi Furusawa, Monodic tree Kleene algebra, Proceedings of 4th International Workshop on Kleene Algebra, Lecture Note in Computer Science, Vol. 4136, PP. 402-416, 2006.
[16] Hiroki Takamura, The variety of modal FLew-algebras is generated by its finite simple members, Advances in Modal Logic vol.6, pp 469-479, College Publications, 2006.
[17] 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, コンピュータソフトウェア, Vol.23, No.3, pp.147-157, 2006.
[18] Martin Hyland, Misao Nagayama, John Power and Giuseppe Rosolini, A category Theoretic Formulation for Engeler-style Models of the Untyped A-Calculus, Proceedings of the Third Irish Conference on the Mathematical Foundations of Computer Science and Information Technology (MFCSIT 2004), Vol. 161, pp. 43-57, Dublin, Ireland, 2006.
[19] Hiroshi Watanabe, Koki Nishizawa and Osamu Takaki, ″A Coalgebraic Representation of Reduction by Cone of Influence″, Electronic Notes in Theoretical Computer Science, Volume 164, Issue 1, 20 October 2006, Pages 177-194, Proceedings of the Eighth Workshop on Coalgebraic Methods in Computer Science (CMCS 2006), (Draft: Programming Science Technical Report, AIST, PS-2006-002, 2006)
[20] Ryo Kashima and Keishi Okamoto, General Models and Completeness of First-Order Modal μ calculus, Accepted by Journal of Logic and Computation, 2007.
[21] Koki Nishizawa and John Power, ″Lawvere Theories Enriched over a General Base″, To appear in Journal of Pure and Applied Algebra, Elsevier. (Draft: Programming Science Technical Report, AIST, PS-2005-005, 2005.) 2007.
[22] Toshifusa Sekizawa, Tatsuhiro Tsuchiya, Tohru Kikuno, and Koichi Takahashi, Analyzing the One Dimensional Ising Model by Probabilistic Model Checking Proceedings of the IASTED Asian Conference on Modelling and Simulation (AsiaMS 2007), pp.199-204, 2007.
[23] Toshifusa Sekizawa, Yoshinori Tanabe, Yoshifumi Yuasa, and Koichi Takahashi: MLAT: A Tool for Heap Analysis Based on Predicate Abstraction by Modal Logic, Proceedings of the IASTED International Conference on Software Engineering (SE 2008), pp.310-317, 2008.

(2)その他の著作物

[24] 高橋孝一, モデル検査入門(チュートリアル), 第一回システム検証の科学技術シンポジウム予稿集, 3 頁～13 頁, 2004.

[25] 武山誠，型理論での定理証明（チュートリアル），第一回システム検証の科学技術シンポジウム予稿集，14 頁～15 頁，2004.
[26] Hitoshi Osaki, Toshinori Takai, ACTAS: A System Design for Associative and Commutative Tree AutomataSimulator, Programming Science Technical Report, AIST, PS-2004-007, 2004.
[27] 高木理，武山誠，渡邊宏，PVS の紹介，算譜科学研究速報，AIST，PS-2005-009，2005.
[28] Koki Nishizawa and Makoto Takeyama, “Algebraic Structure for a Fixed Point Logic and Abstract Interpretation”, Programming Science Technical Report, AIST, PS-2005-012, 2005.
[29] 高井利憲，古澤仁，クリーニ代数によるプログラム解析入門（チュートリアル），第三回システム検証の科学技術シンポジウム予稿集，29 頁～36 頁，2006.
[30] Keishi Okamoto, A First-Order Extension of Modal μ-calculus, Programming Science Technical Report, AIST, PS-2006-003, 2006.
[31] Yoshiki Kinoshita, Koki Nishizawa, and Keishi Okamoto, Formalising Coffman Conditions in First Order Modal μ - Calculus, Programming Science Technical Report, AIST, PS-2006-010, 2006.
[32] Hiroyuki Ozaki, Makoto Takeyama, Yoshiki Kinoshita, Agate: an Agda-to-Haskell compiler, Programming Science Technical Report, AIST, PS-2006-011, 2006.
[33] Hiroki Takamura, Semisimplicity, EDPC and discriminator varieties of modal FLew-algebras (Preliminary Version), Programming Science Technical Report, AIST, PS-2007-002, 2007.
[34] Toshifusa Sekizawa, Yoshinori Tanabe, Yoshifumi Yuasa, and Koichi Takahashi, MLAT: Modal Logic Abstraction Tool, AIST, PS-2007-004, 2007.
[35] Koki Nishizawa, Yukiyoshi Kameyama and Yoshiki Kinoshita, Simulations of Multi-Valued Models for Modal mu-Calculus, Programming Science Technical Report, AIST, PS-2007-005, 2007.
[36] Koki Nishizawa, Algebraic Structure for a modal fixed point logic and abstract interpretation, Programming Science TechnicalReport, AIST, PS-2007-009, 2007.

(3)学会発表（国際学会発表及び主要な国内学会発表）

①招待講演（国内会議 8 件、国際会議 1 件）

[37] 木下佳樹，特集テーマ「さまざまな分野の形式的検証最前線」および一般；What’s going on at AIST/CVS，電子情報通信学会，2005.
[38] 木下佳樹，システム検証の総合環境，情報処理学会関西支部 支部大会，2005.
[39] 木下佳樹，リアクティブシステムの検証の基本，京都大学大学院情報学研究科，2005.
[40] 木下佳樹，2006 総合大会講演論文集，電子情報通信学会，パネル討論会，パネリスト，2006.
[41] 木下佳樹，数理的技法のフィールドワーク，TOPPERS カンファレス 2006，タワーホール船堀，2006.
[42] 木下佳樹，圏論の諸相，第 4 回プログラミングおよびプログラミング言語サマースクール（PPL Summer School 2006），東京大学本郷キャンパス，2006.
[43] 木下佳樹，形式手法最前線－拠点の活動とねらい，組込みシステムシンポジウム 2006(ESS2006 シンポジウム)パネリスト，独立行政法人科学技術振興機構 日本科学未来館，2006.

[44] 木下佳樹，組込みシステムの評価メトリック，JST 情報システムのディペンダビリティ評価に関するワークショップ， JST 研究開発戦略センター, 2006.
[45] 木下佳樹，Introducing CVS's Verification Research Projects，日仏ソフトウェア検証国際集会，The 2nd Franco-Japanese Computer Security Workshop, Tokyo，慶應義塾大学三田キャンパス, 2006.

② 口頭発表（国内会議 37 件、国際会議 9 件）

[46] 永山操，λ-Calculus, ludics and their applications. Preuves, Programmes et Systemes Seminaire，パリ第七大学, 2003.
[47] 池上大介，オートマトンを表現する非可換多項式環のグレブナ基底，Language and Automata シンポジウム，三重県 合歓の里屋内ホール, 2003.
[48] 池上大介，2元線形ブロック符号に対するグレブナ基底を用いた最尤復号法の計算量，電子情報通信学会 情報理論研究会，京都工芸繊維大学, 2003.
[49] 高井利憲，項書換え系と抽象解釈を用いた検証技法，日本数理科学協会年会 ALGI+Logic 分科会, 2003.
[50] 永山操，型なしラムダ計算のモデルについて，ALGI および論理数学合同分科会，大阪府立大学, 2003.
[51] 池上大介，Regular category の中の非決定性オートマトン，記号論理と情報科学研究集会（SLACS 2003），2003.
[52] 西原秀明，等式の対応関係について，記号論理と情報科学研究集会（SLACS），東京大学, 2003.
[53] 高井利憲，A Verification Technique Using Term Rewriting Systems and Abstract Interpretation，日本ソフトウェア科学会第20回記念大会, 2003.
[54] 田辺良則，高井利憲，高橋孝一，時相論理式を用いた抽象化法のツール化に向けて，第一回システム検証の科学技術シンポジウム，大阪, 2004.
[55] 高木理,武山誠,渡邊宏， Kripke 構造の模倣性に関する基本的性質および縮小化・抽象化に対する証明支援系による形式化，第一回システム検証の科学技術シンポジウム，大阪, 2004.
[56] 高井利憲，書換系と抽象解釈を用いた検証技法，第一回システム検証の科学技術シンポジウム，大阪, 2004.
[57] 西澤弘毅，抽象解釈にみられる圏論的構成について，第一回システム検証の科学技術シンポジウム，大阪, 2004.
[58] 池上大介，単項二階論理とオートマトン・様相 μ 計算，第一回システム検証の科学技術シンポジウム，大阪, 2004.
[59] Toshinori Takai, Hitoshi Osaki, ACTAS: Associative and Commutative Tree Automata Simulator, The International Conference on Application of Concurrency to System Design (ACSD2004), McMaster University, 2004.
[60] Toshinori Takai, Hitoshi Osaki, ACTAS: A System Design for Associative and Commutative Tree Automata Theory, RULE2004, Aachen (Germany), 2004.
[61] Hitoshi Furusawa, A free construction of Kleene algebras with tests, Seventh International Conference on Mathematics of Program Construction, Stirling, Scotland, UK, 2004.
[62] 大崎人士，システム検証の自動化とツリーオートマトン，東京工業大学，東京, 2004.
[63] 佐藤貴洋，田辺 良則，萩谷昌巳，BDD を用いたガード付きフラグメントの充足可能性判定，日本ソフトウェア科学会，東京, 2004.
[64] Peter Dybjer, Qiao Haiyan, and Makoto Takeyama, Rondom Generators for Dependent Types, First International Colloquium on THEORETICAL ASPECTS OF COMPUTING, Guiyang, China, 2004.

[65] 木下佳樹，高村博紀，型理論での形式的証明記述の技法について，日本ソフトウェア科学会第22回大会，東北大学, 2005.
[66] 木下佳樹，システム検証の科学研究とフィールドワーク，第二回システム検証の科学技術シンポジウム，大阪, 2005.
[67] Takeuchi Izumi, Kleene category as a model of calculation，第二回システム検証の科学技術シンポジウム，大阪, 2005.
[68] 田辺良則，高橋孝一，山本光晴，佐藤貴洋，戸沢晶彦，萩谷昌己，BDD による実装が可能な様相論理の充足可能性判定手続き，第 7 回プログラミングおよびプログラミング言語ワークショップ(PPL2005), 2005.
[69] Catarina Coquand, Dan Synek, and Makoto Takeyama, “An Emacs Interface for Type-Directed Support for Constructing Proofs and Programs”, User Interfaces for Theorem Provers (UITP 2005), Edinburgh (Scotland), 2005.
[70] 湯浅能史.田辺良則.関澤俊弦.高橋孝一，時相論理による述語抽象化のための充足可能性判定手続き，日本ソフトウェア科学会第 22 回大会，東北大学, 2005.
[71] 池上大介，対話型証明支援系 Agda のプラグイン機構，日本ソフトウェア科学会第 22 回大会，東北大学, 2005.
[72] Koichi Takahashi, Yoshinori Tanabe, Toshifusa Sekizawa, and Yoshifumi Yuasa, Abstraction of programs in PML (Pointer Manipulation Language), JAIST/TRUST - AIST/CVS joint workshop on verification technology (VERITE), 金沢, 2005.
[73] 田辺良則，関澤俊弦，湯浅能史，高橋孝一，抽象化検証ツール TLAT の構築に向けて，第二回システム検証の科学技術シンポジウム，大阪, 2005.
[74] 田辺良則，湯浅能史，関澤俊弦，高橋孝一，様相論理を使用したヒープ検証方式，第 3 回ディペンダブルソフトウェアワークショップ (DSW’06), 2006.
[75] Carl Frederiksen，田辺良則，萩谷昌己，抽象化によるグラフ書換系活性性質検証の一手法，第8回プログラミングおよびプログラミング言語ワークショップ(PPL2006), 2006.
[76] 田辺良則，萩谷昌己，時間付きグラフ書換系の抽象化について，第8回プログラミングおよびプログラミング言語ワークショップ(PPL2006), 2006.
[77] Hiroyuki Ozaki, Agate: an Agda-to-Haskell compiler, TYPES 2006, University of Nottingham, UK, 2006.
[78] Hiroki Takamura, The variety of modal FLew-algebras is generated by its finite simple members, Advances in Modal Logic 2006, Noosa, Sunshine Coast, Queensland, Australia, 2006.
[79] 岡本圭史，木下佳樹，函数記号付一階様相 μ 計算，日本ソフトウェア科学会第 23 回大会，東京大学本郷キャンパス, 2006.
[80] Yukiyoshi Kameyama, Yoshiki Kinoshita, and Koki Nishizawa, Weighted Kripke Structures and Refinement of Models, In Proc. of 23th Conference of Japan Society for Software Science and Technology, Tokyo, Japan, 2006.
[81] 湯浅能史，高橋孝一，田辺良則，関澤俊弦，武山誠，自動証明系と定理証明支援系の連携によるポインタ操作プログラムの検証について，日本ソフトウェア科学会第23回大会，東京大学本郷キャンパス, 2006.
[82] 木下佳樹，高橋孝一，田辺良則，湯浅能史，形式的体系の定理証明支援系上での実現法，第三回システム検証の科学技術シンポジウム,千里ライフサイエンスセンター, 2006.
[83] 岡本圭史，一階様相 μ 計算．第三回システム検証の科学技術シンポジウム,千里ライフサイエンスセンター, 2006.
[84] 高橋孝一，田辺良則，奥田俊弦，湯浅能史，抽象化ツール MLAT について，第三回システム検証の科学技術シンポジウム,千里ライフサイエンスセンター, 2006.
[85] Keishi Okamoto, Formal Verification in a First-Order Extension of Modal μ -calculus, 第4回ディペンダブルソフトウェアワークショップ，東京大学弥生講堂, 2006.

[86] 齋藤正也、山形頼之，YAMPII における P2P 層の実装およびモデル検査の報告，第4回ディペンダブルソフトウェアワークショップ，東京大学弥生講堂, 2006.
[87] 田辺良則，湯浅能史，関澤俊弦，高橋孝一，ポインタを扱うプログラムの様相 μ 計算を利用した検証に向けて，第 9 回プログラミングおよびプログラミング言語ワークショップ PPL2007，石川, 2007.
[88] 湯浅能史，田辺良則，関澤俊弦，高橋孝一, Agda-MLAT 連携による Schorr-Waite マーキングアルゴリズムの検証，日本ソフトウェア科学会第 24 回大会，奈良先端科学技術大学院大学, 2007.
[89] Yoshiki Kinoshita, and Koki Nishizawa, An algebraic semantics of predicate abstraction for PML，日本ソフトウェア科学会第 24 回大会，奈良先端科学技術大学院大学, 2007.
[90] Toshifusa Sekizawa, Tatsuhiro Tsuchiya, Tohru Kikuno, and Koichi Takahashi, Analyzing the One Dimensional Ising Model by Probabilistic Model Checking, the IASTED Asian Conference on Modelling and Simulation (AsiaMS 2007), Beijing, China, 2007.
[91] Toshifusa Sekizawa, Yoshinori Tanabe, Yoshifumi Yuasa, and Koichi Takahashi, MLAT: A Tool for Heap Analysis Based on Predicate Abstraction by Modal Logic, the IASTED International Conference on Software Engineering (SE 2008), Innsbruck, Austria, 2008.

③ポスター発表　（国内 3 件、国際 0件）

[92] 永山 操，木下 佳樹，証明支援系 Agda，日本ソフトウェア科学会第 22 回大会，東北大学, 2005.
[93] 永山 操，池上 大介，武山 誠，統合検証環境，情報社会を支える新しい高性能情報処理技術第 2 回公開シンポジウム，駒場エミナース, 2005.
[94] 木下佳樹，検証における記述量爆発問題の構造変換による解決，デモ展示 CREST「情報を支える新しい高性能情報処理技術」第3回公開シンポジウム，駒場エミナース, 2006.

(4)特許出願
①国内出願 (0 件)
②海外出願 (0 件)

(5)受賞等

①受賞

[1] 西澤弘毅，日本ソフトウェア科学会 高橋奨励賞, 2007.
[2] 田辺良則・高井利憲・高橋 孝一，日本ソフトウェア科学会 第1回解説論文賞, 2007.

②新聞報道

③その他

(6)その他特記事項

［1］「Agda 公式ホームページ http://unit.aist.go.jp/cvs/Agda/ 公開 2006.11」

7 研究期間中の主な活動

ワークショップ・シンポジウム等

年月日	名称	場所	参加人数	概要
2004.2.4～2.6	弟1回システム検証の科学技術シンポジウム	梅田スカイビル会議室	219 名	情報システムのディペンダビリティ、情報処理システム開発の生産性、数理的技法、数理的技法周辺の理論、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について研究討論を行う
2004.5.11～5.12	第1回 AIST/CVS ワークショップ Workshop on Types for Verification	産業技術総合研究所 尼崎サイト システム検証研究センター	講演者 5 名 当プロジェクト 4 名他 全参加者 23 名	型理論・関数型言語の権威の来日が重なったのを機会に、当該分野の検証への適用について、国内外専門家による講演をとおして、基盤的理論体系から実装技術まで幅広く討議する
2004.6.14～6.18	One Week Intensive Course in Advanced Functional Programming AIST version	産業技術総合研究所 尼崎サイト システム検証研究センター	研究員 13 名	Haskell での高度なプログラミング技法(型クラス、モナド、埋め込み言語他)について、Chalmers 大より講師を招いて一週間連続の集中講義を行う。
2004.10.11～10.15	第1回 Agda Implementors Meeting 対話型定理証明システム Agda の共同開発にかかる情報交換	Chalmers University of Technology,Göteborg, Sweden	当プロジェクトより 4 名、Chalmers より 13 名	講演会一日、Code sprint (いくつかのテーマに分かれてプログラミングを行う)三日間
2004.10.21	第2回 AIST/CVS ワークショップ One-day Workshop on Verification and Rewriting (Buchberger, Meseguer workshop.)	産業技術総合研究所 尼崎サイト システム検証研究センター	講演者 7 名(内当プロジェクト3名)他全参加者 26 名	書き換え理論の実装と高信頼性開発への適用、書き換え系の停止性に関する新結果、等号つきオートマトンによる到達可能性解析、数理的理論の探究の機械的補佐、特にアルゴリズム合成に関する講演と討議
2005.4.14～4.20	第2回 Agda Implementors Meeting	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	19 名	Chalmers 大学と Agda 研究開発の進展を共有し今後方向を定めるセミナーと集合合宿形式のコードスプリントの実施。前者では Agda 新機能や次世代プロトタイプの解説など、後者では検証ケーススタディ・技術者養成用演習課題開発等を中心に行なう。

年月日	名称	場所	参加人数	概要
2005.4.18	AIST/CVS Workshop on Automatic and Interactive Verification	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	25 名	アルゴリズミックな自動検証と人知を活かせる対話型の検証の効果的な組み合わせについて討議する、一日ワークショップ。Illinois 大 José Meseguer 教授、Chalmers 大 Thierry Coquand, Peter Dybjer, Beng Nordström三教授他、当研究センターがそれぞれの分野で協力関係にある研究者の同時来日を機会に、本一日ワークショップを開催。
2005.8.30 ～8.31	第3回 Agda Implementors Meeting	Chalmers University of Technology, Dept. of Computer Science	18 名	Chalmers 大学と Agda 研究開発の進展を共有し今後方向を定めるセミナー。Agda2 の仕様と実装方法に関する討議を行う。
2005.10.20 ～10.21	第2回システム検証の科学技術シンポジウム	ライフサイエンスセンター 5F サイエンスホール	10/20 146 名 10/21 112 名	システム検証の二つの代表的なアプローチである数理的技法（formal methods）とテスト技法、数理的技法の対象となる数理的モデルを提供するプログラミング意味論、システム開発への品質保証の導入、検証技術の企業におけるシステム開発への適用事例をはじめとする関係各方面における第一線の研究発表をし、この分野の現状を明らかにする。
2006.1.27	第 1 回 Agda-CAL Workshop	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	13 名	証明作業を共有することで、両者の理論体系・実装を深く理解し、集中討議をする。 再帰的/帰納的述語定義、帰納法の扱い、証明構成操作の技法・実装などについての比較検討。
2006.4.7	第5回 AIST/CVS ワークショップ（AIST/CVS Workshop on Shape Aanalysis and Program Analysis）	システム検証研究センター千里オフィス 6F 会議室	30 名	Mooly Sagiv 教授（Tel-Aviv 大学）の招聘を機に Shape analysis や Program analysis に関する Workshop を開催し講演を依頼。
2006.5.18～5.24	The 4th Agda Implementors Meeting (AIM4)	システム検証研究センター千里オフィス 6F 会議室	14名	Chalmers 大学との共同研究集会。集中合宿式の開発作業コードスプリントの実施と Agda2の研究開発の進展を共有し今後の方向を定める討議をする。今回のコードスプリントでは、Agda2 の開発実作業を進めた。（ユーザーインターフェース、コア言語型検査器、フル言語からコアへの翻訳器、抽象データ型表現、ライブラリ更新。）
2006.5.19	2nd Workshop on Verification Technology (VERITE)	システム検証研究センター千里オフィス 6F 会議室	39 名	北陸先端科学技術大学（JAIST）と当センターとの定例ジョイントワークショップ。第 2 回となる今回は、検証を基礎付ける理論的トピックを重点に行う。

年月日	名称	場所	参加人数	概要
2006.9.25～9.29	The 5th Agda Implementors Meeting (AIM5)	Chalmers 大学 計算機科学工学部	18 名	AIM4でのトピックに新たなものを加え、Agda2 の開発実作業をさらに進める。(終止検査、Agate2 コンパイラ、ユーザーインターフェース、バッチ式フル言語型検査、コア言語検査、フルからコアへの翻訳、ライブラリ)。
2006.10.30～11.1	第3回システム検証の科学技術シンポジウム	千里ライフサイ エンスセンタービル 5F サイエンスホール	136 名	数理的技法(formal methods)とテスト技法、プログラミング意味論、システム開発への品質保証の導入、検証技術の企業におけるシステム開発への適用事例など、第一線の研究発表をし、この分野の現状を明らかにする。
2006.11.27～11.28	JAIST/TRUST - AIST/CVS joint workshop on VERIfication Technology (3rd VERITE)	北陸先端科学技術大学院大学・知識講義棟2階中講義室	約 40 名	北陸先端科学技術大学(JAIST)と当センターとの定例ジョイントワークショップ。
2007.3.6～3.7	JAIST/TRUST - AIST/CVS joint workshop on VERIfication TEchnology (4th VERITE)	北陸先端科学技術大学院大学・知識講義棟2階中講義室	約 40 名	北陸先端科学技術大学(JAIST)と当センターとの定例ジョイントワークショップ。
2007.5.24～5.30	The 5th Agda Implementors Meeting (AIM6)	Chalmers 大学 計算機科学工学部	19 名	依存型プログラミング他のケーススタディを重視、Agda2 の利点を明示する使用例を開発し、今後の Agda2 普及活動に備える。本体と関連するソフトウェアの開発も続行する。(ユーザーインターフェース、Agda1 コードからの変換ツール他)
2007.11.26～11.30	The 7th Agda Implementors Meeting (AIM7)	システム検証研究センター千里オフィス 6F 会議室	12 名	Agda2 依存型プログラム・ライブラリ、場合わけの完全性検査機能と自動生成、知識様相論理実装、CPU 仕様定義などについて作業を行う。

●その他「計算機言語談話会(CLC)」を以下の通り実施した。(平成16～平成19年度)

年月日	名称	場所	参加人数	概要
平成16年4月6日	第九十一回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	毎回講師を含む約 25 名	演題:Coverage Checking Algorithm for LF 講演者:Carsten Schürmann (Yale University)
平成 16 年 4 月 13 日	第百九十二回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:広義重積分体系の充実と誤差の実効的把握 講演者:山崎 洋平 (大阪大学)
平成 16	第百九十三四回計算	システム検証研究	同上	演題:Compositional Syntax and

年月日	名称	場所	参加人数	概要
年 4 月 16 日	機言語談話会	センター 千里オフィス 6F 会議室		Semantics of Tables 講演者:Wolfram Kahl (McMaster University)
平成 16 年 5 月 20 日	第百九十四回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:プロセス代数 CSP のための定理証明器 講演者:磯部 祥尚 (産総研 情報処理研究部門)
平成 16 年 5 月 20 日	第百九十五回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:安全性検証における項書換えを用いた場合分けの支援 講演者:清野 貴博 (北陸先端大言語設計学講座)
平成 16 年6月3日	第百九十六回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:実関数の実効性概念の比較 講演者:河村 彰星 (東京大学コンピュータ科学)
平成 16 年 6 月 10 日	第百九十七回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:様相論理の証明図探索 講演者:松本 利雅 (北陸先端大情報科学研究科)
平成 16 年 6 月 17 日	第百九十八回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:古典論理から型体系へ 講演者:山形 頼之
平成 16 年 6 月 24 日	第百九十九回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:モデル検査事例の紹介 講演者:渡邊 宏 (産総研 システム検証研究センター)
平成 16 年7月1日	第百回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:項書換え系の安全性検証問題のための自動抽象化法 講演者:高井 利憲 (JST 研究員)
平成16 年 7 月 8 日	第百一回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Recursive Object-Oriented Modules 講演者:中田 景子 (京都大学数理解析研究所)
平成16 年 7 月 9 日	第百二回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:テスト付きクリーニ代数の自由生成 講演者:古澤 仁 (産総研 CSV)
平成16 年 7 月 15 日	第百三回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:抽象化を用いた検証ツールの調査 講演者:高井 利憲 (JST 研究員)
平成16 年 7 月 22 日	第百四回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:ACTAS: A System Design for Associative and Commutative Tree Automata Theory 講演者:高井 利憲 (JST 研究員) 大崎 人士 (システム検証研究センター)
平成16 年8月5日	第百五回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:The Time Complexity on a Higher-Order Unification Problem and Elimination of Constants 講演者:吉仲 亮 (東大 学際情報学府)

年月日	名称	場所	参加人数	概要
平成16年9月2日	第百六回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:BDD を用いた 2 方向 CTL 論理式充足可能性決定手続きの実装 講演者:田辺 良則 (産総研 CVS/JST 研究員)
平成 16年 9 月 7 日	第百七回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:高階論理の完全性とその周辺について 講演者:岡本 圭史 (産総研 CVS)
平成 16年 9 月 14 日	第百八回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:組み込みシステム開発への形式的手法の適用 講演者:木下 佳樹 (産総研 CVS), 水口 大知 (産総研 CVS)
平成 16年 9 月 21 日	第百九回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:"サマースクール Marktoberdorf 2004" 参加報告:水口 大知 (産総研 CVS)
平成 16年 9 月 28 日	第百十回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:The Size-change Principle for Program Termination 講演者:Carl Christian Frederiksen (東大 情報理工学系研究科)
平成 16年 10 月 7 日	第百十一回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Forcing for AFA-models and transition systems 講演者:佐藤 憲太郎 (産総研 CVS)
平成 16年 10 月 18 日	第百十二回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:並行論理プログラムの意味論と処理系最適化 講演者:加藤 紀夫 (早稲田大学理工学部CS学科)
平成 16年 10 月 28 日	第百十三回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Checking Sufficient Completeness with Equational Tree Automata 講演者:Joe Hendrix (Department of Computer Science, University of Illinois at Urbana-Champaign)
平成 16年 11 月 5 日	第百十四回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:経済評価の考え方 講演者:岸本充生 (産総研 化学物質リスク管理研究センター)
平成 16年 11 月 11 日	第百十五回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:A Comprehensive Methodology for Developing Safety-Critical Software 講演者:Alan Wassyng (Department of Computing and Software, McMaster Univ.)
平成 16年 11 月 25 日	第百十六回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:LolliMon: executing linear logic specifications 講演者:Jeff Polakow (産総研 システム検証研究センター/JST CREST) : 演題:Reasoning about Term Rewriting in Kleene Categories with Converse

年月日	名称	場所	参加人数	概要
				講演者:高井 利憲 (産総研 システム検証研究センター/JST CREST) 演題:計算代数セミナー報告 講演者:池上 大介 (産総研 システム検証研究センター/JST CREST)
平成 16 年 12 月 2 日	第百十七回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:From algebras and coalgebras to dialgebras 講演者:Erik Poll(Computing Science Department Raboud University Nijmegen, Netherlands)
平成 16 年 12 月 9 日	第百十八回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:The ESC/Java2 Calculi and Object Logics: Implications on Specification and Verification 講演者:Joseph Kiniry (Department of Computer Science, University College Dublin, Ireland)
平成 17 年 1 月 11 日	第百十九回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Kleene Algebra with Tests 講演者:Dexter Kozen (Computer Science Department, Cornell University)
平成 17 年 1 月 13 日	第百二十回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:場の理論から見た部分構造論理 講演者:佐藤 憲太郎 (産総研 システム検証研究センター)
平成 17 年 1 月 27 日	第百二十一回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Transfer Results of Bimodal Logics with Irreflexive Modality 講演者:佐野 勝彦 (京都大学)
平成 17 年 2 月 10 日	第百二十二回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:埋め込み構造を持つクリーニ代数の枠組み 講演者:古澤 仁 (産総研 システム検証研究センター)
平成 17 年 2 月 17 日	第百二十三回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Web アプリケーションのクラス設計仕様に対するモデル化と検証 講演者:崔 銀惠 (産総研 システム検証研究センター) 演題:Web アプリケーションの上流仕様に対する検証講演者:河本 貴則 (産総研 システム検証研究センター)
平成 17 年 2 月 24 日	第百二十四回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:不動点付高階様相論理 講演者:(岡本 圭史 (産総研 システム検証研究センター) 演題:BDD による実装が可能な様相論理の充足可能性判定手続き 講演者:田辺 良則 (産総研 システム検証研究センター/JST CREST))
平成 17	第百二十五回計算機	システム検証研究	同上	演題:Tyrolean Termination Tool

年月日	名称	場所	参加人数	概要
年 2 月 25 日	言語談話会	センター 千里オフィス 6F 会議室		講演者:Aart Middeldorp (University of Innsbruck)
平成 17 年 3 月 10 日	第百二十六回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:形式手法によるセーフティクリティカル組込みソフトウェア開発環境 講演者:小西 晃輔 (株式会社シーディー・アダプコ・ジャパン 複合解析技術室)
平成 17 年 3 月 24 日	第百二十七回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:MPI 通信ライブラリの概要と実装 講演者:石川 裕 (東京大学)
平成 17 年 3 月 25 日	第百二十八回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:汎用システムとしての「ラムダ計算 + 論理」 ″Lambda Calculus + Logic″ as the universal system 講演者:古森 雄一 (千葉大学総合メディア基盤センター)
平成 17 年 3 月 31 日	第百二十九回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:モデル理論と計算機科学 講演者:桔梗 宏孝 (東海大学理学部)
平成 17 年4月7 日	第百三十回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:出張報告 * Dagstuhl seminar ″Mathematics, Algorithms, Proofs″ 2005 * Chalmers 大学 講演者:池上 大介 (産総研 システム検証研究センター/JST CREST)
平成 17 年 5 月 11 日	第百三十一回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Incremental Software Construction 講演者:Ralph-Johan Back (Abo Akademi University and TUCS)
平成 17 年 5 月 12 日	第百三十二回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:XML 変換の大域的な型検査の問題 講演者:戸沢 晶彦 (日本 IBM 東京基礎研究所)
平成 17 年 5 月 19 日	第百三十三回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: 1. 並列合成の論理演算を持つ論理体系 2. 依存型付プログラミング言語処理系の実装 講演者:竹内 泉 (産総研 システム検証研究センター) 尾崎 弘幸(産総研 システム検証研究センター)
平成 17 年 5 月 24 日	第百三十四回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Model-based Development of Safe and Distributed Embedded Software 講演者:Dr. Bernard Dion (Esterel Technologies)

年月日	名称	場所	参加人数	概要
平成 17 年6月2日	第百三十五回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:1. 伝聞の論理　2. Kleene category as a model of calculation 3. パイ計算による仕様を検証する論理体系 講演者:竹内 泉 (産総研 システム検証研究センター)
平成 17 年6月3日	第百三十六回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Mobile Resource Guarantees 講演者: Don Sannella (University of Edinburgh)
平成 17 年 6 月 16 日	第百三十七回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Separation Logic 紹介 講演者:高橋 孝一 (産総研 システム検証研究センター)
平成 17 年 6 月 23 日	第百三十八回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:高信頼性ソフトのための IV&V の取り組み 講演者:片平 真史 (宇宙航空研究開発機構(JAXA) 情報技術開発共同センター), 石濱 直樹 (宇宙航空研究開発機構(JAXA) 情報技術開発共同センター)
平成 17 年 6 月 30 日	第百三十九回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: Verification of Memory Management property of Application Specific OS using Separation logic 講演者:Nicolas MARTI (University of Tokyo)
平成 17 年7月4日	第百四十回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: ″Synchronization support for concurrent protocols and dynamic protocol update.″ 講演者:Pawel T. Wojciechowski (School of Computer and Communication Sciences, Ecole Polytechnique Fe'de'rale de Lausanne (EPFL))
平成 17 年7月7日	第百四十一回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:線型論理における4値論理、ゲーム及びストーカー理論の見地から 講演者:佐藤 憲太郎 (ミシガン大学)
平成 17 年9月8日	第百四十二回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: 1. 定理証明支援系 Agda の FOL プラグイン　2. 一階様相 μ 計算　3. 正規木表現の代数構造について 講演者:1. 池上 大介(産総研 システム検証研究センター/JST CREST) 2. 岡本 圭史(産総研 システム検証研究センター) 3. 高井 利憲(産総研 システム検証研究センター/JST CREST), 古澤 仁(産総研 システム検証研究センター)

年月日	名称	場所	参加人数	概要
平成 17 年 9 月 29 日	第百四十三回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:ピゾ数から出来る準周期格子 講演者:竹内 泉 (産総研 システム検証研究センター)
平成 17 年 10 月 6 日	第百四十四回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: Lawvere Theories for Complete Fibrations and Fibred CCCs 講演者:西澤 弘毅 (産総研 システム検証研究センター)
平成 17 年 10 月 13 日	第百四十五回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Hierarchies of computation tree logics 講演者:Till Plewe (筑波大学)
平成 17 年 10 月 27 日	第百四十六回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:様相不動点論理と抽象解釈のための代数構造 講演者:西澤 弘毅 (産総研 システム検証研究センター)
平成 17 年 11 月 4 日	第百四十七回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: UPPAAL – a tool for model-checking and testing of real-time systems 講演者:Paul Pettersson (Uppsala University, Sweden)
平成 17 年 11 月 24 日	第百四十八回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:第一級限定継続に対する簡潔な型システム 講演者:亀山 幸義 (筑波大学)
平成 17 年 12 月 1 日	第百四十九回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: Agda コンパイラ agate の実装 講演者:尾崎 弘幸 (産総研 システム検証研究センター)
平成 17 年 12 月 15 日	第百五十回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:機能安全規格 IEC61508 について 講演者:松岡 聡(産総研 計測標準研究部門, システム検証研究センター), 水口 大知(産総研 システム検証研究センター)
平成 18 年 1 月 12 日	第百五十一回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:パターンに基づくプログラム変換システム RAPT 講演者:青戸 等人(東北大学 電気通信研究所), 千葉勇輝(東北大学 情報科学研究科)
平成 18 年 1 月 19 日	第百五十二回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: Monotone AC-Tree Automata 講演者:Hitoshi Ohsaki (Reseach Center for Verification and Semantics National Institute of Advanced Industrial Science and Technology (AIST), joint work with Jean-Marc Talbot, Sophie Tison and Yves Roos at LIFL, France)

年月日	名称	場所	参加人数	概要
平成 18 年 2 月 2 日	第百五十三回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: POPL2006 および VMCAI2006 の報告 講演者:高井 利憲 (産総研 システム検証研究センター)
平成 18 年 2 月 9 日	第百五十四回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: Formal Construction and Verification of Home Service Robots : A Case Study 講演者:Moonzoo Kim (Pohang University of Science and Technology)
平成 18 年 2 月 23 日	第百五十五回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: Regular Approaches to Program Correctness 講演者:Georg Struth (University of Sheffield)
平成 18 年 2 月 27 日	第百五十六回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:コンピュータ将棋プレイヤ「激指」と関連技術 講演者:近山 隆 (東京大学 新領域創成科学研究科 基盤情報学専攻)
平成 18 年 3 月 2 日	第百五十七回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: Reasoning about transfinite sequences 講演者:David Nowak (University of Tokyo)
平成 18 年 3 月 7 日	第百五十八回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: 1. Coalgebraic methods in computer science: introduction and beyond 2. A security review of the biometric passport 講演者:1. 蓮尾 一郎 (University Nijmegen, The Netherlands) 2. Bart Jacobs (University Nijmegen, The Netherlands)
平成 18 年 3 月 9 日	第百五十九回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:1. ポインタで表されたデータ構造を扱うプログラムの様相論理を用いた検証方式 2. Symbolic Protocol Analysis in Presence of a Homomorphism Operator and Exclusive Or 講演者:1. 田辺 良則 (産総研 システム検証研究センター) 2. Ralf Treinen (Laboratoire Specification et Verification ECOLE NORMALE SUPERIEURE DE CACHAN)
平成 18 年 3 月 16 日	第百六十回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:モデル検査と用いたアクティブデータベースルールの停止性検査 講演者:崔 銀惠 (産総研 システム検証研究センター)
平成 18 年 3 月 23 日	第百六十一回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: A sequent calculus for 1-backtracking 講演者:山形 頼之 (産総研 システム検証研究センター)
平成 18	第百六十二回計算機	システム検証研究	同上	演題:Achievement of functional

年月日	名称	場所	参加人数	概要
年4月5日	言語談話会	センター 千里オフィス 6F 会議室		safety for safety critical computer systems 講演者:Ron Bell (Institution of Electrical Engineers (IEE) and UK Health & Safety Executive (HSE))
平成 18 年 4 月 13 日	第百六十三回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:XPE Meets TWB 講演者:松本利雅 (北陸先端科学技術大学院大学(JAIST))
平成 18 年 5 月 18 日	第百六十四回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Defunctionalized Interpreters for Higher-Order Programming Languages 講演者: Olivier Danvy (BRICS, University of Aarhus, Denmark)
平成 18 年6月8日	第百六十五回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題(1) 時空間ソフト線形論理とそのコンピュータシステムへの応用 演題(2) A uniform proof-theoretic foundation for paraconsistent logic programming 講演者:上出 哲広 (東京工業高等専門学校情報工学科)
平成 18 年 6 月 15 日	第百六十六回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:プログラミング言語 SML＃の実装と理論 講演者:大堀 淳 (東北大学 電気通信研究所)
平成 18 年 6 月 22 日	第百六十七回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:LCMと証明アニメーション 講演者: 林晋 (京都大学大学院文学研究科)
平成 18 年7月4日	第百六十八回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題 :Statistical Image Steganalysis 講演者:Xiaoyi Yu (JANA Solutions, Inc.)
平成 18 年 7 月 13 日	第百六十九回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:様相論理による抽象化によるポインタ構造の検証について --終了と時刻の扱い 講演者:田辺 良則 (産総研 システム検証研究センター) 演題:モデル検査で状態爆発をいかに抑えるか? 講演者: 高橋 孝一(産総研 システム検証研究センター)
平成 18 年 7 月 20 日	第百七十回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: 求解と証明のインタラクション 講演者:井田 哲雄 (筑波大学 システム情報工学研究科)
平成 18 年8月2日	第百七十一回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Scalable Verification Techniques and Tools for E-Commerce Software 講演者: Sree Rajan (Fujitsu Laboratories of America)
平成 18 年 9 月 21 日	第百七十二回計算機言語談話会	システム検証研究センター 千里オフィス	同上	演題:LMNtal as a Unifying Declarative Language 講演者: 上田 和紀 (早稲田大

年月日	名称	場所	参加人数	概要
		6F 会議室		学理工学術院 コンピュータ・ネットワーク工学科)
平成 18 年 10 月 11 日	第百七十三回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Model Checking: From Hardware To Software And BackAgain 講演者: Edmund M. Clarke (Carnegie Mellon University)
平成 18 年 10 月 26 日	第百七十四回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Weak Inversion and Its Application to Parallelization 講演者: Zhenjiang Hu (University of Tokyo)
平成 18 年 11 月 9 日	第百七十五回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Computation trees and monodic tree Kleene algebra 講演者: 高井 利憲 (産業技術総合研究所システム検証研究センター)
平成 18 年 11 月 13 日	第百七十六回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: Computational soundness and completeness of formal indistinguishability relations in Abadi-Rogaway-type theories 講演者: Gergei Bana (University of California)
平成 18 年 12 月 7 日	第百七十七回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:プッシュダウンシステムを中心としたモデル検査法および管理の視点に基づいたプログラミングパラダイムについて 講演者: 新田直也 (甲南大学理工学部情報システム工学科)
平成 18 年 12 月 14 日	第百七十八回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: Private row types: combining modularity and extensibility in ML 講演者: Jacques Garrigue (名古屋大学大学院多元数理科学研究科)
平成 19 年 1 月 11 日	第百七十九回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: Hybrid formalisms for topological spaces 講演者:Tadeusz Litak (北陸先端科学技術大学院大学情報科学研究科)
平成 19 年 1 月 18 日	第百八十回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:通信プロセスモデルにおける構造操作意味定義と代数意味論 講演者: 結縁 祥治 (名古屋大学大学院情報科学研究科)
平成 19 年 1 月 25 日	第百八十一回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:脳の機能を再現するプログラムの構想 講演者: 一杉裕志(産業技術総合研究所脳神経情報研究部門)
平成 19 年 2 月 1 日	第百八十二回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:構成的型理論 ― 連続講義第1回 講演者: Bengt Nordstrom(シャルマース工科大学)
平成 19 年 2 月 8 日	第百八十三回計算機言語談話会	システム検証研究センター 千里オフィス	同上	演題: 構成的型理論 ― 連続講義第 2 回 講演者: Bengt Nordstrom(シャ

年月日	名称	場所	参加人数	概要
		6F 会議室		ルマース工科大学)
平成 19 年 2 月 15 日	第百八十四回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	講演者: Bengt Nordstrom(シャルマース工科大学) 演題:構成的型理論 ー 連続講義第 3 回
平成 19 年 2 月 15 日	第百八十五回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: 言語間翻訳の諸性質の証明手法について 講演者: 安部 達也 (東京大学情報理工学系研究科)
平成 19 年 2 月 16 日	第百八十六回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:不動点帰納法に基づく不変性検証の補題発見による自動化 講演者: 中野 昌弘 (北陸先端科学技術大学院大学)
平成 19 年 2 月 16 日	第百八十七回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:プログラム自動改良のための定理証明システム 講演者: 小西 善二郎 (東京女子大学)
平成 19 年 2 月 22 日	第百八十八回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Formal Specification and Analysis of Real-Time Systems in Real-Time Maude 講演者: Peter Olveczky(Univ. Oslo)
平成 19 年 2 月 23 日	第百八十九回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: 「砂山のパラドックス」の集合論的表現 講演者: 矢田部 俊介(神戸大学工学部情報知能工学科)
平成 19 年 2 月 23 日	第百九十回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:構成的型理論 ー 連続講義第4回 講演者: Bengt Nordstrom(シャルマース工科大学)
平成 19 年 3 月 1 日	第百九十一回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:構成的型理論 ー 連続講義第 5 回(最終回) 講演者: Bengt Nordstrom(シャルマース工科大学)
平成 19 年 3 月 16 日	第百九十二回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: On the structure of the lattice of normal modal logics containing KTB. 講演者: 宮崎裕 (北海道大学) 演題: TBA 講演者: 加藤和彦 (筑波大学)
平成 19 年 3 月 22 日	第百九十三回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題: 線形時間論理のシーケントシステムについて 演題:パラコンシステントモデル検査のために拡張された分岐時間論理 講演者: 上出 哲広(システム検証研究センター) 演題:ソフトウエアアップデートシステムプロトコルの BAN logic による安全性検証 講演者: 吉田 聡(システム検証研究センター)

年月日	名称	場所	参加人数	概要
平成 19 年 3 月 22 日	第百九十四回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:線形時間論理のシーケントシステムについて 講演者:上出 哲広(システム検証研究センター)
平成 19 年 3 月 22 日	第百九十五回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:ソフトウエアアップデートシステムプロトコルの BAN logic による安全性検証 講演者:吉田 聡(システム検証研究センター)
平成 19 年4月5日	第百九十六回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:デタラメさを精密につくる:メルセンヌツイスター擬似乱数発生法 講演者:松本眞(広島大学)
平成 19 年 4 月 12 日	第百九十七回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Formally Modeling and Verifying Quorum Based Distributed Conflict Resolution Algorithms 講演者:Armin Lawi (九州工業大学)
平成 19 年 4 月 19 日	第百九十八回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:一階様相 μ 計算の完全性について 講演者:鹿島 亮(東京工業大学)
平成 19 年 5 月 10 日	第百九十九回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:An upper bound of the values of promitive recursive functional 講演者:竹内 泉(産業技術総合研究所システム検証研究センター)
平成 19 年 5 月 10 日	第二百回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:構成的証明について 講演者:吉田 聡(産業技術総合研究所システム検証研究センター)
平成 19 年 5 月 31 日	第二百一回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Ordered Categories of Processes 講演者:Michael Winter (Department of Computer Science, Brock University)
平成 19 年 6 月 28 日	第二百二回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:セキュリティプロトコルの論理的検証法について 講演者:長谷部 浩二 (産総研システム検証研究センター)
平成 19 年7月5日	第二百三回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Program Analysis based on Weighted Pushdown Model checkin 講演者:Li Xin (Japan Advanced Institute of Science and Technology)
平成 19 年 7 月 12 日	第二百四回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:セキュリティプロトコルの論理的検証法について 講演者:長谷部 浩二 (産総研システム検証研究センター)
平成 19 年 7 月 26 日	第二百五回計算機言語談話会	システム検証研究センター 千里オフィス	同上	演題:アセンブラプログラムのモデル検査による検証事例 講演者:高井 利憲 (産総研 シ

年月日	名称	場所	参加人数	概要
		6F 会議室		ステム検証研究センター)
平成 19 年 7 月 31 日	第二百六回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:MLL proof nets as error-correcting codes 講演者:松岡 聡 (産総研 計測標準研究部門、システム検証研究センター)
平成 19 年 9 月 25 日	第二百七回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演 題:ITERATIVE ALGEBRAS 講演者:Jiri Adamek (Institute of Theoretical Computer Science,Technical University of Braunschweig, Germany)
平成 19 年 10 月 4 日	第二百八回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:A simple type-theoretic language: Mini-TTS 講演者:武山 誠 (産総研 システム検証研究センター)
平成 19 年 10 月 11 日	第二百九回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:LTL モデル検査のための図示記法とその特徴づけ 講演者:吉田 聡 (産総研 システム検証研究センター)
平成 19 年 10 月 18 日	第二百十回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:min-plus 代数 $N\infty$ 上の様相 μ 計算とその応用 講演者:田辺 良則 (産総研 システム検証研究センター)
平成 19 年 10 月 18 日	第二百十一回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:An algebraic semantics of predicate abstraction for PML 講演者:木下 佳樹 (産総研 システム検証研究センター)
平成 19 年 10 月 25 日	第二百十二回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:業務フロー図検証システムの紹介 講演者:高木理(産総研 システム検証研究センター)
平成 19 年 10 月 29 日	第二百十三回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Model-checking and simulatin-checking of dense-time systems with BDD-like diagrams 講演者:Farn Wang (National Taiwan University)
平成 19 年 11 月 15 日	第二百十四回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Analyzing the One Dimensional Ising Model by Probabilistic Model Checking 講演者:関澤俊弦(産総研システム検証研究センター)
平成 19 年 12 月 18 日	第二百十五回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演 題 : Modular confluence modulo: a complete picture 講 演 者 : Jean-Pierre Jouannaud (Laboratoire d'Infomatique, École Polytechnique)
平成 20 年 1 月 31 日	第二百十六回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演 題 : Extending Refinement Calculus with Separation Logic for Safe Modification of Pointer Programs 講演者: 西村進(京都大学大学院理学研究科)

年月日	名称	場所	参加人数	概要
平成 20 年 2 月 14 日	第二百十七回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:SSA 形式と等価な型システムによるコンパイラ最適化の実装 講演者:松野 裕(東北大学電気通信研究所)
平成 20 年 2 月 21 日	第二百十八回計算機言語談話会	システム検証研究センター 千里オフィス 6F 会議室	同上	演題:Residuated lattices with Operators へ向けて 講演者:高村 博紀(産総研 システム検証研究センター)

8 結び

本計画の波及効果 本計画が周囲に与えている影響について、とくに記しておきたい。本計画の開始と相前後して、産総研にシステム検証研究センターが設置され、本計画は同研究センターで遂行された。 この研究センターでは、本計画と並行して産業などにおけるフィールドワークが遂行されている。 技術者の個人的スキルを向上させるための研修コース研究開発だけでなく、組織的なスキルアップをはかるべく技術導入実験を企業などと共同で行っており、研究センター開始後三年半で二十件以上の検証事例(その多くはソフトウェアの開発現場における事例である)を収集するなど、国内のこの分野の技術移転に先端的役割を果たしているといってよいと考えられる。

本研究の研究分野は、プログラム意味論(sematnics)および数理的技法(formal methods)と呼ばれ、数理科学的背景をもつ強力なシステム検証技術のために必要な一般常識を提供している。 欧米ではこの分野の研究活動の歴史が長く、したがって裾野も広く、計算機科学の基礎知識のひとつとみなされている。 しかし、本計画開始以前には、この分野の国内での研究活動は、講座単位でいくつかの大学に分散するだけで、この分野の知識は、特殊なものとみなされがちであった。 しかし、上記のようなフィールドワーク活動の結果、この研究分野が特殊な、数学のための理論だけを指向しているのではなく、実用を視野に入れた研究も十分に可能であることが学界と産業界に理解されはじめているのではないかと思われる。 一つの重要な研究分野への理解を促進したことが、本計画の重要な波

及効果として、挙げられるのではないかと考えている。

強力なシステム検証技術は、広く産業界から求められている需要の大きい技術であり，信頼に足る技術を提供できれば、それ自体で産業化していく可能性をもつものと考えられる。本計画における基礎研究と、産総研で別途遂行中の企業との連携による実用化研究の成果を相互作用させて、科学に基づくシステム検証技術研究者集団を形成した。 この方向の研究活動が、本計画終了後も国内に定着することは、わが国の情報技術の本格的かつ健全な発展のためには極めて重要だと思われる。

計画遂行のアドミニストレーション 本計画開始後すぐに、産総研は、この分野の研究遂行のために研究ラボ、後に研究センターを設置したため、産総研からの支援は非常に満足のいくものであった。 しかしながら、研究センターの運営が本計画に強く依存する結果となり、しかも必要な資金が殆ど人件費であったので、本計画終了後に研究センターの予算が急激に減額することとなり、研究活動の持続性という点で問題が残った。 本計画に伴って、一名の学生が博士の学位を取得した。 また、二名の社会人が本計画終了後一年以内に博士の学位を取得する見込を得ている。 さらに、本計画では、数学や情報工学で学位を取得してはいるものの、ソフトウェア工学や代数学など、異なる分野の研究を行っていた研究者をプログラム検証の分野に転向させることが多く、すくなくとも七名の研究者を転向させて、この分野の我国の興隆に寄与している。

支援ツールの研究 本計画の提案時には、圏論的手法にもとづく意味論研究の比重をもっと大きくすることを想定していたが、国内に圏論的手法に基づく研究が可能な研究者が殆どいないことに加え、アドバイザリボードからの助言もあって、計画早期に、支援ツールの試作を視野に加えた。 結果的には、そのおかげで研究成果に具体性を持たせることができたが、わが国で殆ど進められていない意味論分野の研究の興隆は、将来の課題として残された。