等式付木構造自動機械にもとづく自動検証器

（研究課題名：刺激応答型実時間システムの自動検証技術：安全性・信頼性技術の開発）

「機能と構成」領域　大崎 人士

要　旨

ネットワークプロトコルの安全性などを検査するには，検査対象の状態空間が有限にならないことがしばしば問題となります．時間制約を扱う場合や，送信するメッセージのデータ構造に着目する場合がこれに相当します．本研究では，ツリーオートマトンと書換系をもちいたモデル検査技法を開発しました．この方法を用いると，たとえモデルの状態空間が有限でなくとも，システムの自動検証が可能となります．実際に，本研究では，研究の理論的背景をもとに自動検証ツールACTASを開発して，具体的な検証問題を自動処理するための方法を検討しました．そこで本研究報告ではツリーオートマトンの理論にもとづく自動検証ツールについての成果と現状について述べます．

1．研究のねらい

高度情報化社会の基盤となる通信システムが安全かつ確実に動作することは，ますます重要になっています．銀行システム，電子商取引などの経済活動にとどまらず，交通システム，通信システムや国防システムにいたるまで，あらゆる場面で通信ネットワークの障害は社会生活に深刻な影響を及ぼします．インターネットのような，公衆ネットワーク回線を通じての通信においては，特に，暗号化による通信の秘密の保護が必要ですが，そこでは破られにくい暗号法の技術と共に，暗号化法を通信網の中で正しく生かして使う技術が必要です．例えば，正規の（想定する）データ受取人になりすまして，暗号を解くための鍵を不正に入手されるようでは，いかに破られにくい暗号法を使用していても，データの秘匿性を保つことはできません．つまり，鍵を不正に入手して暗号化されたデータを入手されるなどという攻撃を避けるための技術が要請されます．これを「通信手順の安全性」といいます．通信手順の安全性を確保することは，解読が困難な暗号化法を考案する技術とは独立のものです．なぜなら，秘密のデータを暗号化して受信者に伝えるとしても，暗号法には復号法が必ずあり（さもないと受信者はデータを読み取れない），復号化の方法も受信者に伝える必要があります．このときに，暗号化にもちいるトリック（多くの場合は，鍵）を横取りされないような通信手順が必要となるのです．ここで問題となるのは，「なりすまし」などの悪意の第三者からの攻撃が決して成功しないことをどのようにして確かめるのかです．

本研究では，情報科学における基礎技術を応用して，情報システムの安全性を検証するための技術について研究しました．具体的には，書換系およびツリーオートマトンの理論による数理的基礎を発展させて，リアクティブシステムの安全性を自動的に検証するための技術を開発し，実際に，自動検証ソフトウエアACTAS（「検証システム」と呼ぶ）を作成しました．

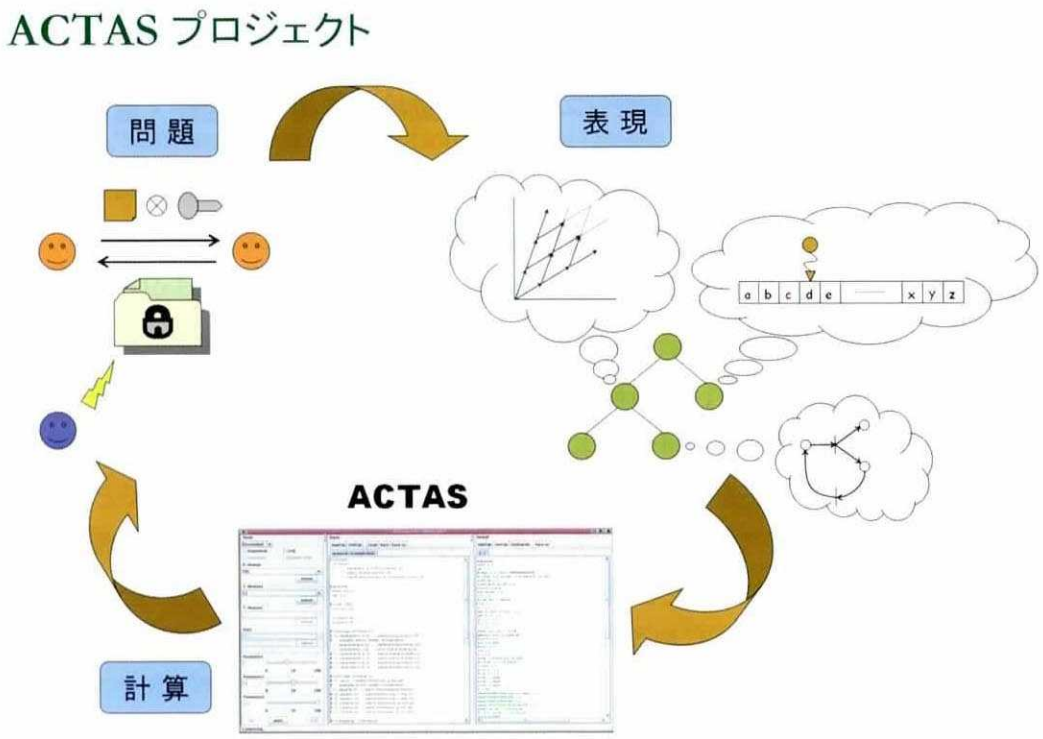


図1：ACTAS プロジェクト概念図

2．研究方法と成果

本研究の目的は，自動化の利点を損なわずに，柔軟な表現力をそなえたモデル化法とその自動検査技法を開発することです．例えば，より広いクラスの暗号通信プロトコルに対して，自然な表現によりモデル化し，安全性を自動的に検証する，ことを目指します．形式言語理論の世界では一般的に，「より強力な表現力を求めると，自動化の利点は失われる」と言われています．本研究の理論的基礎であるツリーオートマトンについても，この考察が当てはまります．従来のツリーオートマトンでは，自動検証に適した演算を構成的に定義することや，各種の決定判定問題を解消することはできますが，その表現力は必ずしも十分であるとは言えません．例えば，$x=y$ のような，線形方程式の（自然数上の）解空間を表現することができません．また，交換則（$x+y=y+x$）や結合則（$(x+y)+z=x+(y+z)$）を仮定すると，受理言語の閉包性（$t \in L$ かつ $t=t'$ ならば，$t' \in L$）が失われてしまいます．本研究では，従来のツリーオートマトンを拡張した新たな枠組みである等式付ツリーオートマトン（本稿タイトルでは，等式付木構造自動機械と記す）を理論的背景としました．そして，この新しい数理的なモデルについての閉包演算および決定問題の解決をしました．等式付ツリーオートマトンを基礎として，リアクティブシステムのための自動検証方法を考案し，現実的な時間で安全性を検証するためのアルゴリズムの開発や，近似計算アルゴリズムの開発などの研究も行いました．本研究（ACTAS プロジェクトと呼ぶ）の概念図を図1に示します．以降の節では，本研究プロジェクトで得られた研究成果をまとめて述べます．

２．１　表現についての研究

本研究者（大崎人士）は，2001年に世界にさきがけて，**等式付ツリーオートマトン**という理論概念を導出しました．等式付ツリーオートマトンは，交換則や結合則を仮定しても受理言語の閉包性を失うことはありません．しかも，従来のツリーオートマトンのように：

- 空（くう）判定問題が決定可能であること
- 受理言語上の集合演算について閉じていること

が多くの場合で成り立つことがわかりました．　具体的には，(1)交換則・結合則を仮定するか，結合則のみを仮定するか，(2)正則な遷移規則のみをもつと仮定するか，正則な遷移規則に加えて単調な（monotone）イプシロン遷移規則をもつと仮定するか，の場合分けにより，表現力に違いが生じます．そこで，それぞれの場合についての性質を調べました．次頁の図２と図３に成果の一覧をまとめます．PRESTO（さきがけ）の研究プログラム期間中には，理論概念の導出以来の未解決の問題とされていた，交換則結合則付き単調ツリーオートマトン（monotone AC-tree automata）についての以下の定理を導くことができました：　交換則結合則付単調ツリーオートマトンの受理言語のクラスは，

1. 交換則結合則付正規ツリーオートマトンの受理言語のクラスを，真に包含している，
2. 補集合の演算について閉じていない，
3. 包含関係（⊆）の判定問題が決定不可能である．

いっぽう，等式付ツリーオートマトンによる自動検証の可能性を理論的に裏付けるためには，空判定問題が決定可能になるための十分条件を調べることが，一つの重要なカギとなります．アルゴリズム実装のためには，空判定の計算量を測定することも必要です．空判定が，計算量的に実装がむずかしい場合であっても，近似判定法があるかどうかを検討することにより，多くの具体的な検証例を手がけることも可能になります．本研究では，上述(1)と(2)の場合分けのすべて対して，空判定についての考察をおこないました．そしてこの考察をもとに，結合則と交換則をうまく扱うことのできなかった従来の理論では秘密保持性の自動検証が難しいとされていた「Diffie-Hellmanの鍵交換プロトコル」や「Shamirのスリーパス・プロトコル」を使う暗号通信手順が，等式付ツリーオートマトンによる自動検証の対象に含められることを示すことができました．

理論的な研究成果のさらに詳しい解説は省略しますが，詳細につきましては，本報告書の最後にある研究成果一覧をご覧ください．また近年，等式付ツリーオートマトンに関する研究が，世界的な広がりをみせています．最新の研究成果はおもに以下の国際研究集会などで報告されています：

- International Conference on Rewriting Techniques and Applications（RTA）
- International Conference on Logic for Programming, Artificial Intelligence and Reasoning (LPAR)
- International Conferences on Foundations of Software Sciences and Computer Structures (FOSSACS)

いずれの会議も，会議録がSpringer-Verlag社のLNCSシリーズとして出版されています．

Closure under Boolean operations

	regular	AC-regular	AC-monotone
closed under $\cup$	✓	✓	✓
closed under $\cap$	✓	✓	✓
closed under $(\ )^c$	✓	✓	×

regular TA $<$ regular AC-TA $<$ monotone AC-TA

	regular	A-regular	A-monotone
closed under $\cup$	✓	✓	✓
closed under $\cap$	✓	×	✓
closed under $(\ )^c$	✓	×	✓

regular TA $<$ regular A-TA $<$ monotone A-TA

図2：ブール閉包性とツリー言語階層 §

Decidability results

	regular	AC-regular	AC-monotone
$t \in \mathcal{L}(\mathcal{A}/\mathrm{AC})$?	✓ (LOGCFL)	✓ (NP-complete)	✓ (PSPACE-compl.)
$\mathcal{L}(\mathcal{A}/\mathrm{AC}) = \emptyset$?	✓	✓	✓
$\mathcal{L}(\mathcal{A}/\mathrm{AC}) \subseteq \mathcal{L}(\mathcal{B}/\mathrm{AC})$?	✓	✓	×

	regular	A-regular	A-monotone
$t \in \mathcal{L}(\mathcal{A}/\mathrm{A})$?	✓ (LOGCFL)	✓ (P-time)	✓ (PSPACE-compl.)
$\mathcal{L}(\mathcal{A}/\mathrm{A}) = \emptyset$?	✓	✓	×
$\mathcal{L}(\mathcal{A}/\mathrm{A}) \subseteq \mathcal{L}(\mathcal{B}/\mathrm{A})$?	✓	×	×

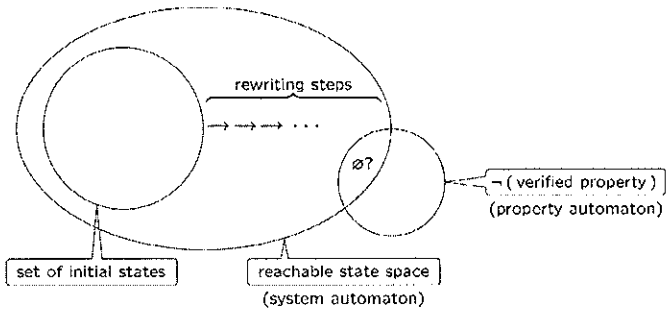
図3：決定可能性と計算量 §

§ PRESTO 実施中に得られた成果は青色で示します.

2．2　自動計算についての研究

等式付ツリーオートマトンの理論を生かしたシステム開発をすることにより，検証の自動化についての検討を行いました．本研究で開発したのは，結合則交換則付ツリーオートマトンを入力として，各種の演算や判定問題の解消を行うためのシステムです．オートマトンの基本的な演算である，共通集合や和集合（∪，∩），所属判定や空判定（∈，$\neq\varnothing$）の機能を備えていることから，ACTAS（Associative Commutative Tree Automata Simulator）と命名しました．さらにACTASでは，結合則交換則付ツリーオートマトンAと結合則交換則書換系Rを与えて，Aの受理言語のRによる書換閉包を受理する結合則交換則付ツリーオートマトンを求めることもできます．図4は，実際にACTASで書換閉包を計算したときに表示されるインターフェース画面です．

書換系とは，書換規則の有限集合で，書換規則は項の順序対です．書換規則は，$l\to r$と書き，lを左辺，rを右辺と呼びます．結合則・交換則を仮定した関数記号を含む書換系を結合則交換則付書換系と呼びます．項tと書換規則$l\to r$が与えられたときに，tの中にlのパターンにマッチする部分項が存在したとき，その部分項はrに置き換えられ，この関係を書換関係と呼びます．項tから項t'に項書換え系Rに含まれる規則で書換えられるとき，$t\to_R t'$と書きます．また，tから0回以上の書換えでt'に到達するとき，$t\to_R^* t$と書きます．結合則交換則付ツリーオートマトンは，結合則交換則付書換系の特殊なクラスとみなすことができることから，書換系とツリーオートマトンは，理論的な親和性がよく，書換系の研究成果をツリーオートマトンへ応用することも容易です．このため，ツリーオートマトンの各種演算や問題解消系を利用して，書換閉包を計算することができます．ツリーオートマトンAの受理言語をLと表すとき，LのRによる書換え閉包というのは，Lに含まれる項からRによって書換えて得られる項全てからなる集合で，$\{t\mid s\to_R^* t, s\in L\}$です．しかし書換閉包を計算手続きは，一般に停止性を保証することはできません．そこで，ACTASでは結合則交換則付ツリーオートマトンAと結合則交換則書換系Rを与えられたときに，(1) Aの受理言語のRによる書換閉包，(2) Aの受理言語のRによる書換閉包を含む集合（強近似書換閉包），(3) Aの受理言語のRによる書換閉包に含まれる集合（弱近似書換閉包）のいずれを計算するのか，を選択することができます．特に，弱近似を行うアルゴリズムでは，いくつかのパラメータを指定することで，現実的な時間で計算の実行を終了させることができます．　書換閉包の計算と同様に，空判定も弱近似判定や強近似判定が可能です．これらの機能を組み合わせて，モデル検査を実現します．書換閉包計算にもとづくモデル検査についての概念図は以下の通りです：



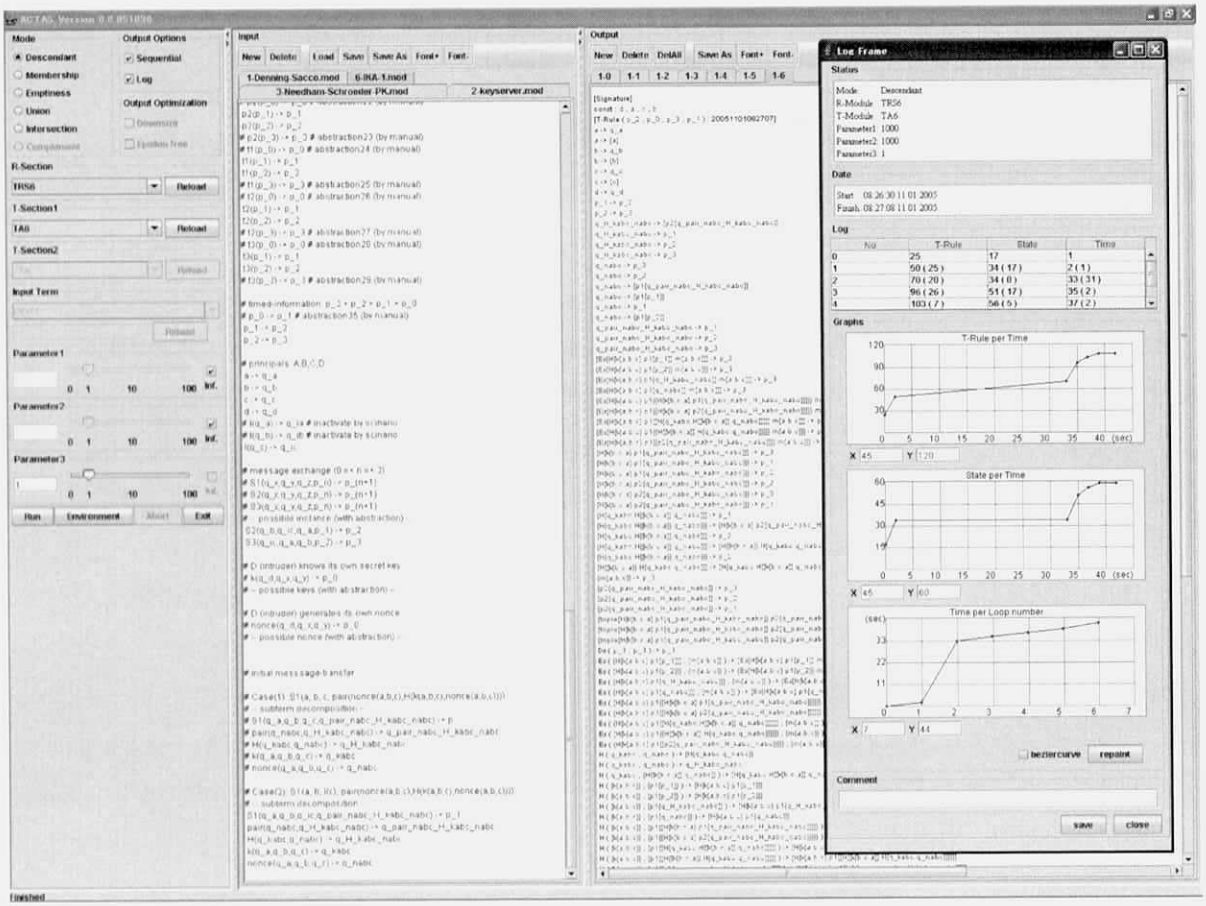


図4：ACTASインターフェース

本稿では詳しい解説を省略しますが，技術的な記述については[論文(国際研究集会) 2]をご参照ください.

3．今後の展望

本研究中に開発した暗号通信手順の安全性自動検証法は，リアクティブシステムと呼ばれる「動作中に外界からの多様な刺激を受けて，その刺激と内部状態から応答を決定する」装置全般に適用可能です. このタイプのシステムは, 銀行のオンラインシステムや携帯電話等の通信システムなど，いちど稼働させてしまうと容易に停止することが出来ないことが特徴です．安全で安定した情報システムの整備が, 社会的な急務となっている現在, 稼働前に十分な安全性の検証をおこなうことは，社会的ニーズでもあります．また，大規模システムやマスプロダクトに対しては，検証で発見された誤りにより設計変更を余儀なくされた場合に，損失を極力小さく抑える必要があるため，設計の初期段階で検証できなければならないという要求もあります．これは，携帯電話などの組込みプログラムが問題を含んでいる場合，その問題発見が遅れると莫大な製品回収コストを要することが一因しています．しかし，リアクティブシステムを単純に遷移系としてモデル化すると，しばしば状態空間が無限となり，従来のモデル検査法は無力です．このため，本研究で開発したツリーオート

マトン理論にもとづく自動検証技術は，今後，暗号通信手順の安全性検証にとどまらず，例えば，携帯電話のようなライフスパンが短いマスプロダクトに対して，予想外の製造コスト（欠陥製品の回収コストなど）が発生する割合を減らして，製品の製造コストを削減することに役立たせることなどに生かせると考えています．

謝　辞

PRESTO（さきがけ）の研究プログラムで実施した私の研究は，いずれもACTASプロジェクトの中核をなす重要な研究テーマです．本件研究を遂行するためには，個人研究テーマではありますが，外部の研究協力者による多くの力添えをいただきました．この場をお借りして御礼申し上げます．また，片山卓也研究総括，領域アドバイザーの先生がたからの辛口のコメントも研究の励みになりましたこと，ここにご報告いたします．最後に，独立行政法人科学振興機構のみなさま，「機能と構成」領域事務所の橋本久雄さん，生田雅一さん，小川龍太郎さん（前任者）には，大変なご助力をいただきました．厚く御礼申し上げます．

4．成果リスト

論　文（国際研究集会）

1. 大崎人士，Jean-Marc Talbot，Sophie Tison，Yves Roos：“Monotone AC-Tree Automata”. In proceedings of 12th International Conference on Logic for Programming, Artificial Intelligence and Reasoning (LPAR'05), Montego Bay (Jamaica). Lecture Notes in Computer Science, Springer-Verlag (2005年12月発表予定).

2. 大崎人士，高井利憲：“ACTAS: A System Design for Associative and Commutative Tree Automata Theory”.
   In proceedings of 5th International Workshop on Rule-Based Programming (RULE'04), Electronic Notes in Theoretical Computer Science, 124巻，97—111頁，Elsevier Science, 2005.

3. 大崎人士，関浩之，高井利憲：“Recognizing Boolean Closed A-Tree Languages with Membership Conditional Rewriting Mechanism”.
   In proceedings of 14th International Conference on Rewriting Techniques and Applications (RTA'03), Lecture Notes in Computer Science, 2706巻，483—498頁，Springer-Verlag, 2003.

4. 大崎人士，高井利憲：“Equational Tree Automata: Towards Automated Verification of Network Protocols”.
   京都大学数理解析研究所講究録，1318号，48—52頁，京都大学，2003.

5. 大崎人士，高井利憲：“Decidability and Closure Properties of Equational Tree Languages”. In proceedings of 13th International Conference on Rewriting Techniques and Applications (RTA'02), Lecture Notes in Computer Science, 2378巻，114—128頁，Springer-Verlag, 2002.

論　文（その他）

6. 大崎人士，Joe Hendrix，José Meseguer：“Sufficient Completeness Checking with Propositional Tree Automata”.
産業技術総合研究所研究速報 AIST-PS-2005-013，産業技術総合研究所，2005.

システム紹介

7. 大崎人士，高井利憲：“ACTAS: Associative and Commutative Tree Automata Simulator”. 4th International Conference on Application of Concurrency to System Design（ACSD'04), 2004.

研究交流

8. Université des Sciences et Technologies de Lille（リール・フランス），招聘講師，(2005年5月21日－6月15日).

9. École Normale Supérieure de Cachan（パリ・フランス），招聘教授，(2004年8月28日－9月30日).

10. University of Illinois at Urbana-Champaign（アーバナ・イリノイ州），招聘研究員，(2004年1月10日－3月31日).

11. 京都大学数理解析研究所（京都），特別講師，(2004年7月26日－7月30日).

外部委員

12. Program Committee Member : 18th International Workshop on Unification（UNIF'04), Cork（Ireland），(2004年7月開催).

13. Program Committee Member : 16th International Conference on Rewriting Techniques and Applications （RTA'05)，奈良市，(2005年4月開催).

14. Organizing Chair : 16th International Conference on Rewriting Techniques and Applications （RTA'05)，奈良市，(2005年4月開催).

15. Conference Co-Chair : Federated Conference on Rewriting, Deduction and Programming （RDP'05)，奈良市，(2005 年4月開催).

など.