

学位論文及び審査結果の要旨

横浜国立大学

氏名	坂田 康亮
学位の種類	博士(理学)
学位記番号	環情博乙第463号
学位授与年月日	令和3年3月25日
学位授与の根拠	学位規則(昭和28年4月1日文部省令第9号)第4条第1項及び 横浜国立大学学位規則第5条第2項 (論博の場合は第2項)
研究科(学府)・専攻名	環境情報学府 情報環境専攻
学位論文題目	Efficient signature-based algorithms for computing Gröbner bases
論文審査委員	主査 横浜国立大学 准教授 原下秀士 横浜国立大学 教授 西村尚史 横浜国立大学 教授 四方順司 横浜国立大学 教授 野間淳 横浜国立大学 教授 梶原健

論文及び審査結果の要旨

多項式環のイデアルの良い生成元を与えるグレブナ基底の理論は、Buchbergerにより導入され、最初の基本的なグレブナ基底を求めるアルゴリズムはBuchbergerアルゴリズムと呼ばれる。グレブナ基底は、方程式系の研究において、強力な道具であり、理論・応用において幅広く利用されるため、より効率的なグレブナ基底を求めるアルゴリズムが求められている。その中で、FaugèreによるF4アルゴリズムとF5アルゴリズムは、その高速性や潜在的な可能性から代表的なアルゴリズムとされ、坂田氏は、特にF5アルゴリズムを基にした、signature-basedアルゴリズムについて研究を行っている。F5アルゴリズムはsignatureと呼ばれるものを計算中に保持しておくことにより、計算中に現れる無駄な計算(zero reduction)を大幅に削減することが出来るが、理論および実装が難しいとされる。坂田氏は、その課題について取り組み、signature-basedアルゴリズムの効率化、具体的な実装可能なアルゴリズムの提出、そのアルゴリズムの正確性と停止性の研究を行った。本論文は、Introduction(第1章)とConclusions(第5章)を含めて全5章から構成されている。

第2章「Notations and algorithms of Gröbner bases」では、環論、単項式順序、グレブナ基底およびグレブナ基底を求めるBuchbergerアルゴリズムなど基本事項が解説されている。

第3章「Signature-based algorithms for computing Gröbner bases」では、F5アルゴリズムの具体的な実装アルゴリズムaltRB(alternative rewrite basis algorithm)の提出とその正確性と停止性の証明が行われている。F5アルゴリズムは提出されてから時間が経つが、実装の難しく、坂田氏は実装に成功した(特に日本では)稀有な存在である。その実装を基に、様々な加群順序にも対応できる実装可能なアルゴリズムとしてaltRBを提示し、その正確性と停止性を証明した。正確性とは、そのアルゴリズムが停止時に正しいsignature Gröbner基底を出力することを指し、停止性はそのアルゴリズムが有限回の操作で停止すること指す。Signature Gröbner基底のアルゴリズムにおいて、正確性と停止性の証明の理解は難しく、一部には疑問視する研究者もいたが、坂田氏は、より簡単なものから段階的に複雑なアルゴリズムを考察してゆくことにより、明快でself-containedな証明を与えることに成功した。

第4章「An efficient strategy for signature-based algorithms」では、signature-basedアルゴリズム全般において有効な、簡約化の回数削減手法の提案を行った。簡約化とは、ある多項式系を法として、多項式のある項を与えられた単項式順序で小さいものにしていく操作であるが、signature-basedアルゴリズムでは、signatureとも整合性を保ちつつ簡約を行うため、s-簡約と呼ばれるものが用いられる。また、signature-basedアルゴリズムではsignature Gröbner基底を求めることに注意する。Signature Gröbner基底を求める際、s-簡約の操作が計算量において支配

的になる傾向が認められ、その回数の削減は重要である。坂田氏は、アルゴリズムの出力で得られる Gröbner 基底から reduced Gröbner 基底を求める際、最終的に不要になる元の簡約化を省略するという着想から selective-full reduction strategy を提案した。従来手法としては、only-top reduction と full reduction があったが、それらの良いところを上手く抽出し、有効な reduction strategy の実現に成功した。代表的なベンチマーク問題においても、目的であった、reduced Gröbner 基底を求める際の簡約化の回数の削減に成功しただけでなく、アルゴリズムの出力で得られる Gröbner 基底を求める際においても、selective-full reduction strategy の有効性を得ることが出来ている。長い歴史のある分野で、有効な strategy を提出したことは画期的といえる。

第5章「Conclusions」では、本研究の成果を総括している。

以上のように、坂田氏の論文では、実装を意識した有効なアルゴリズムの提出とその正確性と停止性の証明および signature Gröbner 基底を求めるアルゴリズムの効率化について、意義深い研究成果をあげている。これまでの研究成果の公表に関しては、学術雑誌論文（査読有）2 篇および7 件の口頭発表などを通して公表され、いずれも高く評価されている。

以上から、本論文は博士（理学）の学位論文として十分な価値を有すると審査員全員一致して認めるものである。

注 論文及び審査結果の要旨欄に不足が生じる場合には、同欄の様式に準じ裏面又は別紙によること。