

モデル検査と型推論

高階モデル検査における両者の等価性をめぐるサーベイ

概要

「モデル検査を使った型推論の論文はあるか」という問いに答える。結論を先に述べると、**ある**。ただし予想される形とは違う。モデル検査を型推論の道具として**使う**のではなく、両者が**同じ問題**であることが示されている。高階再帰スキームのモデル検査は交差型の型検査と等価であり (Kobayashi–Ong, LICS 2009)、この等価性が高階関数プログラム検証の実用的なアルゴリズムを生んだ。一方で、Hindley–Milner 型推論そのものにモデル検査を適用した研究は見当たらない。本稿はこの分野の主要論文を辿り、なぜそうなるかを述べる。掲載する書誌はすべて DBLP で実在を確認した。

目次

1	問いの整理	1
2	等価性の発見	1
2.1	出発点: 高階再帰スキームの決定可能性	1
2.2	交差型による定式化	2
2.3	等価性の一般化	2
2.4	型システムの側の展開	2
3	等価性を実装に変える	3
3.1	アルゴリズム	3
3.2	プログラム検証への適用	3
3.3	無限データ領域への拡張: 述語抽象と CEGAR	3
4	型推論との直接の結合	3
5	型解析とモデル検査の併用	4
6	Hindley–Milner にモデル検査は使われていない	4
7	全体像	5
8	読む順序	5
9	本稿の限界	6

1 問いの整理

「モデル検査を使って型推論」という言い方には、少なくとも三つの読み方がある。

1. **型推論アルゴリズムをモデル検査で検証する。** 型推論の実装が正しいことをモデル検査器で確かめる。
2. **モデル検査を型推論の道具として使う。** 型を求める過程でモデル検査器を呼ぶ。
3. **モデル検査と型推論が同じ問題である。** 一方を他方に還元する。

文献を当たると、実質的な蓄積があるのは第三の読み方であり、そこから第二の読み方が派生している。第一の読み方については、少なくとも Hindley–Milner の文脈では見当たらない。理由は第 6 節で述べる。

2 等価性の発見

2.1 出発点: 高階再帰スキームの決定可能性

高階再帰スキーム (higher-order recursion scheme、以下 HORS) は、単一の無限木を生成する一種の木文法である。プログラミング言語の側から見れば、再帰と木構成子を持つ名前呼びの単純型付きラムダ計算の項にあたる。

C.-H. Luke Ong. *On Model-Checking Trees Generated by Higher-Order Recursion Schemes*. LICS 2006.

Ong は、HORS が生成する木のモナディック二階述語論理 (MSO) による性質検査が**決定可能**であることを示した。これが分野の出発点である。ただしこの証明はゲーム意味論に基づいており、そのままでは実装できるアルゴリズムを与えなかった。

2.2 交差型による定式化

Naoki Kobayashi. *Types and higher-order recursion schemes for verification of higher-order programs*. POPL 2009.

Kobayashi は、HORS のモデル検査を**交差型の型検査**として定式化し直した。安全性 (trivial automata で表せる性質) については、性質 φ から交差型システムを構成し、

$$G \text{ の生成する木が } \varphi \text{ を満たす} \iff G \text{ がその型システムで型付く}$$

が成り立つ。ゲーム意味論を経由しない、型理論の言葉による特徴づけである。

2.3 等価性の一般化

Naoki Kobayashi and C.-H. Luke Ong. *A Type System Equivalent to the Modal Mu-Calculus Model Checking of Higher-Order Recursion Schemes*. LICS 2009.

本稿の問いに対する中心的な答えがこれである。上の対応が、安全性に留まらず**モーダル μ 計算**の全体に拡張された。 μ 計算の論理式に対応する交差型システムが構成され、モデル検査問題と型付け可能性が等価であることが示されている。

この時点で「モデル検査を型推論で解く」と「型推論をモデル検査で解く」は、同じ命題の言い換えになる。分野が第三の読み方に落ち着いたのは、この結果による。

同じ二人による計算量の解析もある。

Naoki Kobayashi and C.-H. Luke Ong. *Complexity of Model Checking Recursion Schemes for Fragments of the Modal Mu-Calculus*. ICALP 2009 / Logical Methods in Computer Science 2011.

2.4 型システムの側の展開

等価性が確立すると、型システムを広げることがモデル検査の対象を広げることになる。

Takeshi Tsukada and Naoki Kobayashi. *Untyped Recursion Schemes and Infinite Intersection Types*. FoSSaCS 2010.

Naoki Kobayashi and Atsushi Igarashi. *Model-Checking Higher-Order Programs with Recursive Types*. ESOP 2013.

前者は無限交差型により型無し再帰スキームへ、後者は再帰型を持つプログラムへ対象を広げる。いずれも「型システムを設計し、その型検査がモデル検査に等価であることを示す」という同じ筋で進む。

3 等価性を実装に変える

3.1 アルゴリズム

等価性そのものは決定手続きを与えるが、素朴に実装すると型の候補が爆発する。実用的なアルゴリズムは、木を部分的に構成しながら交差型を推測する形をとる。

Naoki Kobayashi. *A Practical Linear Time Algorithm for Trivial Automata Model Checking of Higher-Order Recursion Schemes*. FoSSaCS 2011.

問題自体は n 階で n 重指数時間完全であるにもかかわらず、実際のプログラムから生じる入力では線形に近く振る舞う、という主張である。これが実装可能性を開いた。

3.2 プログラム検証への適用

Naoki Kobayashi, Naoshi Tabuchi, and Hiroshi Unno. *Higher-order multi-parameter tree transducers and recursion schemes for program verification*. POPL 2010.

3.3 無限データ領域への拡張: 述語抽象と CEGAR

HORS は有限のアルファベット上の木しか扱えない。整数など無限のデータを持つプログラムを扱うには抽象化が要る。

Naoki Kobayashi, Ryosuke Sato, and Hiroshi Unno. *Predicate abstraction and CEGAR for higher-order model checking*. PLDI 2011.

有限状態やプッシュダウンのモデル検査で確立していた述語抽象と CEGAR (counterexample-guided abstraction refinement、反例に導かれた抽象化の洗練) を、高階のブールプログラムと再帰スキームへ持ち込んだ仕事である。これにより整数を扱う高階関数プログラムの自動検証器が現実のものになった。

抽象化の洗練は、その後も別の角度から追究されている。

Naoki Kobayashi and Xin Li. *Automata-Based Abstraction Refinement for μ HORS Model Checking*. LICS 2015.

Xin Li and Naoki Kobayashi. *Equivalence-Based Abstraction Refinement for μ HORS Model Checking*. ATVA 2016.

4 型推論との直接の結合

ここまでは「モデル検査 = 型検査」であった。第二の読み方、すなわちモデル検査を型推論の道具として使う仕事も現れる。

Ryosuke Sato, Naoki Iwayama, and Naoki Kobayashi. *Combining higher-order model checking with refinement type inference*. PEPM (POPL 併設) 2019.

精製型 (refinement type) の推論と高階モデル検査を組み合わせる。精製型推論は述語を含む型を求める問題であり、その求解にモデル検査を使う。逆向きに、モデル検査の前段として精製型推論で問題を小さくする、という使い方もされる。本稿の問いに文字どおり答える論文としては、これが最も近い。

同じ流れで、論理式の側を型で解くものもある。

Youkichi Hosoi, Naoki Kobayashi, and Takeshi Tsukada. *A Type-Based HFL Model Checking Algorithm*. APLAS 2019.

高階不動点論理 (HFL) の検証を型に基づくアルゴリズムで行う。

5 型解析とモデル検査の併用

等価性とは別の、より素朴な組み合わせもある。

Hiroshi Unno, Naoki Kobayashi, and Akinori Yonezawa. *Combining type-based analysis*

and model checking for finding counterexamples against non-interference. PLAS 2006.

情報流の非干渉性について、型に基づく解析が「安全と言えない」と答えたときに、モデル検査で実際の反例を探す。型システムは健全だが完全ではないので、拒否された理由が本物の欠陥なのか解析の粗さなのかが分からない。その判別にモデル検査を使う、という役割分担である。

6 Hindley–Milner にモデル検査は使われていない

文献を当たった範囲では、**Hindley–Milner 型推論そのものにモデル検査を適用した論文は見つからなかった**。無い理由は明快で、次の二点に尽きる。

■**HM は単一化で解ける**。HM の型推論は制約生成と単一化に還元され、和集合素集合データ構造を使えばほぼ線形時間で解ける。決定手続きが既にあり、しかも安価な問題に、状態空間探索を持ち込む動機がない。

■**モデル検査が要るのは型が決定不能に近づくときである**。交差型の型推論は一般には決定不能であり、精製の推論は述語の探索を伴う。高階モデル検査が登場するのは、まさにそうした**難しい型システム**においてである。第 6 節の主題に即して言えば、モデル検査と型推論が出会うのは型システムが十分に表現力を持ったときであって、HM はその手前にいる。

なお、HM 型推論の**正しさ**を機械検証する研究は多数あるが、そこで使われるのはモデル検査ではなく定理証明器である。本リポジトリの `HMSoundness.v` と `HMTypedSafety.v` もその系統に属する。

7 全体像

年	論文	会議	位置づけ
2006	Ong	LICS	HORS の MSO 検査が決定可能
2006	Unno–Kobayashi–Yonezawa	PLAS	型解析とモデル検査の併用
2009	Kobayashi	POPL	安全性を交差型で特徴づけ
2009	Kobayashi–Ong	LICS	μ 計算との等価性
2009	Kobayashi–Ong	ICALP	計算量
2010	Tsukada–Kobayashi	FoSSaCS	無限交差型
2010	Kobayashi–Tabuchi–Unno	POPL	木変換器への拡張
2011	Kobayashi	FoSSaCS	実用的アルゴリズム
2011	Kobayashi–Sato–Unno	PLDI	述語抽象と CEGAR
2013	Kobayashi–Igarashi	ESOP	再帰型
2015	Kobayashi–Li	LICS	自動機械による抽象化洗練
2016	Li–Kobayashi	ATVA	等価性に基づく抽象化洗練
2019	Sato–Iwayama–Kobayashi	PEPM	精製型推論との結合
2019	Hosoi–Kobayashi–Tsukada	APLAS	HFL の型に基づく検査

太字の三本が、本稿の問いに直接答えるものである。等価性を確立した Kobayashi–Ong 2009、それを無限データへ広げた Kobayashi–Sato–Unno 2011、そして型推論と明示的に組み合わせた

Sato–Iwayama–Kobayashi 2019 である。

8 読む順序

初めて触れる場合は、次の順を勧める。

1. Kobayashi, POPL 2009。安全性に限れば議論が追いやすく、交差型による特徴づけの核心が見える。
2. Kobayashi–Ong, LICS 2009。等価性の全体像。
3. Kobayashi–Sato–Unno, PLDI 2011。理論が実装に変わる箇所。
4. Sato–Iwayama–Kobayashi, PEPM 2019。型推論との結合。

概観としては次も便利である。

Naoki Kobayashi. *Higher-Order Model Checking: From Theory to Practice*. LICS 2011.
<https://www-kb.is.s.u-tokyo.ac.jp/~koba/papers/lics2011.pdf>

Naoki Kobayashi. *Model Checking Higher-Order Programs*. Journal of the ACM, 2013.
<https://dl.acm.org/doi/10.1145/2487241.2487246>

9 本稿の限界

書誌はすべて DBLP の著者レコードから機械的に抽出し、題名・著者・会議・年を確認した。ただし各論文の内容についての記述は、要旨と二次資料に基づくものであり、全文を精読した結果ではない。技術的な細部を引用する際は原典に当たられたい。

また、検索は Kobayashi と Ong を中心に行った。両者がこの分野の中心であることは確かだが、網羅的なサーベイではない。特に、型システムと自動機械の対応を扱う他の系統（例えば型状態解析やセッション型と検証の関係）は範囲外である。