G-018

代数の自動証明を目的とした分散システム
The distributed system for the proof algebra

舩戸 正和 † 仁木 直人 ‡ 鈴木 秀男 §
Masakazu Funato Naoto Niki Hideo Suzuki
小林 英恒 ¶ 村尾 裕一 ‖ 小野 陽子 ‡
Hidetune Kobayashi Hirokazu Murao Yoko Ono

1. はじめに

数式処理および計算機代数の研究は発展し、数値・数式融合計算を初めとして多方面の分野との協調に関する研究が盛んである。計算機代数における試みのひとつとして，証明システムとの連携に関する研究も盛んになってきている。自動証明システムの多くは数式処理における計算の正当性を保障したり、証明システムで必要となる数式の計算に数式処理システムを利用しようというものである。

計算機上で抽象代数の命題証明を行うには、代数の基本的な定義や対象命題の証明過程を形式化し記述する必要がある。計算機に入力された証明過程に対して公理系と推論規則が正しく適用されているかどうか検査する。

本研究では、抽象代数、特に環論を対象とした証明システムの開発を行っている。抽象代数の分野の中で、環論は論理的に簡潔な分野である。したがって、環論は証明の自動化もそれほど難しくないであろうという認識に立ち、環論の抽象的な理論そのものを計算機上で展開する研究を行い、。この研究の目標は環論の自動証明システムを構築することである。

本システムは、数学者による命題証明を支援することを目的とする。命題証明をシステム化することにより、新たな命題証明を行なう際に必要となる公理や既に証明されている命題の探索と適用を可能とする。

2. Isabelle を用いた命題証明

本研究では、定義や命題の形式的表現および証明過程の検査に、対話型の汎用証明システムである Isabelle[1] を使用している。Isabelle は形式言語 (Meta Language)[2] を用いて、定義や証明過程を記述する。Isabelle で利用できる形式的な表現方法は 2 種類ある。一つは Isabelle の処理系に直接取り込むために数学記号などををタグ付きのテキストで記述する方法である。もう一つは xemacs 上で x-symbol を利用することにより、数学記号をそのまま表示できる方法である。

Isabelle ではあらかじめ記述された代数に関する定義や論理規則がパッケージとして用意されており、証明処理に利用することができる。Isabelle は一階論理や高階論理などの複数の論理規則をサポートしており、本研究では高階論理 [3] を用いて証明処理を行う。

Isabelle での証明は backward proof である。以下に、Isabelle を用いた命題証明の一例を記述する。まず、対象命題の証明に必要となる定義を記述する。

```
constdefs
"cmp g f == λx.  g (f x)"
"idmap A == λx∈A. x"
"constmap A B == λx∈A. SOME y.  y ∈
B"
"invfun A B (f ::  'a ⇒ 'b) == λy∈B.
∈ x.  (x ∈ A ∧ f x = y)"
```

次に、証明すべき対象命題をゴールとして与える。

```
lemma eq_fun:"⟦ f ∈ A → B; f = g ⟧
⟹ g ∈ A → B"
```

続いて、与えたゴールに対して証明過程を記述する。

```
proof -
assume p1:  "f ∈ A → B" and p2:  "f
= g"
from p1 and p2 show ?thesis
apply auto
done
qed
```

記述した証明過程に従って演繹則の適用と項の書き換えを行い、次に証明すべき複数のサブゴールへと分解・変形する。各サブゴールに対し同様の操作を繰り返し、全てのサブゴールがあらかじめ記述された定義や証明済みの命題に一致すれば証明終了となる。

証明操作のほとんどは自動化されておらず、命題証明に必要となる定義や証明過程を利用者が記述する必要がある。

3. 自動証明システム構築への課題

本研究では自動証明システムを構築することを目標としている。Isabelle に対して対象命題をゴールとして与えると、自動的に必要な定義や証明過程を検索し証明処理を行なうシステムである。

自動証明システムを実現するために解決しなければならない問題として、

1. 抽象代数を扱うための基礎定義集合の確定
2. 推論規則集合の決定
3. 個々の演繹則の適用条件および適用方向の決定
4. 証明済み命題と証明過程の記録と再利用
5. システム規模の増大に対する対処

†東京理科大学 大学院 工学研究科 経営工学専攻
‡東京理科大学 工学部 経営工学科
§職業能力開発総合大学校 東京校
¶日本大学 理工学部 数学科
‖電気通信大学 電気通信学部 情報工学科

などがあげられる。

本研究において、1. および 2. については、Isabelle に用意されている汎用の定義集合および高階論理を用いている。また、抽象代数を扱うために必要な定義については追加を行い、基礎定義集合はほぼ確定している。

しかし、3. については、公理系を用いた演繹のみが定型化されているに留まっている。4. については、新たな命題の証明を行うには、証明済みの命題を用いて演繹を行うことが必要となる。そこで、証明済みの命題や証明過程を「どのような命題の証明に現れ、どのように使われたか」という情報を付加して再利用に用いる。また、5. については、情報の付加によって記録内容が増大対処が必要になってくる。

本研究では 3. ～ 5. を解決する方針として

- 命題や証明過程を記録した知識ベースの構築
- 知識ベースおよび証明処理機構の分散化

を行なう。

3.1 知識ベースの構築

定理や証明過程の再利用と演繹則適用の決定支援を目的として Isabelle で記述された内容を記録し知識ベースとして構成する。記録する内容は、抽象代数を扱うための基礎定義集合と命題 (ゴール) である。また、Isabelle での証明過程において生成されるサブゴールについても記録を行なう。

記録されたゴールとサブゴールには、証明過程が付加されて記録される。これに加えて、サブゴールには発生元のゴールと該当サブゴールの前後に発生しているサブゴールおよび発生処理のために用いられた演繹についても記録を行う。

現在までに定義およびゴールのデータベース化が完了している。データベース定義は以下の通りである。

名前 Isabelle 上で表現された定義や命題の名称を表す

区分 定義、定理、補題などを識別する

内容 定義の内容または与えたゴール

証明 証明済みの定理や補題の場合、記述した証明過程

このデータベースは部分文字列を用いた Web 上での検索を可能としている。表示方法としてタグ付きのテキストをそのまま表示する方法と、x-symbol で表現することのできる数学記号を表示する方法の 2 種類を用意している。

記録した内容は知識ベースとして利用できるよう、ゴールおよびサブゴールの使用している定義による分類を行っている。また、同様のサブゴールが発生する演繹にどのようなゴールが適用されているかパターンマッチを用いた分析を行っている。

また、ゴールやサブゴールの記述方法に変化が生じた場合に対応するため記述内容について履歴の管理を行っている。

3.2 証明システムの分散化

抽象代数には群論・環論・体論等の分野があり、使用する研究者群および頻用する定理群に大きな差がある。すなわち、抽象代数の全分野を対象とするシステムをつくり、それを共同利用することは効率的ではない。しかし、各分野は相互に関連していることから、複数のシステムが他とは独立に動作させることには、知識ベースに重複するレコードが多い等の無駄が多く、他分野での新しい成果を利用することも困難である。また、複雑な対象命題を証明する方法として、多数の演繹則適用を機械的に試行する方法や複数の数学者が協調して証明を行うことを可能にする必要がある。

このため、分野ごとに構成された知識ベースの相互利用と推論処理機構の協調を目的として、証明システムを分散環境に展開する。本システムの分散化における課題として、知識ベースからの証明済み命題の探索、相互利用するにあたっての知識へのアクセス権の管理がある。これらの課題を解決するために、証明システムを Ninf[5] を用いて PC グリッドとして実装する。

4. 今後の課題

本研究で開発しているシステムでは、知識ベースに記録された命題や証明過程をパターンマッチによって分析している。機械的なパターンマッチでは、類似した命題や証明過程の関連性を完全には把握する困難である。したがって、演繹則適用を自動化すると不適切な適用が行われる可能性がある。このため、一部において利用者による演繹則適用のチェックが必要となり、証明処理を完全に自動化するに至っていない。今後は、演繹則適用の自動化を行うために、知識ベースの構成や利用方法を見直す必要がある。

参考文献

[1] Isabelle, http://www.cl.cam.ac.uk/Research/HVG/Isabelle/

[2] L.C. Paulson, ML for the working programmer, Cambridge University Press, 1991,1996.

[3] Tobias Nipkow,Lawrence C. Paulson,Markus Wenzel, A Proof Assistant for Higher-Order Logic, Springer-Verlag, 2002-2003.

[4] 陳 凌釣, 小林 英恒, 村尾 裕一, 鈴木 秀男, A Machine Proof of the Proposition “Ideal $\subseteq \bigcup_i$ PrimeIdeal$_i$ $\Rightarrow$ Ideal $\subseteq$ PrimeIdeal$_i$”, Computer Algebra - Algorithms, Implementations and Applications 研究集会報告集, 京都大学数理解析研究所 講究録 1295, 2002.

[5] Ninf Project Home Page, http://ninf.apgrid.org/