

平成 30 年 6 月 4 日現在

機関番号：12401

研究種目：研究活動スタート支援

研究期間：2015～2016

課題番号：15H06081

研究課題名(和文) 認知的プログラミングによる自動定理発見

研究課題名(英文) Automated Theorem Finding by Epistemic Programming

研究代表者

高 宏彪 (GAO, HONGBIAO)

埼玉大学・理工学研究科・助教

研究者番号：50756955

交付決定額(研究期間全体)：(直接経費) 1,100,000円

研究成果の概要(和文)：1988年Wosにより提案された世界的に知られている未解決難問である自動定理発見問題とは、新しく面白い定理を自動的に発見する自動推論プログラムが持つべき一般的性質を明らかにする問題である。本研究は強相関論理に基づく前向き推論による手法に基づいて、認知的プログラミングによる自動定理発見を行うという試みで、自動定理発見問題の完全解決に対して新しい突破口を切り拓くものである。

研究成果の概要(英文)：The problem of automated theorem finding is still an open problem which was originally proposed by Wos in 1988. The problem of automated theorem finding is "What properties can be identified to permit an automated reasoning program to find new and interesting theorems, as opposed to proving conjectured theorems?" This research performed automated theorem finding by using forward reasoning approach based on strong relevant logic and epistemic programming, and opened up a new breakthrough to solve the problem of automated theorem finding.

研究分野：自動推論

キーワード：自動推論 自動定理発見 認知的プログラミング 離散数学

1. 研究開始当初の背景

(1) 1988年 Wos により提案された世界的に知られている未解決難問である自動定理発見問題とは、新しく面白い定理を自動的に発見する自動推論プログラムを持つべき一般的性質を明らかにする問題である。その解決は、様々な分野で多くの応用があり、特に、計算的学習、予測、発見に対して系統的な方法論と強力的な道具を提供することができる。

(2) 国外では、Wu による幾何学定理の自動証明と発見[6]、および Colton による純粋数学理論の自動形成[3]があったが、それぞれ、特定数学分野の具体的な定理を証明する際の偶然の発見、および既存自動定理証明系、モデルチェッカー、データベースの組み合わせによる例題生成と反例探しであり、自動定理発見問題を系統的に解決しようとする試みではなかった。

(3) 国内では、応募者のグループ以外の研究が報告されていない。応募者のグループは、知識発見を基礎づける論理体系として強相関論理を構築し[1]、汎用前向き推論エンジン FreeEnCal を開発し[2]、科学者の研究活動における学習、予測、発見の認識プロセスを計算論的な手法と認識プログラミング言語 EPLAS を提案した[5]。

(4) 応募者は、強相関論理に基づく前向き帰結演算による自動定理発見という一般的系統的な方法論[4]を提案し、開発した汎用前向き推論エンジン FreeEnCal を用いて NBG 公理集合論、Peano 数論、グラフ理論三つの数学の分野に事例研究を行い、幾つかの定理の再発見ができたという原理的な提案した方法論を実証した。

2. 研究の目的

(1) 本研究は、応募者が既に提案した自動定理発見のための系統的方法論に基づいて、認識的プログラミングによる自動定理発見を行うという新しい試みで、科学者の学習、予測、発見における認識プロセスに対して、認識的プログラミングパラダイムの有効性と実用性を明らかにする。

3. 研究の方法

(1) まず、NBG 公理集合論、初等整数論の形式理論を構築する。次に、EPLAS を用いて記述した、形式理論における定理発見認識過程の EPLAS プログラム群を EPLAS 処理系上で繰り返し実行し、既知定理の再発見あるいは既知未解決問題の解決を確かめる。更に、閉帰結論理式をすべて洗い出し、新しい経験定理の候補として列挙する。述語抽象、概念形成、

帰納推論、仮説生成などの方法も利用して、面白い新しい経験定理の特定方法を明らかにする。

(2) そして、グラフ理論、組合せ理論、抽象代数学、公理幾何学も含めた実用的な離散数学形式理論グリッドを構築し、上記研究方法項目(1)得た研究成果に基づいて、研究を更に展開する。

4. 研究成果

(1) 強相関論理 EcQ の第2級(論理定理における必然的帰結演算子の入れ子の深さは2まで)論理定理集合に基づいて、汎用前向き推論エンジン FreeEnCal を用いて NBG 公理集合論の第2級形式理論を生成し、また、NBG 公理集合論の既知定理も強相関論理 EcQ に基づいて形式化し、それらを合わせて NBG 公理集合論の形式理論知識ベースを構築した。

(2) 強相関論理 EcQ の第2級論理定理集合に基づいて、FreeEnCal を用いて初等整数論の第2級形式理論を生成し、また、初等整数論の既知定理および既知未解決問題も強相関論理 EcQ に基づいて形式化し、それらを合わせて初等整数論の形式理論知識ベースを構築した。

(3) 強相関論理 EcQ の第2級論理定理集合および上記成果項目(1)で得た NBG 公理集合論の第2級形式理論に基づいて、FreeEnCal を用いてグラフ理論の第2級形式理論を生成し、グラフ理論の形式理論知識ベースを構築した。

(4) 強相関論理 EcQ の第2級論理定理集合に基づいて、FreeEnCal を用いて公理化幾何の第2級形式理論を生成し、公理化幾何の形式理論知識ベースを構築した。

(5) 公理集合論教科書と数学史、論理学史書籍の記述から、数学者が数学理論を展開する際に行った学習、予測、発見の手順を推定し、それを真似するという手法で述語抽象と概念形成の過程を強相関論理に基づく前向き帰結演算による自動定理発見に応用し、EPLAS で記述した。

(6) 初等整数論における数学帰納法をどうやって強相関論理に基づく前向き帰結演算による自動定理発見に用いるのかを明らかにし、EPLAS で記述した。また、帰納推論、仮説生成などの方法も強相関論理に基づく前向き帰結演算による自動定理発見に応用し、EPLAS で記述した。

(7) どうやって背理法を強相関論理に基づく前向き帰結演算による自動定理発見に用いるのかを明らかにし、EPLAS で記述した。

(8) 429 個の既知な NBG 公理集合論定理を分析し、NBG 公理集合論経験定理の面白さに四つのインパクトファクター（述語抽象と概念形成の階層、論理演算子の級、前向き推論過程の長さ、定理図式）を見つけた。四つのインパクトファクターに基づいて、NBG 公理集合論経験定理の面白さを定量的に定義し、面白さのメトリックを定義した。

(9) 定義した面白さのメトリックを用いて、上記成果項目(1)に取った NBG 公理集合論経験定理の面白さを定量的に分析した。面白くない NBG 公理集合論経験定理は「0」として標記され(EPLAS で記述した)面白さの数値が高ければ高いほど、定理の数がだんだん減少していくという図1の結果を取って、定義した面白さのメトリックの有効性を明らかにした。

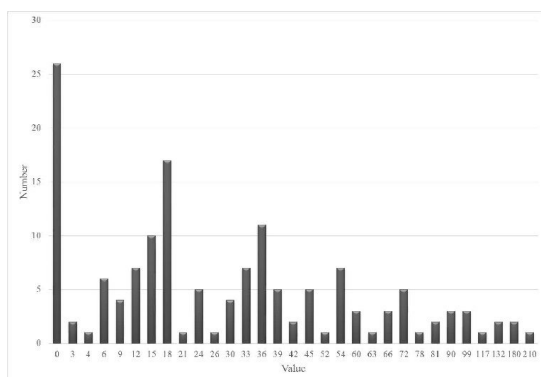


図1 NBG 公理集合論経験定理の面白さを定量的に分析した結果

(10) 959 個の既知な初等整数論定理を分析し、上記成果項目(8)に見つけた四つのインパクトファクター（述語抽象と概念形成の階層、論理演算子の級、前向き推論過程の長さ、定理図式）は初等整数論にも適用できることがわかった。その四つのインパクトファクターに基づいて、初等整数論経験定理の面白さを定量的に定義し、汎用な面白さのメトリックを定義した。

(11) 定義した面白さのメトリックを用いて、上記成果項目(2)に取った初等整数論経験定理の面白さを定量的に分析した。面白くない初等整数論経験定理は「0」として標記され(EPLAS で記述した)面白さ「0」ではない初等整数論経験定理の面白さの値が正規分布に近づくという図2の結果を取って、定義した面白さのメトリックの汎用性を明らかにした。

(12) 研究の実用性を示すために、「Wide-mouthed-frog」プロトコルおよび「Secret Splitting」プロトコルに対して、強相関論理に基づく前向き帰結演算による手法で形式化分析を行って、推論した結論から、攻撃行為を発見できた。強相関論理に

基づく前向き帰結演算による手法は離散数学における概念の学習と発見に応用できるだけでなく、暗号プロトコルの推論的分析による欠陥発見、新しい攻撃パターンの予測と発見にも応用できることを明らかにし、この研究の実用性を示した。

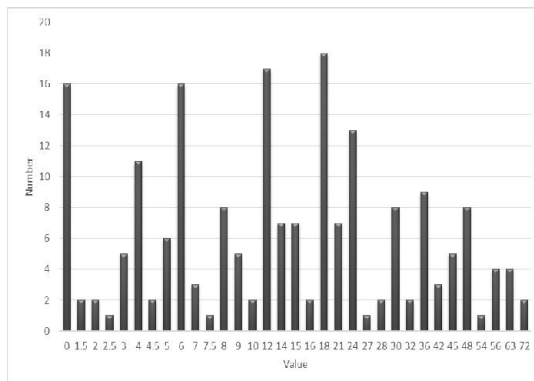


図2 初等整数論経験定理の面白さを定量的に分析した結果

(13) 本研究成果の位置づけは提案した強相関論理に基づく前向き帰結演算による自動定理発見の体系的な方法論および認識プログラミングによる記述し実行することを通じて、自動定理発見問題の完全解決に対して新しい突破口を切り拓くものである。

<引用文献>

- Jingde Cheng, Entailment Calculus as the Logical Basis of Automated Theorem Finding in Scientific Discovery, AAAI Technical Report SS-95-03, 1995, pp. 105-110
- Jingde Cheng, Shinsuke Nara, and Yuichi Goto, FreeEnCal: A Forward Reasoning Engine with General-Purpose, Lecture Notes in Computer Science, Vol. 4693, 2007, pp. 444-452
- Simon Colton, Automated Theory Formation in Pure Mathematics, 2002
- Hongbiao Gao, Yuichi Goto, and Jingde Cheng, A Systematic Methodology for Automated Theorem Finding, Theoretical Computer Science, Vol. 554, 2014, pp. 2-21
- Isao Takahashi, Shinsuke Nara, Yuichi Goto, and Jingde Cheng, EPLAS: An Epistemic Programming Language for All Scientists, Lecture Notes in Computer Science, Vol. 4487, 2007, pp. 406-413
- Wentsun Wu, Mathematics Mechanization: Mechanical Geometry Theorem-Proving, Mechanical Geometry Problem-Solving, and Polynomial Equations-Solving, 2000

5. 主な発表論文等

(研究代表者、研究分担者及び連携研究者に

は下線)

〔雑誌論文〕(計 6 件)

Da Bao, Kazunori Wagatsuma, Hongbiao Gao, and Jingde Cheng, Predicting New Attacks: A Case Study in Security Analysis of Cryptographic Protocols, Lecture Notes in Electrical Engineering, peer-reviewed, Vol. 393, 2016, pp. 263-270

DOI:10.1007/978-981-10-1536-6_35

Hongbiao Gao and Jingde Cheng, Measuring Interestingness of Theorems in Automated Theorem Finding by Forward Reasoning: A Case Study in Peano's Arithmetic, Lecture Notes in Computer Science, peer-reviewed, Vol. 10192, 2017, pp. 115-124

DOI:10.1007/978-3-319-54430-4_12

Hongbiao Gao and Jingde Cheng, Automated Theorem Finding by Forward Reasoning Based on Strong Relevant Logic: A Case Study in Tarski's Geometry, Lecture Notes in Electrical Engineering, peer-reviewed, Vol. 393, 2016, pp. 55-61

DOI:10.1007/978-981-10-1536-6_8

Hongbiao Gao, Yuichi Goto, and Jingde Cheng, A Set of Metrics for Measuring Interestingness of Theorems in Automated Theorem Finding by Forward Reasoning: A Case Study in NBG Set Theory, Lecture Notes in Computer Science, peer-reviewed, Vol. 9243, 2015, pp. 508-517

DOI:10.1007/978-3-319-23862-3_50

Hongbiao Gao, Yuichi Goto, and Jingde Cheng, Automated Theorem Finding by Forward Reasoning Based on Strong Relevant Logic: A Case Study in Graph Theory, Lecture Notes in Electrical Engineering, peer-reviewed, Vol. 352, 2015, pp. 23-30

DOI:10.1007/978-3-662-47487-7_4

Yuichi Goto, Hongbiao Gao, and Jingde Cheng, A Predicate Suggestion Algorithm for Automated Theorem Finding with Forward Reasoning, Lecture Notes in Computer Science, peer-reviewed, Vol. 10192, 2017, pp. 125-134

DOI:10.1007/978-3-319-54430-4_13

〔学会発表〕(計 2 件)

Hongbiao Gao and Jingde Cheng, An Epistemic Programming Approach for Automated Theorem Finding, Proceedings of the 14th International Conference on Cognitive Informatics & Cognitive Computing, peer-reviewed,

2015, pp. 49-58

Jingchen Yan, Kazunori Wagatsuma, Hongbiao Gao, and Jingde Cheng, A Formal Analysis Method with Reasoning for Cryptographic Protocols, Proceedings of the 12th International Conference on Computational Intelligence and Security, peer-reviewed, 2016, pp. 566-570

〔図書〕(計 件)

〔産業財産権〕

出願状況(計 件)

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

取得状況(計 件)

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

6. 研究組織

(1) 研究代表者

高 宏 彪 (GAO, Hongbiao)
埼玉大学・大学院理工学研究科・助教
研究者番号：50756955

(2) 研究分担者

()

研究者番号：

(3) 連携研究者

()

研究者番号：

(4) 研究協力者

()