IA-002

【既発表論文紹介】

Stateful Manifest Contracts

関山 太朗† 五十嵐 淳‡

Taro Sekiyama Atsushi Igarashi

出典：The 44th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2017), pp. 530–544

本講演では国際会議 POPL 2017 にて発表した、顕在的契約計算 (manifest contracts) に命令型プログラミングの基本機能であるプログラム状態変更（メモリ操作）機構を導入した研究について発表する。顕在的契約計算ではプログラムの仕様をプログラミング言語で記述した述語（ソフトウェア契約）を篩型(refinement type)と呼ばれる型に与えることで表現する。一般にプログラムが任意の述語を満たすかは決定不能であるため、顕在的契約計算ではプログラムが篩型に書かれた述語を満たすことが静的に決定できないような場合、その述語の検査を実行時に行うハイブリッド検査によって仕様の検査を行う。これによりプログラミング言語で記述された表現力の高い仕様を許容しつつ、実際のプログラム開発におけるプログラムの静的検査が難しい状況に対処することを目指している。

我々はこれまでの純粋関数型プログラミングだけが可能であった顕在的契約計算に対し、命令型プログラミングの基本機能である状態変化機構を導入した。ここで問題となるのはプログラム状態に依存した述語の存在である。これまでの顕在的契約計算の型検査の正当性は実行時検査をパスした仕様はプログラムの実行中常に成り立つことに依存していたが、プログラム状態の変更が可能になったことで、実行時検査をパスした後状態変化により成り立たなくなるような述語が書けるようになってしまう。このような状態に依存した述語はこれまでの顕在的契約では扱うことができない一方で、プログラムの状態を検査することは命令的プログラムの安全性検査を行う上では重要となる。 我々は型検査機構が状態変化を検知できるよう、Nanevski らのホーア型を取り入れた顕在的契約計算を新たに設計、さらに状態変更を伴うような仕様として不適切な述語を検知するためにリージョンに基づく効果システムを導入し、我々の顕在的契約計算の健全性を証明した。

† 国立情報学研究所（発表当時は日本 IBM 東京基礎研究所）

‡ 京都大学