２０１４年度　博士研究員研究成果報告書

氏名（所属研究室）　森口　草介（理工学研究科高橋和子研究室）
研　究　課　題　正当性が保証されたシステムの構築支援手法の研究
研　究　期　間　２０１４年4月1日～２０１５年3月３１日
研 究 成 果 概 要（**日本文（全角）の場合は2,500字程度、英文（半角）の場合は90字×65行程度**）

本研究課題について、二つの目的を挙げた。一つは記述した証明の対象を修正する手法およびその影響範囲についての研究、もう一つは証明のリファクタリング指標についてである。

１）記述した証明の対象を修正する手法およびその影響範囲についての研究については、過去に提案した対話的修正機構に関する拡張と、ネットワークプロトコルの検証が主な成果となる。対話的修正機構について、これまでは宣言された型に新たなデータの種類を追加することだけが可能だったが、今回は拡張可能な範囲を広げ、レコード型を拡張する手法を提案し、プログラミングおよびプログラミング論研究会にて発表した。なお、この論文はワークショップにおいて高く評価され、論文賞を受賞した。

一方、対話的修正機構の応用としてネットワークプロトコルについての検証とその修正を試みた。Content-Centric Networking というネットワークアーキテクチャで用いられているプロトコルについて検証したところ、修正時の影響の範囲が予想以上に大きく、また根本的な検証手法の変更も多い（帰納法を用いるが、どの要素に基づく帰納法であるかが変わる）ため、比較的小規模な変更にのみ対応している対話的修正機構では対応が難しいことがわかった。そのため、対話的修正機構ではなく、より大きな単位であるネットワークの記述そのものをモジュールとして分離、再利用することを考え、特定の仕様を満たす任意のネットワークに対して、プロトコルが正常に動くことを証明した。この証明は、具体的なネットワークの記述を与えると、そのネットワークで正常に動くことを示す記述が得られる。この証明をオープンソースとして公開しているほか、証明の過程で得られた固定のネットワークに関する証明をプログラミング研究会にて発表した。

２）証明のリファクタリング指標については、指標そのものを挙げることはできなかったが、対話的修正機構による修正内容を、修正する対象と合成するための手法を提案した。この際に、修正を直接合成することは難しく、証明を等価な別に形式に変形することで合成を可能とした。この変換はプログラムが処理をしやすいという観点に基づいているが、応用として、より人間の可読性を重視した変換手法についてすすめることでリファクタリングの方法と指標を与えることが可能となる。

その他に、新たな試みとしてプログラムを生成するプログラムの検証方法について提案し、高信頼な理論と実装のための定理証明および定理証明器（TPP2014）という研究集会において発表し、またディペンダブルシステム研究会においてポスター発表を行った。この手法では、プログラムの検証システムにおいて、ある特定の値をプログラムの記述そのものと判定することで、プログラムによって生成されるプログラムについて検証が可能となる。多くのシステムで

はこのような検証のために新たに複数の規則などを追加し、システムを再構築する必要があるが、本研究の手法ではシステムの再構築は必要ない場合があり、また再構築が必要な場合であっても、ほとんどの場合では本来必要となる変更よりは少なくなる。

発表一覧

1) 森口 草介・高橋 和子, 対話的修正と被修正系との合成手法, 日本ソフトウェア科学会 第 31 回大会, Sep., 2014.

2) 森口 草介, プログラム生成の検証へ向けて, 高信頼な理論と実装のための定理証明および定理証明器 (TPP2014), Dec., 2014.

3) 森口 草介, プログラム検証システムの拡張としてのプログラム生成の検証, 第 12 回 日本ソフトウェア科学会 ディペンダブルシステムワークショップ, Dec., 2014.

4) 森口 草介・高橋 和子, レコードの拡張を許す対話的修正機構, 第 17 回 プログラミングおよびプログラミング言語ワークショップ, Mar., 2015. (論文賞)

5) 森嶋 崇・後藤 瑞貴・森口 草介・高橋 和子, Coq を使ったツリー型ネットワークトポロジ上での CCN のモデル化と検証について, 第 103 回 情報処理学会 プログラミング研究会, Mar., 2015.

6) 後藤 瑞貴・森口 草介・高橋 和子, 定性空間表現の Coq による形式化およびその平面性の証明, 第 103 回 情報処理学会 プログラミング研究会, Mar., 2015.

CCN のプロトコルに関する証明は以下のサイトで公開されている。
https://github.com/chiguri/CCNprotocol