氏名（本籍）	永井（ながい）　彰（あきら）（青森県）
学位の種類	博士（理学）
学位記番号	甲第1127号
学位授与の日付	平成29年3月18日
学位授与の要件	学位規則第4条第1項該当
学位論文題目	**On the Efficient Implementation of Boolean Gröbner Bases** **（ブーリアン・グレブナー基底の効率的な実装について）**
論文審査委員	（主査）教授　佐藤　洋祐
	教授　瀬尾　隆　　教授　関川　浩
	准教授　橋口　博樹　　准教授　柳田　昌宏

論文内容の要旨

近年，グレブナー基底は，暗号や符号など多くの分野で重要なツールとなっている．本論文では，係数をブール環とする多項式環（ブール多項式環）におけるグレブナー基底（ブーリアン・グレブナー基底）について扱う．本論文は理論，実装，応用の3つの内容から構成され，まずブーリアン・グレブナー基底の計算理論である計算アルゴリズムに触れる．ここでは，ブール多項式環における重要な定理であるBoolean extension theoremとBoolean Nullstellensatzを示し，次にブーリアン・グレブナー基底ならびに包括的ブーリアン・グレブナー基底の計算アルゴリズムについて述べる．特に，包括的ブーリアン・グレブナー基底では，消去イデアルの計算に対する効率的な計算アルゴリズムを提案する．しかし，これら計算アルゴリズムを実装することは容易ではなく，これまでブーリアン・グレブナー基底の実装は，一部のソフトウェアのみと限定的であった．そこで本論文では，ブール多項式環の数学的性質を用いて，これら計算アルゴリズムを，MathematicaやMaple等の一般的な計算機代数ソフトウェアにおいて実装可能，かつ並列計算可能な効率的実装方法を提案する．また，ブーリアン・グレブナー基底の計算に最適な計算機代数ソフトウェアを実験から示す．この実験により，ブーリアン・グレブナー基底の計算には，オープンソースの計算機代数ソフトウェアSageMathが有効であることを導く．最後に，この効率的実装の適用例として，数独ソルバーと数独の難易度付けに触れる．数独の解と数独の難易度を求めるためには，ブーリアン・グレブナー基底の計算を多数行う必要があり，これまでは，リアルタイムで数独を解くことができなかったが，本実装によりそれを達成する．また，ブーリアン・グレブナー基底を

用いた数独の難易度付けは，数独ソルバーよりも計算量が大きく，その計算に膨大な時間を要してきたが，提案する並列分散計算を適用することで数秒で求めることが可能になった．このように，本論文ではブーリアン・グレブナー基底の計算理論，その実装と応用までを述べ，ブーリアン・グレブナー基底の実用化に寄与する．

論文審査の結果の要旨

一般のブール多項式環におけるブーリアン・グレブナー基底を計算するプログラムは、現在のどの数式処理システムにおいても実装されていない。標数２の体上の多項式環におけるグレブナー基底の計算プログラムをそのまま用いて効率的な実装をおこなうことが不可能であることが主な理由である。

申請者はブール多項式環の準同型写像を汎用数式処理システム上で実装する巧妙な方法を考案した。本論文ではこの方法について数学的な詳細を含めて述べられている。さらに、応用例として、申請者が実装したプログラムを用いて得られたいつかの結果が述べられている。

本論文では、まず第１章においてブーリアン・グレブナー基底に関する先行研究の紹介を含め、論文の概要が述べられている。論文の結果を理解する上で必要なバックグラウンドとなる数学理論について、第２章ではブール多項式環の理論、第３章ではブーリアン・グレブナー基底の理論、第４章では包括的ブーリアン・グレブナー基底の理論について概説が与えられている。 第５章と６章が論文の主要部である。第５章において、申請者が考案した実装法について、背景にある数学理論も含め詳細な記述が与えられている。この実装法は申請者によって、数式処理システム SageMATH 上に実装され、現時点で世界最高速なブーリアン・グレブナー基底の計算プログラムとなっている。第６章では、申請者によって実装された高速プログラムを用いることではじめて明らかになったいくつかの結果が応用例として述べられている。具体的には、数独問題の難易度に関する先行結果の論文のデータの間違いを明らかにするとともに、正しい計算データを基に、難易度に関する新しい数学的定義を提案している。

これらの結果は主論文を構成する論文 1-4 で報告されている。いずれも世界的に認められた学術雑誌あるいは国際会議のプロシーディングスであり、計算機代数の進歩に大きな貢献をもたらしている。よって、本論文は学位（博士）論文として十分価値があると認める 。