様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２７　年　　６　月　　９　日現在

機関番号：　３２６５７
研究種目：　基盤研究(C)
研究期間：　2011～2014
課題番号：　２３５４００５７

研究課題名（和文）代数群の作用を受ける代数多様体の研究

研究課題名（英文）A study of the algebraic varieties with an algebraic group action

研究代表者
中野　哲夫（Nakano, Tetsuo）

東京電機大学・理工学部・教授

研究者番号：００２１７７９６

交付決定額（研究期間全体）：（直接経費）　　4,100,000円

研究成果の概要（和文）：本研究ではブーリアングレブナ基底を用いて，連立ブール方程式の効率的解法である井上アルゴリズムと，その数独型パズルへの応用の研究を行った．まず，一般化井上アルゴリズムを用いて連立ブール方程式を解く際に現れる全ての樹形図の３つ組データの最少値として，井上不変量を定義した．応用として，数独型パズルを連立ブール方程式で定式化し，４独および対角型５独パズルの場合に井上不変量の分類を行い，２つの特殊な対角型５独パズルを除いて，全ての唯一解をもつパズルの井上不変量は自明であることを証明した．また，9×9の数独パズルの場合は，井上不変量が数独パズルの難易度を表すすぐれた指標であることを実験で確認した．

研究成果の概要（英文）：In this research, we have studied the Inoue algorithm, which is a very efficient method for solving a system of the Boolean polynomial equations, and its application to the puzzles of Sudoku type. We have firstly defined the Inoue invariant of such a system, which is the triple data of the minimum tree diagram among all the trees appearing in the process of the generalized Inoue algorithm. As an application, using the formulation of the puzzles of Sudoku type in terms of the Boolean polynomial equations, we have classified the Inoue invariant of the 4-doku and the diagonal 5-doku puzzles. It turns out that in these cases, every puzzle with a unique solution has a trivial Inoue invariant (2,1,1) except 2 special types of diagonal 5-doku puzzles. We have also shown by experiments that, in the case of Sudoku puzzles (9 times 9), the Inoue invariant is an excelent indicator of the difficulty of the puzzles.

研究分野：　代数幾何学，計算代数学

キーワード：　Booleanグレブナ基底　井上アルゴリズム　数独型パズル

１．研究開始当初の背景

(1) ブーリアングレブナ基底は，体上の多項式環のイデアルの通常のグレブナ基底の変種であって，ブール多項式環のイデアルの標準基底である．ブーリアングレブナ基底は，1980 年代に佐藤，坂井らによってはじめて導入され，以来，理論面・応用面の両方からさかんに研究されている（引用文献[3]参照）．

(2) 井上は，引用文献 [2] において，ブーリアングレブナ基底を用いて連立ブール方程式の解を求める優れたアルゴリズム（井上アルゴリズム）を提唱した．井上アルゴリズムは，与えられた連立ブール方程式の定めるイデアルに属する ASP(=Almost Solution Polynomial，ほとんど解けた形の多項式)を巧みに用いる．すなわち，イデアルに属する ASP を SP(=Solution Polynomial, 解けた形の多項式)に変換することにより，より多くの変数の値を定めていくのである．もし，イデアルに属する ASP がなくなってしまった場合は，あらかじめ変数順序を１つ固定しておき，まだ値の定まっていない変数のうち最少のものを選び，更にこの変数の取りうる値を任意に１つとり，その SP をイデアルに付け加えて，このイデアルについて再び ASP を探して SP に変換し，より多くの変数の値を定めていく．井上アルゴリズムの実行結果は１つの樹形図で明確に表示できるが, ASP がなくなった時に新しい変数を選び，その取り得る値を選ぶ時点は，樹形図ではちょうど分岐点になっている．分岐点での分岐数は，選んだ変数の取り得る値の個数に等しい．井上アルゴリズムを実行していくと，樹形図が成長していくのであるが，連立ブール方程式の解は，この樹形図の葉（行き止まりの点）になる．ただし，すべての葉が解を与えるわけではなく，たとえばもとの連立方程式が唯一の解をもつ場合は，１つの葉のみが解を与え，それ以外の葉はすべて解でない．樹形図の成長は有限回で止まり，この井上アルゴリズムで連立ブール方程式の全ての解を求めることができる．

(3) 井上アルゴリズムは，引用文献[2]において，数独パズルを効果的に解くのに応用された．数独パズルとは，9×9 の升目に 1 から 9 までの数字を，各行，各列，９個の 3×3 ブロックに重複しないように埋めるパズルで，世界的に楽しまれ，また，数学的構造が複雑なため代数的組み合わせ論の研究対象としても興味深く，多くの研究がなされている．数独パズルは，連立ブール方程式を用いて簡単に定式化することができる．井上は，数式処理システム Risa/Asir 上に井上アルゴリズムを実装し，このプログラムを用いて，数独パズルのブール連立方程式は，数秒から数分程度でパソコンを用いて解くことができることを見出した．

２．研究の目的

(1) ブーリアングレブナ基底は，1980 年代にその基礎付けがなされて以来，文献が散在しており，現在では手にはいらないものも多い．従って，まずブーリアングレブナ基底の初等的かつ厳密な基礎付けの再構築をすることが最初の目標である．

(2) 井上アルゴリズムは，井上によって Risa/Asir 上に実装されたが，私達の研究室では別の優れた数式処理システムである Magma（引用文献[1]）を用いて代数計算を行っている．そこで，井上アルゴリズムを Magma 上に実装し，独自のプログラムの開発とプログラムの改良を行うことを目的とした．

(3) 井上アルゴリズムは，分岐点においてまだ値の決まっていない変数を選ぶ際，あらかじめ１つの固定した変数順序を用いて，値が未決定の変数のうち最小の変数を選ぶ．これは，井上アルゴリズムの実行結果を一意的に定めるためである．従って，井上アルゴリズムは，１つ固定した変数順序に依存して，分岐点で選択する変数が決まる．この変数順序への依存は，井上アルゴリズムの弱点の１つであって，分岐点で選択する変数を任意に選ぶことも可能である．この変数順序への依存を解消するように井上アルゴリズムを改良することも重要な目的である．

(4) 引用文献[2]には，人間にとって易しい数独パズルは分岐点なしで解けることが報告されている．これは，井上アルゴリズムが数独の難易度判定に使えることを示唆している．そこで，井上アルゴリズムを連立ブール方程式の難易度判定に用いること，さらに数独パズルの難易度判定に応用することを最終目標とした．

３．研究の方法

この研究は，基本的には代数学と計算機を用いて行った．ブーリアングレブナ基底の理論的基礎付けとその応用には，ブール多項式環を用いるため，ブール代数を多く用いる．また，ブーリアングレブナ基底の計算や井上アルゴリズム，井上不変量の計算には数式処理システム Magma (引用文献[1])を用いて，平成２３年度に科研費で購入させていただいた高性能のワークステーション Del Precision T7500 上で計算した．

４．研究成果

(1) ブーリアングレブナ基底理論の基礎づけと計算アルゴリズムの実装．単位的可換環 B であって，任意の元 b の２乗が b に等しいとき B をブール**環**という．B をブール環とし，B 上の多項式環 $B[x]=B[x_1,\cdots,x_n]$ を考える．さらに，B[x]を $x_i^2-x_i$ $(1 \leqq i \leqq n)$で生成されるイデアルで割った剰余環をブール**多項**

式環といいB(x)で表す． B[x]またはB(x)のイデアルの標準基底であるブーリアングレブナ基底の基礎理論については，すでに佐藤・坂井らによって 1980 年代に構築されているが，彼らは特別な型の単項式簡約化を用いて，体上の多項式環のイデアルの通常のグレブナ基底とほぼ類似の理論が成立することを示した．筆者は，単項式簡約化と同値である特別な割算アルゴリズムを用いて理論全体を見通しよく再構成した．すなわち，まず，割算アルゴリズムを用いて，B[x]の有限生成イデアルＩについて，Buchbergerの判定法とグレブナ基底の構成アルゴリズムを証明し，更に，得られたグレブナ基底を極小化・簡約化・stratify することによって，stratified ブーリアングレブナ基底を構成する．Stratified ブーリアングレブナ基底はイデアルＩから一意的に定まり，B[x]またはB(x)のイデアルの標準基底を与える．

実際の計算では，F_2={0,1}を２元体として，$B=F_2^m$ の形のブール環を扱うことがほとんどである．この場合は，Stratified ブーリアン基底は，各成分ごとに F_2[x]のイデアルの簡約グレブナ基底の計算をしてから，各成分のグレブナ基底をまとめることによって簡単に得られる．この成分ごとの計算によるブーリアングレブナ基底の計算アルゴリズムは井上によって数式処理システム Risa/Asir に実装されたが，筆者達のグループは数式処理システム Magma に実装して，計算実験などを行っている．以上の結果は発表論文①にまとめた．

(2) 分岐数予想の解決．井上アルゴリズムの実行結果は，先に述べたように樹形図で表される．多くの数独パズルの連立ブール方程式の解を井上アルゴリズムで解いてみたところ，全ての分岐点で分岐数が２以上であった．分岐数の定義からは分岐数が１という可能性もあるので，井上アルゴリズムの樹形図では任意の分岐点で分岐数は必ず２以上であろう，という予想をした．この予想は，ASP の性質の詳しい解析によって肯定的に解決することができた（発表論文②）．

(3) 井上不変量の定義と連立ブール方程式の難易度評価．引用文献[2]で示唆されているように，井上アルゴリズムは連立ブール方程式の標準的な解法であるがゆえに，その方程式の難易度判定に用いることができると考えられる．そこで，連立ブール方程式の難易度を判定する不変量として，以下の井上不変量を提唱した．まず，井上アルゴリズムでは分岐点でまだ値の定まっていない変数を１つ選ぶのであるが，あらかじめ変数の順序を１つ固定しておき，まだ値未決定の変数のうち最小の変数を選択する．これは，井上アルゴリズムの実行結果を一意的にするためであるが，一方では，最初に任意に選ぶことのできる変数順序にアルゴリズムの遂行結果が依存してしまう，という欠点でもある．そこで，まず，井上アルゴリズムの分岐点において，値未決定の任意の変数を選択することを許すことにして，この拡張化を**一般化井上アルゴリズム**と呼ぶ．一般化井上アルゴリズムでは，分岐点での変数の選択枝がたくさんあるため，実行結果は一般に多数あり，多数の樹形図が生み出される．これらの樹形図の３つ組データ（節の数，葉の数，高さ）の最小値を，この連立ブール方程式の**井上不変量**と定義する．井上不変量は，連立ブール方程式の数学的な不変量であって，この連立ブール方程式を一般化井上アルゴリズムで最短手順で解く際の難易度を表している．ただ，多数の樹形図の３つ組データの最少値として定義されているので，実際に計算するのは困難という弱点がある．そこで，筆者は，分岐点での変数を，樹形図の３つ組データをできるだけ小さくなるように選ぶ戦略（標準戦略）を考案し，井上不変量をとてもよく近似する**計算可能井上不変量**を定義した．計算可能井上不変量は，実際に計算可能であって，例えば数独パズルから生じる連立ブール方程式であれば，数分から数時間程度で計算することができる．

(4) 数独型パズルの井上不変量の計算と難易度判定．まず，数独型パズルのうち最も簡単な**４独**，および**対角型５独パズル**をとりあげた．４独とは 4×4 の升目の各行，各列，４個の 2×2 ブロックに１から４の数字を重複しないように埋めるパズルであり，対角型５独とは，5×5 の升目を用いて，ブロックの条件がない代わりに２つの対角線の条件を課したパズルである．これら２種類の多くのパズルの井上不変量を計算した結果，すべての例の井上不変量が自明，すなわち(2,1,1)であったので，４独および対角型５独（ただし唯一解をもつもの）の井上不変量はすべて自明であろう，との予想をたてて研究を進めた結果，次の定理を得た．

定理（i）唯一の解をもつ４独パズルはすべて，自明な井上不変量(2,1,1)をもつ．
（ii）唯一の解をもつ対角型５独パズルは，２種類の特殊なパズルを除いて，すべて自明な井上不変量(2,1,1)をもつ．例外の２種類のパズルはいずれも井上不変量(4,2,2)をもつ．

従って，対角型５独の場合は，筆者の予想は正しくなかったが，自明でない井上不変量をもつ２種類の特殊なパズルを発見することができた．6×6 の升目の各行，各列，２つの対角線および６個の 2×3 ブロックに，１から６の数字が重複しないように埋めるパズルを**対角型６独パズル**という．対角型６独パズルの場合は，自明でない井上不変量をもつ多くのパズルが存在することを確認した．さらに井上不変量の最大値については，次の部

分的な結果を得た：

定理 (i) 唯一解をもつ対角型６独の初期値（ヒント）の最少個数は５である．
(ii) ５個の初期値をもち唯一解をもつ対角型６独の計算可能井上不変量の最大値は(10,5,4)であり，この計算可能井上不変量をもつパズルは（数字の入れ替え，回転，折り返しを除いて）ちょうど２種類ある．

対角型６独では計算機を用いた井上不変量の分類は大変であり，筆者の研究室の設備では上記定理がほぼ限界であることも判明した．以上の結果は，発表論文③にまとめた．

(5) 最後に数独（9×9）の場合の井上不変量の計算について述べる（引用文献[5]）．数独の場合は，４独や対角型５独のような井上不変量の分類は困難である．そこで，筆者は，数独の難易度と井上不変量の関係を調べた．結果は次の表のようにまとめられる．

パズル	計算可能 II	井上不変量
Level 1	(2,1,1)	(2,1,1)
Level 2	(2,1,1)	(2,1,1)
Level 3	(2,1,1)	(2,1,1)
Level 4	(2,1,1)	(2,1,1)
Level 5	(2,1,1)	(2,1,1)
Level 6	(2,1,1)	(2,1,1)
Level 7	(2,1,1)	(2,1,1)
Level 8	(2,1,1)	(2,1,1)
Level 9	(4,2,2)	(4,2,2)
Level 10	(4,2,2)	(4,2,2)
Level 11	(4,2,2)	(4,2,2)
Level 12	(6,3,3)	(4,2,2)
Level 13	(4,2,2)	(4,2,2)
Level 14	(4,2,2)	(4,2,2)
Level 15	(8,4,3)	
Level 16	(36,18,7)	
Level ∞	(86,43,12)	

表１：数独の難易度と（計算可能）井上不変量の相関

この表で，計算可能 II は計算可能井上不変量を表す．また，Level 1 から Level 15 のパズルは標準的な数独パズルの問題集（引用文献[4]）から易しいもの（Level 1）から難しいもの(Level 15)を無作為にとった. Level 16 と Level ∞のパズルは，それぞれ，インカーラ博士が作成した有名な「世界で一番難しい数独パズル」の 2010 年度版および 2012 年度版である．Level 15,16,∞のパズルの井上不変量は計算できていない．

この表から，数独パズルの難易度と（計算可能）井上不変量は強い相関があることがわかる．たとえば，計算可能井上不変量が(2,1,1)の数独を初級，(4,2,2)の数独を中級，(4,2,2)を超える数独パズルを上級と呼ぶことが可能である．

筆者達は多くの数独パズルの計算可能井上不変量を計算したが，Level ∞のパズルのもつ(86,43,12)が現在のところ数独パズルの計算可能井上不変量の最大値である．

これらの実験を行うことにより，井上不変量が(4,2,2)より大きい数独パズルを作成したり見つけることは大変難しいことがわかってきた．井上不変量が最大の数独パズルを真の「世界で一番難しい数独」と呼んでよいが、そのパズルを作成（または発見）することは本テーマの最大の課題である．この問題については今後も井上不変量の数学的研究を続け，解決を目指したい．

<引用文献>
[1] W. Bosma, J.J. Cannon, C. Fieker, A. Steel (eds), Handbook of Magma functions, Http://magma. maths.usyd.edu.au/magma/.
[2] S. Inoue, Efficient Singleton Set Constraint Solving by Boolean Groebner Bases, Communications of JSSAC **1** (2012), 27-37.
[3] Y. Sato, S. Inoue, A. Suzuki, K. Nabeshima, K. Sakai, Boolean Groebner Bases, J. Symbolic Computations **46** (2011), 622-632.
[4] Time Intermedia, IQ Number Place 300 Vol.4, Gakken Publishing, Tokyo, 2010.
[5] T. Nakano, S. Minami, S. Harikae, K. Arai. H. Watanabe, Y. Tonegawa, On the Inoue invariants of the puzzles of Sudoku type II, submitted.

５．主な発表論文等
（研究代表者，研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 3 件）
① T. Nakano, Y. Tonegawa, Introduction to Boolean Groebner bases and their applications to puzzles of Sudoku type, J. of Algebra and Applied Math., 査読有, **12** (2014), 1-31.
② T. Nakano, On the branch number of the tree diagrams in the Inoue algorithm, J. of Algebra and Applied Math., 査読有, **12** (2014), 49-57.
③ T. Nakano, K. Arai, H. Watanabe, On the Inoue invariants of the puzzles of Sudoku type, Communications of JSSAC に掲載確定，査読有.

〔学会発表〕（計 0 件）

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計　0　件）

○取得状況（計　0　件）

〔その他〕
ホームページ等
http://math.ru.dendai.ac.jp/~nakano/

６．研究組織
(1)研究代表者
中野　哲夫（NAKANO, Tetsuo）
東京電機大学・理工学部理学系・教授
研究者番号：00217796

(2)研究分担者
なし

(3)連携研究者
なし