Graph-Embedded Rewrite Systems: Combination and Undecidability Results

Serdar Erbatur [1] Andrew M. Marshall [2]
Paliath Narendran [3] Christophe Ringeissen [4]

[1]University of Texas at Dallas, Dallas, USA

[2]University of Mary Washington, Fredericksburg, USA

[3]University at Albany and SUNY, Albany, USA

[4]Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France

FroCoS 2025

Protocol Analysis

Protocol analysis based on the Dolev-Yao intruder model: successful approach, with a number of tools for checking various security properties of protocols.

See for example [AC06, AFN17, CCcCK16, cCDK12, DDKS17]

Standard problem to many of these symbolic methods: determine what a potential “intruder” can learn from the exchange of messages during the run of a protocol.

That is, analyse the *intruder knowledge*.

Two Notions of Knowledge

Two decision problems in modeling intruder knowledge, where the intruder capabilities is specified by an equational theory E:

1. Deduction Problem: given a sequence of messages M and a message t, can we deduce/compute t from M?

   Is there a recipe s such that $s\sigma_M =_E t$?
   written $\sigma_M \vdash_E t$ if this holds

2. Static Equivalence: given two sequences of messages M_1 and M_2, can we distinguish an instance of a protocol running M_1 from one running M_2?

   Is there no recipe equation $s = t$ such that $s\sigma_{M_i} =_E t\sigma_{M_i}$ and $s\sigma_{M_j} \neq_E t\sigma_{M_j}$ for $i \neq j$?
   written $\sigma_{M_1} \approx_E \sigma_{M_2}$ if this holds

NB: in recipes, private constants are forbidden

Knowledge Decidability

The knowledge problems are undecidable in general. However, for many equational theories modeling various protocols, decision procedures are known. For example:

- Blind signatures
- Trap-door commitments
- Malleable encryption
- Theory of addition
- Encryption/decryption

Many of these theories can be modeled via subterm convergent term rewrite systems (TRSs), where the right-hand side of any rule is either a constant or a subterm of the left-hand side.

The knowledge problems are decidable for the class of subterm convergent TRSs, see [AC06].

Non-subterm Convergent

The decision procedures designed for subterm convergent TRSs also work for convergent TRSs that are "beyond subterm".

Example: Blind signatures

Subterm:

$$\begin{aligned} open(commit(x, y), y) &\to x, \\ getpk(host(x)) &\to x, \\ checksign(sign(x, y), pk(y)) &\to x, \\ unblind(blind(x, y), y) &\to x, \end{aligned}$$

Non-subterm:

$$unblind(sign(blind(x, y), z), y) \to sign(x, z)$$

Beyond Subterm: Borrow From Graph Theory

Develop a, hopefully simple, definition that extends the subterm convergent definition and encompasses the "beyond subterm" examples?

Borrow some ideas from graph theory, such as edge contraction, to introduce a rule schema, R_{gemb} :

For any $f \in \Sigma$
(1) $f(x_1, \ldots, x_n) \rightarrow x_i$

(2) $f(x_1, \ldots,\ x_{i-1},\ x_i,\ x_{i+1}\ \ldots,\ x_n) \rightarrow f(x_1, \ldots,\ x_{i-1},\ x_{i+1},\ \ldots,\ x_n)$

For any $f, g \in \Sigma$
(3) $f(x_1, \ldots, x_{i-1}, g(\bar{z}), x_{i+1},\ \ldots, x_m) \rightarrow g(x_1, \ldots, x_{i-1}, \bar{z}, x_{i+1}, \ldots, x_m)$

(4) $f(x_1, \ldots, x_{i-1}, g(\bar{z}), x_{i+1}, \ldots, x_m) \rightarrow f(x_1, \ldots, x_{i-1}, \bar{z}, x_{i+1}, \ldots, x_m)$

Graph-embedded TRS

A term t' is *graph-embedded* in a term t if $t \rightarrow^*_{R_{gemb}} s \approx t'$ where

- s is well-formed,
- $s \approx t'$ represents equality modulo an appropriate form of permutation (extending leaf permutation)

A TRS R is *graph-embedded* if for any $l \rightarrow r \in R$, r is graph-embedded in l, or r is a constant.

Example: Blind signatures

$$\begin{aligned} & unblind(sign(blind(x,y),z),y) \\ \rightarrow^{(1)}\ & sign(blind(x,y),z) \\ \rightarrow^{(4)}\ & sign(x,y,z) \\ \rightarrow^{(2)}\ & sign(x,z) \end{aligned}$$

Knowledge Problems in Graph-embedded TRSs

Theorem ([SEMR23])

There exists a graph-embedded convergent TRS where deduction is undecidable.

Theorem ([SEMR23])

There exists a subclass of graph-embedded convergent systems, called **contracting** *convergent systems, for which any system in that subclass has decidable deduction and static equivalence.*

Proof idea: In a contracting TRS, it is possible to get a property called local stability [AC06] implying decidability of both deduction and static equivalence.

In a contracting TRS, the right-hand sides are of depth at most 2, and it includes *projecting* rules, where a *projecting* rule is a rule of the form $\ell[x] \to x$.

New Undecidability Results: Static Equivalence

What happens beyond contracting?

Theorem

Static equivalence becomes undecidable for contracting TRSs without the depth restriction on the right-hand sides.

Proof idea:

- Adapt a TRS encoding of LBA initiated to show undecidability of static equivalence in permutative theories [EMNR24],
- consider additional projecting rules to get an encoding based now on a TRS which is almost contracting, except the depth restriction.

New Undecidability Results: Deduction

What happens beyond contracting?

Theorem

Deduction is undecidable for rule (4) graph-embedded TRSs.

Proof idea: reuse a TRS encoding of a modified PCP initially used to show the undecidability of deduction in homeomorphic-embedded TRSs [SEMR23, BSE+24].

Theorem

Deduction is undecidable for rule (3) graph-embedded TRSs.

Proof idea: Encoding a modified PCP as a deduction problem modulo a rule (3) graph-embedded TRS, using a binary symbol f to represent strings, e.g., $f(a, f(b, c))$ represents abc.

New Combination Results

Initial result:

Theorem ([AC06])

Deduction and Static Equivalence are decidable in any subterm convergent TRS.

New combination result:

Theorem

Deduction and Static Equivalence are decidable in an equational theory $R \cup E$ where (R, E) is any equational TRS such that

- *R is contracting E-convergent,*
- *E is a permutative theory closed by paramodulation*

Proof idea: Same reduction approach as in [EMR20] where R is assumed to be subterm E-convergent.

Reduction for Deduction

Lemma (Deduction)

Let E be any syntactic permutative theory and R any contracting E-convergent TRS such that $|R|$ is defined. For any normalized substitution ϕ and any normalized term t, we have that

$$\phi \vdash_{R \cup E} t \text{ if and only if } \phi_* \vdash_E t$$

where ϕ_* denotes the (computable) completion of ϕ.

Remark: the computation of ϕ_* requires the guessing of terms of size at most $|R|$, where $|R|$ is defined if E is a permutative theory closed by paramodulation.

Reduction for Static Equivalence

Lemma (Static Equivalence)

Let E be any syntactic permutative theory and R be any contracting E-convergent TRS such that $|R|$ is defined. For any normalized substitutions ϕ and ψ, we have

$$\phi \approx_{R \cup E} \psi \text{ iff } \bar{\psi} \models_{R \cup E} Eq(\bar{\phi}) \text{ and } \bar{\phi} \models_{R \cup E} Eq(\bar{\psi}) \text{ and } \bar{\phi} \approx_E \bar{\psi}$$

where

- *$\bar{\phi}$ (resp., $\bar{\psi}$) is the (computable) recipe-based completion of ϕ (resp., ψ)*
- *$Eq(\bar{\phi})$ (resp., $Eq(\bar{\psi})$) is a (computable) finite set of recipe equations for $\bar{\phi}$ (resp., $\bar{\psi}$) obtained by guessing terms of size at most $|R|$*
- *$\theta \models_{R \cup E} Eq$ denotes that for any $t = t' \in Eq$, $t\theta =_{R \cup E} t'\theta$*

Concluding Remarks

Undecidability results: going beyond contracting TRSs is difficult.

Decidability results: combinations of contracting TRSs and (simple) permutative theories.

Open problem: How to consider Associativity-Commutativity (AC) and rewriting modulo AC?

References I

Martín Abadi and Véronique Cortier, *Deciding knowledge in security protocols under equational theories*, Theor. Comput. Sci. **367** (2006), no. 1-2, 2–32.

Mauricio Ayala-Rincón, Maribel Fernández, and Daniele Nantes-Sobrinho, *Intruder deduction problem for locally stable theories with normal forms and inverses*, Theor. Comput. Sci. **672** (2017), 64–100.

Carter Bunch, Saraid Dwyer Satterfield, Serdar Erbatur, Andrew M. Marshall, and Christophe Ringeissen, *Knowledge problems in protocol analysis: Extending the notion of subterm convergent*, CoRR **abs/2401.17226** (2024).

Rohit Chadha, Vincent Cheval, Ştefan Ciobâcă, and Steve Kremer, *Automated verification of equivalence properties of cryptographic protocols*, ACM Trans. Comput. Log. **17** (2016), no. 4, 23:1–23:32, Available as Research Report at https://hal.inria.fr.

Ştefan Ciobâcă, Stéphanie Delaune, and Steve Kremer, *Computing knowledge in security protocols under convergent equational theories*, J. Autom. Reasoning **48** (2012), no. 2, 219–262.

Jannik Dreier, Charles Duménil, Steve Kremer, and Ralf Sasse, *Beyond subterm-convergent equational theories in automated verification of stateful protocols*, Principles of Security and Trust (Berlin, Heidelberg) (Matteo Maffei and Mark Ryan, eds.), Springer Berlin Heidelberg, 2017, pp. 117–140.

Serdar Erbatur, Andrew M. Marshall, Paliath Narendran, and Christophe Ringeissen, *Deciding knowledge problems modulo classes of permutative theories*, Logic-Based Program Synthesis and Transformation - 34th International Symposium, LOPSTR 2024, Milan, Italy, September 9-10, 2024, Proceedings (Juliana Bowles and Harald Søndergaard, eds.), Lecture Notes in Computer Science, vol. 14919, Springer, 2024, pp. 47–63.

References II

Serdar Erbatur, Andrew M. Marshall, and Christophe Ringeissen, *Computing knowledge in equational extensions of subterm convergent theories*, Math. Struct. Comput. Sci. **30** (2020), no. 6, 683–709.

Saraid Dwyer Satterfield, Serdar Erbatur, Andrew M. Marshall, and Christophe Ringeissen, *Knowledge problems in security protocols: Going beyond subterm convergent theories*, 8th International Conference on Formal Structures for Computation and Deduction, FSCD 2023, July 3-6, 2023, Rome, Italy (Marco Gaboardi and Femke van Raamsdonk, eds.), LIPIcs, vol. 260, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023, pp. 30:1–30:19.