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
4
2006.07

定義の正当化

情報科学方面の学会での「チュートリアル」で圏論 (category theory) を紹介する依頼をうけたのを機会に、圏論がどのように情報科学に応用されているか、筆者が何故圏論が有効だとおもうのか、についてあらためてかんがえてみた。応用をさがすという数学への接しかたは、本職の数学者にとって、必ずしも、このましい態度ではないかもしれないが、役にたつものを作ってしまったことの結果であるとあきらめて辛抱してもらうことにしよう。

圏論とは？

圏論は、写像や準同型についての理論で、数学的構造に関する議論に適した手法を与えます。数学の中で使われる他に、情報科学や理論物理学などでも理論展開の枠組を与えています。圏は函手を導入するために、函手は自然変換を導入するために導入した、といわれています。

情報科学への圏論の有効な応用の一つに、定義の正当化 (justification) のための根拠をあたえることがある。理論をたてるにあたっては、いくつかの新しい定義を、まったく自由にあたえることができる。しかし、ある定義からは豊富な議論がうみだされるが、べつの定義からは、たいした議論がでてこない、という場合がある。圏論の概念を、豊富な議論をみちびくような、よりよい定義をえらぶための指針として用いることができる。自然現象を説明することを旨とする自然科学では、定義のしかたをえらばなければならない、などという状況は、めったにあらわれなかったのではないか。情報科学は情報を対象とするために、何でもかんでも定義できてしまい、その結果、かえって、よい定義の基準が必要になったのかもしれない。

いろいろな概念を圏、函手、自然変換などとして定式化するのが圏論のやりかたである。概念を対象として定義し、さらに対象のあいだにうまく射が定義できて、圏を構成できれば、概念の定義はまず最低限の基準をみたしたといってよいだろう。しかし圏をつくっただけでは、あまり大したことはいえない。
圏をつくることができたとして、次にしらべたいのは、例えば、その圏と Set や Cat などの基本的な圏のあいだの随伴の有無である。例えば Set への忘却函手があってそれが左随伴をもてば、これはいわゆる自由代数が存在することを意味するから、そこからいろいろな帰結がえられる。Set への忘却函手がさらに monadic であれば、その圏には積や等化射 (equaliser) などの極限が存在し、しかもそれが台集合の極限のうえにつくられることまでわかる。

極限や余極限が存在するかどうかなど、圏の内部構造にも大きな意味があるのはもちろんである。帰納的な定義は、帰納的極限、あるいは filtered diagram の余極限の存在によって正当化することができる。n-tuple が n 個のものの積によって説明できるのはいうまでもないし、等化射によって等式の解集合を表現きるから、極限が存在すればいろいろなことがみちびかれる。

定義した概念を圏として定式化できるかどうか、さらに、その圏が随伴や極限などの構造を、どの程度豊富にもっているかをもって、定義の良し悪しをきめるのは、そう的はずれなことではあるまい。これをもって、定義を正当化する根拠にすることができるようにおもう。

圏論においては、「正しい」定義をさがすのがむずかしい、一旦しかるべき定義をみつけたら、必要とする定理の証明が、殆ど自明なものになってしまうこともおおいといわれる。これは、定義を評価する手段にもちいることができるというのと同じことをしめしているのではないか。

システム検証研究センター長　木下佳樹

＜ＣＶＳニュースレター　４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
●尼崎サイト：〒 661-0974　兵庫県尼崎市若王寺（なこうじ）3-11-46

●トピックス 1

2005 年度 システム検証研究センター 研究成果報告会

CVS では、6 月 1 日に昨年 2005 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。冒頭、CVS 木下センター長より 2005 年度を振り返り、総括を行った後、各研究項目についてそれぞれの班長が進捗や具体的な成果、そしてこれからの進め方などの発表を行いました。

本レターでは、今回発表された全 20 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て冊子として発行を予定しております。発行のご報告は、ホームページ上でさせていただきます。
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 でダウンロードも可能です。
http://unit.aist.go.jp/cvs/techrep.html

2005 年度システム検証研究センター 研究成果報告 全 20 研究項目概要

---

1. 数理モデル
班長：木下佳樹
班員：岡本圭史　高村博紀　竹内泉　武山誠　中原早生　西澤弘毅
数理モデル研究班は算譜意味論、特にリアクティブシステムのシステム検証にあらわれる数理的現象を研究している。平成 17 年度の研究テーマを、命題様相 μ 計算における抽象化の代数的意味論、一階様相 μ 計算、正則 ω 表現の準代数構造、正則木表現の準代数構造の四つに設定した。

2. 支援ソフトウエア研究開発
班長：高橋孝一
班員：田辺良則　関澤俊弦　湯浅能史　高井利憲
ポインタを操作するプログラムのソースコードの検証を行うための様相論理を用いた述語抽象化ツール MLAT(Modal Logic Abstraction Tool）のプロトタイプの作成を行った。

3. PML
班長：木下佳樹
班員：尾崎弘幸　高橋孝一　田辺良則
研究用ポインタ操作言語 PML の意味論を厳密に構築する。具体的には、PML 上の Hoare 論理を定義し、その健全性を証明する。さらに、その証明を Agda 上で実行する。

4. 対話型検証
班長：武山誠
班員：池上大介　清野貴博　西原秀明　永山操　Jeff Polakow
対話型定理証明と自動検証技法群を統括する統合検証環境の構築について、背景と完成像のイメージ、要素技術研究開発の内容などを中心に紹介した。

5. 依存型付作譜言語
班長：尾崎弘幸
班員：加藤紀夫　武山誠
依存型付作譜言語研究班は、Agda を用いた依存型プログラミングを探求するプロジェクトである。Agda 自身を題材に Agda 言語で記述 / 実行 / 検証することを目指している。2005 年度は、Agda から Haskell への変換機能と最適化機能を開発した。今後、最適化機能の改良、ライブラリの開発、事例作りに取り組む予定である。

6.YAMPII 検証プロジェクト
班員：高橋孝一　水口大知　山形頼之（2006 年度研究者）
並列計算用プログラミングインターフェースである MPI の実装、YAMPII を対象として C ソースコードモデル検査器を開発している。プロジェクトの現状について報告する。

7. フィールドワーク 1
班長：大崎人士
班員：尾崎弘幸　小池憲史
ソフトウェア開発工程に導入可能なモデル検査技法についての研究を行った。これまでの研究を通じて得られたモデル化技法を洗練し、モデル検査における要素技術としての位置づけを確立した。また、モデル検査法を効果的に開発現場へ導入するための方法を検討し、モデル化および検査式作成のための技術者育成を行った。

8. フィールドワーク 2
班長：高橋孝一
班員：清野貴博　竹内泉　宮本賢治
本研究では、TACC で行われている産総研イントラ業務システムの設計開発に、形式的記述と検証によって貢献する。05 年度は、代数付き π 計算を使い動作データ構造を統合した記述を与えた。

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
●尼崎サイト：〒 661-0974　兵庫県尼崎市若王寺（なこうじ）3-11-46

9. フィールドワーク 3
班長：山形賴之
班員：R. Affeldt　池上大介　齋藤正也　高井利憲
山下伸夫　吉田聡
食品産業向け商品処理装置のソフトウェア更新システムのセキュリティについて、形式的手法を用いて検証した。その結果について報告する。

10. ソフトウェア認証
班長：松岡聡
班員：木下佳樹　水口大知
20 世紀の終盤から、ソフトウェアは現代人が生きていく上での社会基盤の一端を担うようになった。しかし、その一方でソフトウェアの品質の劣化が指摘されることが多くなってきている。この問題は、日本だけでなく先進国共通である。この問題に対処するため欧州では、ソフトウェアについて第 3 者認証を導入して品質を改善しようとしている。本発表では、欧州のこの動きに対応して設置されたソフトウェア認証研究班の平成 17 年度の活動報告および今後の活動予定について報告する。

11. 研修コース
班長：西原秀明
班員：池上大介　大崎人士　尾崎弘幸　武山誠　崔銀恵
永山操　渡邊宏
全体カリキュラムを作成してモデル検査に関するコース、対話型証明に関するコースを体系付けた．モデル検査研修コース初級編が完成し、テキストは出版されその教授法はノウハウとして登録された。
(出版物については本紙 P5 を参照ください。)

12. π計算の論理
竹内泉
代数付きパイ計算は、代数仕様の項をパイ計算に付け加えることによってパイ計算を拡張したものである。この計算体系の設計、及び、その性質を証明する論理体系の設計を行なった。

13. 空間表現の意味論に関する研究
竹内泉
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である PLCA 表現を提案する。PLCA 表現は点 (point)、有効辺（line)、周 (circuit)、範囲 (area)、この四種類の要素を使って図形を表現する。

14. LCM のための列計算
班長：山形賴之
班員：Stefano Berardi（トリノ大学情報学科）
Proof Animation は形式検証で与えられた証明をプログラムとして再び解釈することで形式化の誤りを検出しようとするものである。Proof Animation のための数学体系である Limit Computable Mathematics の形式体系 PA_1 を与えた。

15. 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に関する理論研究（閉包性，計算量，階層性）および、等式付ツリーオートマトンにもとづくソフトウエア開発（特に, 計算エンジン高速化）を行った。等式付ツリーオートマトンにもとづく、仕様記述言語

◆シリーズ「システム検証技法」
本シリーズでは、CVS で研究を行っているシステム検証技法について、概要を出来るだけわかりやすく解説していきます。第一弾は、現在注目されている「モデル検査法」を取り上げ、3 回に分けて解説します。

モデル検査法①

「モデル検査による検証とは？」

モデル検査はハードウェアやソフトウェアなどのシステムのモデルが、設計者の意図する性質をみたしているかどうかを「全数検索」によって数学的に検証する方法の一つです。全数検索といった作業は計算機が得意とし、作業を計算機に任せて自動化できます。モデル検査は非常に高い信頼性が得られる形式検証が自動実行できる検査法で、近年の計算機パワーの目覚しい向上とあいまり、実用化が期待されています。実際、モデル検査を原理とした検証ツールがいくつも開発されています。インターネット上のフリー百科事典で model checking を検索してみると、その例を見ることができます。

ちなみに、形式検証とは、ソフトウェアの仕様や振る舞いをプログラムとは別の数式や論理式で表現し、数学的な証明手段によって、そのソフトウェアの誤りがないかどうかを調べる手法です。

モデル検査が検証できるのは、時相論理と呼ばれる論理で記述できる性質です。時相論理は、安全性（たとえばデッドロックなどのおかしな状態には陥らない性質）や、応答性（要求すればい

産業技術総合研究所　システム検証研究センター http://unit.aist.go.jp/cvs/
●千里サイト：〒 560-0083　大阪府豊中市新千里西町 1-2-14　三井住友海上千里ビル 5F
●尼崎サイト：〒 661-0974　兵庫県尼崎市若王寺（なこうじ）3-11-46

のための充足完全性の自動検査法を研究開発し、定義拡張や言語論的な考察を行った。

16. Java プログラムの検証事例
関澤俊弦　崔銀恵　竹内泉　高橋孝一
産総研一般公開のために Java で作成された LEGO プログラムの検証を行なった。検証の結果，不具合は発見されなかったが、検証対象への取り組みおよび進捗状況を事例として報告する。

17. 形式仕様開発支援環境の研究
清野貴博
CVS では、Agda を核とする統合検証環境を提唱し、その開発に取り組んでいる。本業務項目では、その一環として代数仕様言語 CafeOBJ が持つ簡約器を呼び出すプラグインを開発する。

18. 数理的技法
渡邊宏
余代数を使い、抽象化技法 Cone of Influence Reduction を表現する数理モデルを完成させた.

19. 評価法
班長：古澤仁
班員：竹内泉　崔銀恵　渡邊宏
数理的技法の便益性評価のための Web システムの上流設計データ収集実験で収集されたデータを分析評価し、通常のレビューと MBR 手法によるレビューをコストと効果の両面で比較した。

20. フォールトトレラント分散アルゴリズムの検証
崔銀恵
ディペンダブル分散システムの実現のための中核となる耐故障分散アルゴリズムの自動検証法の研究状況について報告する。

第三回システム検証の科学技術シンポジウム講演者募集

開催日：2006 年 10 月 30 日（月）～ 11 月 1 日（水）
開催場所：千里ライフサイエンスセンタービル
サイエンスホール（大阪府豊中市）

講演者募集〆切：2006 年 8 月 25 日（金）
原稿〆切：2006 年 9 月 4 日（金）

第三回目のシンポジウムを開催にあたり、システム検証の科学技術に関する研究発表、サーベイおよびチュートリアル講演を募集しています。

【分野例】
情報処理システムのディペンダビリティ / 情報システムの機能安全とその認証 / 情報処理システム開発の生産性 / 数理的技法（formal methods）（モデル検査、定理証明）/ 数理的技法周辺の理論（算譜意味論、プログラミング論理、書換系）/ 情報処理システムのテスト、品質保証、開発方法論 / 検証手法の導入事例研究

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/verification2006/

つか必ず応答があるという性質）といった、システムの「振る舞い」に関する性質のほとんどを記述することが可能です。このような振る舞いに関する性質は、複雑な表現になるため、正しさを検証することが困難となります。仮に、テストなどによって振る舞いのバグが発見できても、原因の特定が困難です。そこで効力を持つのがモデル検査です。モデル検査は、検証に失敗した場合、つまりバグが存在する場合に、そのバグにどうやって到達したのかの履歴を出力するので、デバクのための非常に有用な情報を提供するので、的確なバグの洗い出しが可能になるのです。

モデル検査は、全数検索を原理としているので、検索対象数が天文学的になっては実用的でなくなります。したがって、検索対象数がそれほど多くなく、しかも本質的な間違いがあってはいけないシステムデザインレベルなどに有用です。さらに、最近のさまざまな研究により、モデル検査の適用範囲は広がってきています。本連載では、今後このようなモデル検査の最新の話題、実際問題へ適用する際の注意点などについて述べていきます。

副研究センター長　高橋孝一

連載予定タイトル
第二回：「モデル検査と状態爆発問題」
第三回：「モデル検査による検証の落とし穴」

産業技術総合研究所　システム検証研究センター　http://unit.aist.go.jp/cvs/
●千里サイト：〒 560-0083　大阪府豊中市新千里西町 1-2-14　三井住友海上千里ビル 5F
●尼崎サイト：〒 661-0974　兵庫県尼崎市若王寺（なこうじ）3-11-46

●トピック 2

文部科学大臣表彰「若手科学者賞」受賞
大崎人士（自動検証研究チーム長）

当研究センター大崎人士（自動検証研究チーム長）が「総合領域分野における自動検証技術の研究（等式付ツリーオートマトンとシステム自動検証技術の研究）」においてその業績が認められ、平成１８年度文部科学大臣表彰若手科学者賞を受賞いたしました。

■受賞コメント　大崎人士

総合領域分野での受賞というのは、私の研究スタイルを評価していただいたようで、とてもありがたく思います。
情報システムの安全性の自動検証技術の開発を出発点とした本研究は、等式付きツリーオートマトン理論という木構造言語理論の新たな一研究分野を築くことに貢献しました。理論的には従来ほとんど未開拓だった木構造言語の豊かな階層化という他の追随を許さない新規性を持つと同時に、等式付きツリーオートマトン理論に根ざした自動検証ツールの実装とアルゴリズム開発を通じ、現代情報システムの安全性検証技法の発展に貢献すると考えられるようになりました。

提唱する理論は、世界的にも広がりを見せており、すでに暗号プロトコルや仕様記述などの自動検証で成果を挙げています。このように、自動検証技術の研究開発に端を発した学術的業績が等式付きツリーオートマトンという概念として定着し、新たな研究分野へと発展していくことに皆様から期待を頂けたことは、何よりもの喜びです。今後も特定の理論や成果のみにとらわれることなく、広い視野で研究を進めて生きたいと思います。

■文部科学大臣表彰若手科学者賞について

本賞は、次代を担う若手研究者の自立を促し、我が国発の独創性の高い科学技術の発信に貢献するため、萌芽的な研究あるいは、独創的視点に立った研究等、高い研究開発能力を示す顕著な研究業績を挙げた若手研究者個人に対し授与される賞です。

●トピック 3

CVS 教程①
「4 日で学ぶモデル検査（初級編）」が出版されました

CVS ニュースレターでも以前よりご紹介しておりますモデル検査研修コース（初級編）のテキストが、このたび CVS 教程①「4 日間で学ぶモデル検査（初級編）」として、1 冊の本にまとめられ出版されました。

－本書前書きより－
本書はもともと、当研究センターとある企業との共同研究において、モデル検査をほとんど知らない技術者への教本として作られました。その後記述をより一般的になるように改良し、当研究センターが開発しているモデル検査研修コースのテキストして使用し改良を重ね、その結果今回本の形にまとめたものです。

CVS では数理的技法に関する研修コースカリキュラム「CVS 教程」を開発していますが、本書は CVS 教程の入り口の一つとなるものです。今後も、モデル検査のさらに進んだ内容や対話型検証法の教科書も開発し、数理的技法を体系的に習得するための教材を揃えていく計画ですので、どうぞご期待ください。

CVS 教程①「4 日で学ぶモデル検査 (初級編)」
著者：産総研システム検証研究センター
発行：株式会社エヌ・ティー・エス

産業技術総合研究所　システム検証研究センター http://unit.aist.go.jp/cvs/
●千里サイト：〒 560-0083　大阪府豊中市新千里西町 1-2-14　三井住友海上千里ビル 5F
●尼崎サイト：〒 661-0974　兵庫県尼崎市若王寺（なこうじ）3-11-46

●イベント・講演会

2006 年 03 月～ 2006 年 06 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）
03/02	David Nowak（東京大学）
03/07	蓮尾一郎（University Nijmegen, The Netherlands）
	Bart Jacobs（University Nijmegen, The Netherlands）
03/09	田辺良則（CVS）
	Ralf Treinen（Laboratoire Specification et Verification ECOLE NORMALE SUPERIEURE DE CACHAN）
03/16	崔銀惠（CVS）
03/23	山形賴之（CVS）
04/04	Ron Bell（Institution of Electrical Engineers (IEE) and UK Health & Safety Executive (HSE)）
04/13	松本利雅（北陸先端科学技術大学院大学）
05/18	Olivier Danvy（BRICS, University of Aarhus, Denmark）
06/08	上出哲広（東京工業高等専門学校情報工学科）
06/15	大堀淳（東北大学　電気通信研究所）
06/22	林晋（京都大学大学院文学研究科）

（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/

◆ワークショップ 随時開催中

AIST/CVS Workshop on Shape Analysis and Program Analysis
2006 年月 04 日 07 日
（場所：システム検証研究センター千里サイト）
講演者
1. 小林直樹（東北大学）
2. 関浩之（奈良先端科学技術大学院大学）
3. Sagiv Mooly（Tel Aviv University）
4. 小川瑞史（北陸先端科学技術大学院大学）
5. 大崎人士（CVS）
6. 田辺良則（CVS）

2nd JAIST/AIST Joint Workshop on Verification Technology (VERITE) with guests from Chalmers　2006 年 05 日 19 日
（場所：システム検証研究センター千里サイト）
講演者
1. 青木利晃（北陸先端科学技術大学院大学）
2. Catarina Coquand（Chalmers University of Technology）
   Ulf Norell（Chalmers University of Technology）
3. Bengt Nordström（Chalmers University of Technology）
4. 西澤弘毅（CVS）
5. 岡本圭史（CVS）
6. René Vestergaard（北陸先端科学技術大学院大学）
7. Peter Dybjer（Chalmers University of Technology）
8. 緒方和博（北陸先端科学技術大学院大学）
9. 山形賴之（CVS）

直近のスケジュールはこちらから▼
URL：http://unit.aist.go.jp/cvs/workshop/Workshop-top.html

◆研修コース

2006 年 03 月 06 日～ 09 日
第 12 回モデル検査研修コース初級編（Spin）

2006 年 03 月 27 日～ 30 日
第 13 回モデル検査研修コース初級編（Spin）

2006 年 04 月 03 日～ 06 日
第 2 回対話型検証研修コース初級編

（場所：システム検証研究センター千里サイト）

研修コースの URL：
http//unit.aist.go.jp/cvs/training-course/training-course-top.html

出版

◆テクニカルレポート

2006 年 02 月発行
PS-2006-002　渡邊宏、西澤弘毅、高木理
"A Coalgebraic Representation of Reduction by Cone of Influence"

2006 年 04 月発行
PS-2006-003　Keishi Okamoto
"A First-Order Extension of Modal μ - calculus"

2006 年 05 月発行
PS-2006-004　Hiroki Takamura
"The variety of modal FLew-algebra is generated by its finite simple members"

2006 年 05 月発行
PS-2006-005　Toshinori Takai and Hitoshi Furusawa
"Monodic tree Kleene algebra (Preliminary Version)"

※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

◆書籍

「CVS 教程①　4 日で学ぶモデル検査（初級編）」
出版社：株式会社エヌ・ティー・エス

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