特別研究報告書

スマートコントラクトのガス消費量の Reource Aware ML を用いた静的解析

指導教員：末永　幸平　教授，五十嵐　淳　教授

京都大学工学部情報学科

小野　雄登

2021 年 2 月 2 日

スマートコントラクトのガス消費量の Reource Aware ML を用いた静的解析

小野　雄登

内容梗概

2009 年にビットコインを用いた取引がオープンソフトウェアで始まって以来，現在に至るまでにブロックチェーンを技術基盤とする様々な仮想通貨が開発されている．スマートコントラクトは，仮想通貨の取引における契約の締結や履行を自動化する仕組みであり，ブロックチェーン上で動作するプログラムとして扱われる．

Tezos は，スマートコントラクトを用いたブロックチェーンを技術基盤とする仮想通貨の 1 つで，コントラクトはスタックベースのプログラミング言語 Michelson で書かれている．Tezos のスマートコントラクトには，ガスの概念が存在し，ガスはコントラクトの実行にかかる手数料を表している．コントラクトの各命令のの評価毎に命令の実行内容に比例した量のガスが消費され，消費量の合計が許容ガス消費量を超えると，その命令が直ちに停止され，命令の実行による値の変更が取り消される．ガスの消費量の計算は複雑で，前もってガスの消費量を正確に見積もることは難しいとされている．

本研究では，プログラミング言語型のツールである Resource Aware ML（以下，RAML と略記する．）を用いて，スマートコントラクトのガス消費量の静的な解析を行うプログラムを実装した．RAML は，OCaml の文法を用いたプログラムを入力として受け取り，プログラムのリソース消費量の限界値を指定されたメトリックに従って自動的に，かつ静的に計算し，その解析結果を多項式の値として出力するツールである．

実装の過程は大きく 2 つに分けられる．始めに，Michelson プログラムのスタック構造を，RAML において Ocaml のリスト構造を用いたプログラムとして実装した．次に，実装したプログラムに対して，RAML のメトリックの 1 つである tick メトリックを用いて，出力として得られるプログラムのリソース消費量からコントラクトのガス消費量を見積もれるかどうかを検証した．tick メトリックは，リソース消費の値や発生するタイミングを，ユーザーが関数として定義することができるメトリックである．

Mihcelson プログラムの RAML での実装では，スタックの要素をヴァリアン

ト型 t として定義し，コントラクトの各命令を (t list -> t list) 型をもつ関数として定義した．Michelson プログラムでのコントラクトは初期スタックとそれを変更する一連の命令として実装されているので，同様に RAML においてコントラクトを実装し，RAML の steps メトリックを用いてリソース消費量を計算した．結果として，基本的なスタックの操作に関する命令や，簡単な算術演算や条件分岐の命令については多項式で表現されたが，ループ命令や，リストや集合に対する再帰を含んだ命令については多項式で表現できないものも存在した．

ガス消費量の見積もりの検証では，コントラクトの実行におけるガス消費量は，コントラクトの実行中の複数の過程において発生するガス消費量の合計で計算されることがわかったが，研究における時間的制約から，そのうちの 1 つである interpreter cost について取り組むことに決めた．RAML で実装したコントラクトの各命令について，その命令のガス消費量に相当する値の tick 関数を定義し，tick メトリックを用いてリソース消費量の分析を行った．結果として，コントラクト実行時のログに表示される interpreter cost に相当する値に概ね等しい値を出力として得られた．ただし，ガスの消費量が引数の値に依存するような命令などは，正確な消費量を見積もることはできなかった．

本研究において実装しなかった，もしくはリソース消費量が解析できなかったコントラクト命令の実装や，コントラクトの実行中の他の過程において発生するガス消費量の見積もりは，今後の課題とする．

Static Analysis for Gas Consumption of Smart Contracts Using Resource Aware ML

Yuto Ono

Abstract

スマートコントラクトのガス消費量の **Reource Aware ML** を用いた静的解析

目次

1 序論

tezos のコントラクトにはガスの概念が用いられている．コントラクトの実行において一定量のガスが消費されるが，この量が制限を超えるとコントラクトの実行が取り消される．tezos のコントラクトはスタックベースのプログラミング言語 Mihchelson を用いたプログラムによって書かれており，ガスの消費量は Michelson プログラムの内容によって決まる．本研究では，Resource Aware ML（RAML）を用いて，コントラクトのガス消費量の推測を試みる．RAML は，OCaml プログラムを入力として受け取り，そのリソース消費量の限界値を出力するプログラミング言語型のツールである．Michelson プログラムのスタック構造を OCaml のリスト構造を用いて OCaml プログラムとして表現し，RAML の tick メトリクスを用いて，リソース消費量としてコントラクトのガス消費量に近しい値が得られるかどうかを検証する．

2 背景知識

2.1 tezos と Michelson について
2.2 コントラクトのガス消費の仕組み
2.3 Resource Aware ML について

3 RAML での Michelson プログラムの実装

4 検証結果と考察

5 改善点

6 結論

謝辞

参考文献

[1] Caplener, H. D. and Janku, J. A.: Improved Modeling of Computer Hardware Systems, *Computer Design*, Vol. 12, pp. 59–64 (1973).

[2] Beizer, B.: Towards a New Theory of Sequential Switching Networks,

IEEE Trans. Computers, Vol. C–19, pp. 936–956 (1970).

[3] 村上伸一: 微分方程式の解曲線の表示, 情報処理, Vol. 14, pp. 231–238 (1970).

[4] 平井有三, 福島邦彦: 両眼視差抽出機構の神経回路網モデル, 信学論 (D), Vol. 56–D, pp. 465–472 (1973).

[5] Baraff, D.: Curved Surfaces and Coherence for Non-penetrating Rigid Body Simulation, *SIGGRAPH '90 Proceedings* (Beach, R. J.(ed.)), Dallas, Texas, ACM, Addison-Wesley, pp. 19–28 (1990).

[6] 對馬雄次ほか: ボリュームレンダリング専用並列計算機のアーキテクチャ, 並列処理シンポジウム JSPP'94, pp. 89–96 (1994).

[7] Barnett, S. and Storey, C.: *Matrix Methods in Stablity Theory*, Nelson, London (1970).

[8] J. E. ホップクロフト, J. D. ウルマン（木村, 野崎訳）: 言語理論とオートマトン, サイエンス社, chapter 6 (1972).

[9] 寺沢寛一: 自然科学者のための数学概論, 岩波書店, pp. 325–328 (1955).