D-01　定理証明支援系 Rocq による研究室配属アルゴリズムの形式的検証

後藤大征*，西村俊二**
（*大分工業高等専門学校　専攻科　電気電子情報工学専攻，**大分工業高等専門学校　情報工学科）

1. 背景・目的

近年のIT普及に伴い，ソフトウェア開発は社会基盤に不可欠な要素となっている．特にプログラム作成の工程は開発の中心であり，不具合やバグの発生する可能性があることから，プログラムの信頼性の確保が重要である．代表的な検証方法として動的テストが挙げられるが，有限のテストケースしか検証できない．一方，形式手法はプログラムが満たすべき性質を数学的に証明することで，あらゆる入力に対する正当性を保証できる．その反面，形式手法の学習コストの高さや開発時間の増加などの課題[1]から，実際の開発現場での活用は限定的である．

こうした背景のもと，足立の先行研究[2]では，大分工業高等専門学校情報工学科で実際に使用される研究室配属アルゴリズムを対象に，定理証明支援系 Rocq [3]を用いた形式的検証が試みられた．この研究では，学生数と研究室数をそれぞれ２つに限定した小規模な条件下におけるアルゴリズムの性質が証明された．これにより，形式手法の有効性が示されると同時に，Rocqでは背理法が直接利用できないため，証明に工夫が求められるといった実践的な課題も浮き彫りとなった．

本研究では，従来研究での限定した状況下における検証を踏まえ，任意の学生数と任意の研究室数におけるアルゴリズムの性質を証明することで，形式手法の現実的応用への足掛かりとすることを目的とする．形式手法の実用事例として，身近なアルゴリズムについて適用可能であることを具体的に示し，検証の際にどのような知識が必要になるのかを明らかにする．

2. Rocq

フランス国立情報制御研究室（INRIA）の研究グループによって開発されたRocq [3]は，広く利用されている定理証明支援系の１つであり，Calculus of constructionsという高階型システムに基づく．定理証明支援系とは，ユーザが記述した形式証明の正当性を機械的に検証するシステムである．Rocq は型理論に基づいた定理証明系である.具体的には,論理式の形で定理を述べることができ，コンピュータとの対話で証明を作ることもできる．

3. 研究室配属アルゴリズム

研究室配属アルゴリズムは，大分工業高等専門学校の情報工学科で研究室配属を行う際に使用されるアルゴリズムであり,学生の成績順位に基づき研究室配属を行う．全学生のリスト，全研究室のリスト，各学生の希望研究室リストを入力として与えると，各研究室の配属状況を出力として返す．また，本アルゴリズムの前提として，学生の希望研究室には希望順序が存在し，すべての研究室が１つずつ記述されているものとする．本アルゴリズムの出力が満たすべき３つの性質を表１に示す．

4. 証明

4.1. 形式化

性質の証明を行う際，論理的な検証が可能な形にするために，数学的な表現に形式化する必要がある．本研究における形式化では，学生を St ，研究室を G といった型で表し，これらを用いてアルゴリズムを関数として定義する．定義した関数を用いて，表１に示した性質を表２のように記述することができる．全体の配属アルゴリズム alloc は，単一の複雑な関数としてではなく，より単純な機能の階層的な構造で設計した．

表 **1**　アルゴリズムの出力が満たすべき性質

1	すべての学生はそれぞれただ１つの研究室に配属される．
2	制限人数を超過して学生が割り振られることはない．
3	学生の成績順位が高いものの希望研究室が配属先研究室に反映されやすい．

表 **2**　３つの性質の形式化

1	forall labs, alloc = Some labs -> exactly one assign labs.
2	forall labs, alloc = Some labs -> forall i : Fin.t total_labs, countSome (Vector.nth labs i) <= capacity.
3	forall labs, alloc = Some labs -> forall s1 s2 : St, wish s1 = wish s2 -> rank s1 < rank s2 -> forall r1 r2, lab_of s1 labsV = Some r1 -> lab of s2 labsV = Some r2 -> r1 <= r2.

4.2. 性質1

性質１を最終的な配属関数 alloc に対して直接行うのは非常に困難である．そこで，アルゴリズムの階層的な定義に基づき，証明も同様に階層的に進める戦略を採用した．まず最も原始的な操作に対し，性質が成り立つことを示し，その結果を利用して１つ上位の操作でも性質が成り立つことを示す．このように，ボトムアップに性質が受け継がれることを示すことで，最終的に alloc 関数でも性質が満たされることを示す．このように，複雑なアルゴリズム全体の性質を，検証可能で扱いやすい単位に分割して論証することが可能となった．

4.3. 性質2

一般に,Rocq が採用する構成的論理の体系では，古典論理で多用される背理法を直接用いることができない．これにより，先行研究[2]では，証明の方針が立てられないという課題が存在した．本研究ではこの課題に対し，形式化の段階で性質の証明が自明となるように，型構造を設計するという方針を採用した．具体的には，個々の研究室の配属状況を，可変長のリストではなく，長さが制限人数 capacity に固定されたデータ型であるベクターとして定義した．

4.4. 性質3

性質３は本アルゴリズムが保証すべき最も特徴的な性質であり，証明方針として，学生の成績順位を変数とする数学的帰納法を用いて行う．同一の希望研究室リストを持つ２人の学生がいるとき，順位の高い学生の配属が優先されることを示す．

現在の進捗として，性質1と性質2の証明が完了しており，今後は性質３の証明を行う．

参考文献

[1] A. Reid, L. Church, S. Flur, S. de Haas, M. Johnson, and B. Laurie. Towards making formal methods normal: meeting developers where they are.
Human Aspects of Types and Reasoning Assistants(2020).
[2] 足立 湧綺,「定理証明支援系 Coq による研究室配属アルゴリズムの形式的検証」，大分工業高等専門学校情報工学科　卒業研究，2023-1-20.
[3] About The Rocq Prover.
url: https://rocq-prover.org/about (accessed 2025-8 1).