様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科研費 KAKENHI

科学研究費助成事業　　研究成果報告書

平成 ２６ 年　 ６ 月 ２３ 日現在

機関番号：３２６６０
研究種目：基盤研究(C)
研究期間：2011～2013
課題番号：２３５０００２５
研究課題名（和文）組み合わせ問題に対する可換代数的手法

研究課題名（英文）Algorithms for combinatorial problems based on commutative algebra

研究代表者
佐藤　洋祐（Sato, Yosuke）

東京理科大学・理学部・教授

研究者番号：５０２５７８２０

交付決定額（研究期間全体）：（直接経費）　2,200,000円、（間接経費）　660,000円

研究成果の概要（和文）：本質的に整数演算を含まないような組み合わせ問題の解法に焦点をしぼり、その解法のために必要な、可換代数の理論について、ブーリアン・グレブナー基底を中心に研究をおこなった。その結果、ブーリアン・グレブナー基底が最適な可換代数の手法であることが判明した。
数式処理システムRisa/Asirを用いて実装をおこない、われわれの理論の有効性を確認した。特に、効率的な並列アルゴリズムが構築できることが実証された。

研究成果の概要（英文）：We investigated a theory of commutative algebra that is needed for a solution algorithm for combinatorial problems. We have concentrated on problems which do not essentially contain integer arithmetic. As a result, we found that our algorithm based on Boolean Groebner bases methods is the best method.We also implemented our method on the computer algebra system Risa/Asir and showed the efficiency of our algorithm, especially our algorithm is more practical on the environment of parallel computations.

研究分野：総合領域

科研費の分科・細目：情報学基礎

キーワード：ブーリアン・グレブナー基底

１．研究開始当初の背景

(1) 組み合わせ問題の一つである整数計画問題は工学を含む様々な分野で重要な研究テーマの一つになっている。整数計画問題で扱う問題は、数学的にはプレスバーガー算術([1])とよばれる一階術語言語で記述可能な問題の一部にすぎず、プレスバーガー算術の限量子消去法のアルゴリズムによって厳密解をすべて求めることが可能である。しかしながら一般にこのアルゴリズムの計算量は消去したい変数の個数にたいしてトリプルエクスポネンシャルであることが知られており、およそ実用的ではない。実際、現在利用できる整数計画問題を扱うソフトウエアでは、商用も含めほとんどのもので、線形計画法と分岐限定法とよばれる探索技法を組み合わせた初等的（あまり高度な数学を使わない）手法が用いられている。

(2) 近年、多項式環イデアルのグレブナー基底を利用した計算機代数の手法が提案され([2])、それに続く多くの研究者の成果によって、ソフトウエアの開発も含め、著しい発展をみせている。

２．研究の目的

(1) 組み合わせ問題はその多くが集合制約の解消問題としてとらえることができる。本研究では、集合のブール環としての構造に着目し、集合制約問題をブール多項式環上のイデアルの問題として考えることで、グレブナー基底をはじめとする、可換代数における斬新的なツールを用いた代数的解法の構築とその有効性を検証することを目的とする。

(2) 現実に現れる整数計画問題においては、個々の変数がとる値の整数は何らかの集合の個数を表す場合が多く、実際にはそれらの集合の間に集合としての関係、すなわち集合の和や積などの演算を用いて表される関係が存在する場合が多い。しかしながら、上記のいずれの方法でも、このような集合制約を扱うことはできない。ブール代数の古典的な結果であるスコーレムの集合演算における限量子消去法のアルゴリズム([3])は、一般の集合制約を集合の個数に関する式のみで構成される論理式に変換して解法をおこなう。この論理式は整数計画問題で扱う式よりもはるかに単純な構造をしている。

最近[4]や[5]において、集合制約と集合の個数に関する式が混在する制約にたいして、これを集合の個数に関する式のみで構成されるプレスバーガー算術の論理式に変換し解法するアルゴリズムが相次いで発表された。これらのアルゴリズムを用いると、プログラムの停止性の証明やデータ構造の健全性の検証などが可能になる。しかしながら、どちらもプレスバーガー算術の限量子消去法のアルゴリズムに基づいているため、適用できる制約は非常に小規模なものに限定される。われわれは集合制約を効率的に解くための手法として、ブーリアン・グレブナー基底の理論を構築し、それに基づく集合制約ソルバーをフリーソフトウエアとして公開してきた。数百個程度の変数の問題でも扱うことが可能であり、スコーレムの限量子消去法よりもはるかに高速なアルゴリズムを実現している。集合に関する制約をわざわざ整数に関する制約に変換して解くよりも、集合のブール代数構造を直接利用した解法の方が効率的であることが主な理由なのであるが、二種類の限量子∀と∃が入れ子になって現れるような制約にたいしては著しく性能が低下するという欠点があった。これにたいし、われわれがここ数年おこなってきた Comprehensive Gröbner Bases の研究結果を用いて、Comprehensive Boolean Gröbner Bases の高速な計算アルゴリズムを構築できることが[6,7,8]で明らかになり、この欠点を克服できることが判明した。われわれの手法は、集合制約と集合の個数に関する式が混

在する制約にたいしても適用可能であり、集合のブール代数構造を直接利用するので、変換された整数に関する式のみを扱う[4]や[5]よりもはるかに効率的なアルゴリズムが実現できると予想される。

(3) 本研究では、集合の個数に関する式が整数計画問題に表れるようなものに焦点をしぼり、それらと集合制約が混在するような制約にたいして、有効で実用的なアルゴリズムを構築することを目標とする。
本研究は、[2]らの方法と同様にグレブナー基底を利用した可換代数の手法に基づくものであるが、全く別の種類のグレブナー基底であるブーリアン・グレブナー基底を利用するものであり、彼らのアプローチとは本質的に異なる。[4]や[5]の方法が既存の算法を利用したアルゴリズムを用いているのにたいし、本研究では、われわれのオリジナルであるブーリアン・グレブナー基底を用いる。本研究の目標が達成されれば、集合制約のような知識処理においても可換代数の手法が有効であることが実証されることになる。

参考文献

[1] M.Presburger, Uber die Vollstandigkeit eines gewissen Systems der Arithmetik ganzer zarlen, Comptes rendues du premier Congres des Math.desPaysSlaves,Warsaw,pp92-101,395,1929.
[2] P.Conti and C.Traverso, Buchberger algorithm and integer programming,AAECC-9, Springer LNCS 539, pp130-139, 1991.
[3] Fenstak,J.E. ed "Selected Works in Logic by Th. Skolem",Scand.Univ.Books,Universitetsforlaget, Oslo, 1970.
[4] P. Revesz, Quantifier-Elimination for the First-Order Theory of Boolean Algebras with Linear Cardinality Constraints,Proceedings of ADBIS'04, Springer LNCS 3255, pp1-21, 2004.
[5] V. Kuncak, H. Nguyen and M. Rinard, An Algorithm for Deciding BAPA:Boolean Algebra with Presburger Arithmetic, Proceedings of CADE-20, Springer LNAI 3632,pp260-277, 2005.
[6] Yosuke Sato,Akira Nagai & Shutaro Inoue, On the Computation of Elimination Ideals of Boolean Polynomial Rings, LNCS 5081, pp 338-348, Springer-Verlag Berlin Heidelberg 2008.
[7] Shutaro Inoue,Yosuke Sato and Akira Suzuki, On Algorithms for Calculus of Sets,Proceedings of the First International Conference on Mathematical Aspects of Computer and Information Sciences(MACIS 2006),pp 148-153, 2006.
[8] Yosuke Sato & Shutaro Inoue, On the Construction of Comprehensive Boolean Gröbner Bases, Proceedings of the Seventh Asian Symposium on Computer Mathematics(ASCM 2005), pp 145-148, 2005.

３．研究の方法

(1) 本研究では、まず、本質的に整数演算を含まないような組み合わせ問題にターゲットを絞り、そのための可換代数的解法のための、ブーリアン・グレブナー基底の理論を研究し発展させる。

(2) 次に、整数演算が本質的に必要であるような集合制約として記述できるような組み合わせ問題に対する可換代数的解法とプレスバーガー算術の限量子消去法のアルゴリズムよりもはるかに有効な限量子消去アルゴリズムについて研究する。

４．研究成果

(1) 整数に関する制約を含んでいるように思われる組み合わせ問題でも、本質的に整数演算を含まないものは、世の中に数多く存在する。例えば、数独パズルの問題では、１から９までの数を扱うが、整数としての演算は全く現れない。問題を無理やり整数演算を用いて記述し、なんらかの手法で解くことは可能であるが、本質的な解法ではないので非効率的である。実際、通常の有理数体上の多項

式環におけるグレブナー基底を用いた解法に関する研究がいくつか報告されているが、いずれも実用的ではない。数学構造を全く使わないヒューリスティックなプログラムで、ずっと高速なものが多数存在する。整数演算を含まないので、順列組み合わせの群構造以外は、代数構造が無いように思われるが、実はこの問題は本質的に集合制約として記述することができ、そこには集合の族から構成されるブール環の構造が介在する。
本研究では、まず、この種の本質的に整数演算を含まないような組み合わせ問題の解法に焦点をしぼり、その解法のために必要な、可換代数の理論について、ブーリアン・グレブナー基底を中心に研究をおこなった。その結果、ブーリアン・グレブナー基底が最適な可換代数の手法であることが判明した。これらの結果は研究業績①で報告されている。

(2) 計算機代数の分野では、理論の構築だけでは研究は不完全で、その有効性を実証するためにプロトタイププログラムを作成する必要がある。検証プログラムの実装は、数式処理システム Risa/Asir 上でおこなった。大学院生にもプログラムの作成等によって研究に協力してもらった。並列アルゴリズムの有効性を検証するためにおこなった OpenXM による実装により、われわれの理論の有効性が実証された。これらの結果は研究業績③で報告されている。

(3) 一般の制約にたいしては限量子消去の有効なアルゴリズムを構築するには至らなかったが、ブール制約において得られた知見を応用することにより、複素数領域における限量子消去をグレブナー基底の計算でおこなう有効なアルゴリズムを構築できた。これらの成果は研究業績④、⑤で報告されている。

５．主な発表論文等

〔雑誌論文〕（計５件）

① Yosuke Sato, Shutaro Inoue, Akira Suzuki, Katsusuke Nabeshima and Ko Sakai, Boolean Gröbner Bases, Journal of Symbolic Computation, Vol 46/5, pp 622-632, 2011. 査読有

② 井上秀太郎、佐藤洋祐、グレブナー基底を使った数独の難易度判定と問題作成、数理解析研究所講究録第１７８５巻、pp51-56、2012. 査読無

③ 佐藤裕介、井上秀太郎、佐藤洋祐、数独の難易度判定のためのブーリアングレブナー基底の並列計算について、数理解析研究所講究録第１８４３巻、pp28-37、2013. 査読無

④ 深作亮也、井上秀太郎、佐藤洋祐、代数的閉体における限量子消去アルゴリズムについて、COE Lecture Note Vol.49,Kyushu University, pp 27-32, 2013. 査読無

⑤ Ryoya Fukasaku,Shutaro Inoue and Yosuke Sato, On QE Algorithms over Algebraically Closed Field, Proceedings of Fifth International Conference on Mathematical Aspects of Computer and Information Sciences, pp21-25, 2013. 査読有

〔学会発表〕（計５件）

①井上秀太郎、佐藤洋祐、数独の最小分岐数の計算について、日本数式処理学会理論分科会及びシステム分科会合同研究会、２０１２年１月２２日

②Yosuke Sato, Why we need and how we compute parametric Groebner Bases, Bioinformatics Week in Odaiba, ２０１２年１月２７日

③Yosuke Sato and Shutaro Inoue, Parallel Algebraic Computations for Combinatorial Problems, NII Shonan Meeting on Parallel Methods for Constraint Solving and Combinatorial Optimization, ２０１２年５月３１日

④ Shutaro Inoue and Yosuke Sato, On parallel Computations of Boolean Groebner bases for combinatorial problems, Conference on Applications of Computer Algebra 2012, ２０１２年６月２８日

⑤ Yosuke Sato, Stability of Groebner Bases in Terms of a Commutative von Neumann Regular Ring, The Tenth Asian Symposium on Computer Mathematics, ２０１２年１０月２７日

６．研究組織

(1)研究代表者

佐藤　洋祐（SATO, Yosuke）
東京理科大学・理学部・教授
研究者番号：50257820