

外96-46

早稲田大学大学院理工学研究科

博士論文概要

論文題目

論理を指向した代数系とその応用

申請者

山崎 勇

Isamu Yamazaki

1996年12月

計算機を用いた自動証明の研究は、計算機の出現後まもなく始められ、その後の半世紀に渡る研究と計算機の発達により、現在では世界の多くの大学で証明システムが開発され、使用される状況になっている。例えば群論や幾何学の分野では自動証明システムにより新定理の発見もなされている。

しかし、目立った成果を上げた場合を見ると、証明対象を特定の領域に限定し、tuningした証明システムを用いたものが多く、汎用の証明システムでは、いまだに実行効率が悪い。多くの証明システムでは、それぞれ工夫を凝らした証明戦略を用いている。しかし、その証明戦略の適用条件、副作用、限界、改良可能性、他の戦略との関係、他の戦略との相性、他の戦略との統合可能性、といった問題に対して、統一的な視点から見通すための横断的な方法論がないため、それぞれの理論に基づいて、その都度個別に検討しているのが現状である。

そこで、証明戦略を統一的に検討できる視点を提供するための道具として、新しい代数系を提案する。推論加群系と名付けたこの代数系は、その上で推論と充足を代数的に記述でき、かつ線形空間と同じような扱いができるため、論理の問題をこの代数系の上で記述し、多くの証明戦略を、例えば準同形写像として、統一的に捕らえることができるものと期待される。

推論加群系 推論加群系は線形空間の系に非常に似ている。線形空間の系はスカラー \mathbf{R} 、列ベクトル空間 V 、行ベクトル空間 U からなると見ることができる。例えば $u \in U$ と $v \in V$ との内積 $u * v$ は \mathbf{R} の元であり、ベクトルのスカラー倍は $v \cdot r$ および $r \cdot u$ と記すことができる。 V から V への線形変換、および U から U への線形変換はいずれも行列で表され、任意の行列は $\sum_{j \in J} v_j \cdot u_j$ と書ける。そして U と V とは互いに他の双対空間である。これとまったく並行した話が推論加群系でも成り立つ。

推論加群系は環 \mathbf{R} 、推論加群 D （右 \mathbf{R} 加群）、および事実加群 Ψ （左 \mathbf{R} 加群）からなる。 $\psi \in \Psi$ と $d \in D$ との内積 $\psi * d$ は \mathbf{R} の元である。 $\alpha \in \mathbf{R}$ による $d \in D$ への右作用 $d \cdot \alpha (\in D)$ と、 $\psi \in \Psi$ への左作用 $\alpha \cdot \psi (\in \Psi)$ とが与えられている。 $m = \sum_{i \in I} d_i \cdot \psi_i$ は Ψ から Ψ への右 \mathbf{R} 準同形写像であると同時に、 D から D への左 \mathbf{R} 準同形写像である。また、 D と Ψ とは、互いに他の双対加群の部分加群である。

環 \mathbf{R} は代入から放置性を除いた総代入をさらに拡張した、左単一化関数から生成される加群に、合成による乗法を入れた環である。左単一化関数 $l(\hat{t}; \hat{s})$ の機能は次のように解釈される。乗法 “.” によって右方から伝えられてきた変数記号の値を項列 \hat{s} に代入した結果と、項列 \hat{t} を单一化しようとする。单一化できなければその左単一化関数の値は 0 である。单一化できるならば、そのとき \hat{t} の変数記号に与えられるべき項

をその変数記号の値として、乗法 “.” によって左方へ伝える。 \hat{u} を基礎項列、 \hat{X} を変数記号列とすると、 $l(\hat{X}; \hat{u})$ は総代入と等価な働きを持つ。

推論加群 D は、素論理式 $P_k(\hat{X}_k)$ ($k \in K$) を生成元とする有限生成右 \mathbf{R} 加群である。また事実加群 Ψ は、素事実 $\tilde{P}_k(\hat{X}_k)$ ($k \in K$) を生成元とする有限生成左 \mathbf{R} 加群である。 D と Ψ とは互いに相手の双対加群の部分加群である。すなわち $\psi \in \Psi$ は D から \mathbf{R} への左 \mathbf{R} 準同形写像である。この写像 $\psi \in \Psi$ による $d \in D$ の像を $\psi * d$ と記して、これを ψ と d の内積と称する。これは同時に Ψ から \mathbf{R} への右 \mathbf{R} 準同形写像 $d \in D$ による $\psi \in \Psi$ の像である。素事実と素論理式との内積は次のように左単一化関数となる。 $\tilde{P}_i(\hat{t}) * P_j(\hat{s}) = l(\hat{t}; \hat{s}) \cdot \delta_{ij}$

また $m = \sum_{j \in J} d_j \cdot \psi_j$ ($d_j \in D, \psi_j \in \Psi$) と表記されるものに、 D から D への左 \mathbf{R} 準同形写像機能と、 Ψ から Ψ への右 \mathbf{R} 準同形写像機能を与えることができる。そこでこのように書かれる m の全体を M とする。 M は環 $\text{End}_{\mathbf{R}}(D)$ と環 $\text{End}_{\mathbf{R}}^O(\Psi)$ の部分環である。

\mathbf{R} の元と M の元とは項を変形する手続きを表しているので、これら環を乗法と加法を持つプログラム言語と考えることができる。例えば並列計算は加法で、コンパイラによる部分計算は乗法で実現される。

推論代数系の計算を実行する数式処理系 rpdr を prolog の上に作成した。rpdr は代数的証明システム papend において用いている。

推論加群系の代数 推論加群 D はねじれ加群であるので、 D の空でない部分集合は一次独立ではない。しかし、準一次独立なる概念を定義することができ、それによりほぼ線形空間と同等の概念や操作を利用できるようになる。 $B \subset D$ が準一次独立であることは、 B の全ての基礎例が一次独立であることを意味する。

任意の $d \in D$ に対してその汎双対元なる元 $\psi \in \text{Hom}_{\mathbf{R}}(D, \mathbf{R})$ ($\subset \Psi$) が存在して、 $d \cdot (\psi * d) = d$ を満たす。また $d \in D$ が含む変数記号（代表変数）の全体が $\{\hat{X}\}$ のとき、 $\psi * d = l(\hat{X}; \hat{X})$ を満たす $\psi \in \text{Hom}_{\mathbf{R}}(D, \mathbf{R})$ を d の双対元と称する。準自由元（単独で準一次独立な元）の汎双対元は双対元である。従って準自由元は双対元を持つ。 ψ が d の汎双対元であれば、方程式 $d \cdot \alpha = e$ ($e \in D, \alpha \in \mathbf{R}$) が解を持つとき $\alpha = \psi * e$ は解である。またこの時、 $m = 1_M - d \cdot \psi$ は d から生成される部分加群の補部分加群への射影となるので、これを用いて方程式から d 成分を消去できる。そして限られた範囲では、与えられた $d \in D$ の汎双対元または双対元 ($\in \Psi$) を実際に構成できる。このことは、射影などの準同形写像が必要な時、それを実際に構成し、それを用いて写像計算を進めることができるという点で、推論加群系の実用上の価値を高めている。

代数的証明原理 推論加群系とある関係にある加群 U と加群 D ($\subset D$) に「推論」と「充足」を埋め込むことができる。すなわち変換 $u : W$ (割り当ての全体) $\rightarrow U$ と $d : C$ (節の全体) $\rightarrow D$ および変換 $c : D \rightarrow C$ を、次が成り立つように定義できる。

$$w \models c \Rightarrow \forall d_T \in (d(c) \text{ の基礎例の全体}) [u(w) * d_T \geq 0],$$

$$\forall d_T \in (d \text{ の基礎例の全体}) [u(w) * d_T \geq 0] \Rightarrow w \models c(d).$$

その結果 D の和は健全な推論となる。また非負の作用 $\alpha \in R^+ \subset R$ を適当に定義すると、非負の作用も健全な推論となる。さらに、次の代数的証明原理が成り立つ。

節集合 $S = \{c_i\}_{i \in I}$ が一般 Horn 条件を満足するならば、 S が充足不可能であるための必要十分条件は、次の一次方程式（証明方程式）が解 α_i を持つことである。

$$\sum_{i \in I} d(c_i) \cdot \alpha_i = d(\square), \quad \alpha_i \in R^+ \quad (\square \text{ は空節})$$

一般 Horn 条件とは、Horn 節集合であるという条件を最大限緩和したものである。この方程式の左辺は S からの論理的帰結を、左辺は矛盾を表す。

証明方程式を解く方法として、未知数の係数に直交する射影を施す消去法を考えられる。これは解の非負性を考慮しない解法である。そこで補助述語を導入し、非負性を考慮した手続きとすることができる。この手続きは、モデル生成による充足可能性判定法とも見なせる。これに基づく代数的証明システム papend を試作した。この手続きは改良の余地があるものの、充足可能な節集合に対しても無限ループに陥らずに判定できる場合がある。

推論加群系は準同形写像を活用することで、自動証明の効率向上のための戦略を求めるために利用できる。例えば abstraction の理論において、推論加群系の準同形写像を abstraction として利用することができる。同様な理由で、推論加群系は理論の類似性や等価性を論じる際に利用できる。また推論と充足を推論加群の上で代数的に表現できるので、論理の問題を推論加群系の上に移して、代数的に考えることに使える。

以上のごとく推論加群系は推論と充足が表現でき、かつ線形空間と同様の概念・操作が可能であるので、論理が関わる分野や計算機科学の分野の問題解決に大いに利用され、発展することが期待される。