様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　元 年　 ６ 月 ２１ 日現在

機関番号：２０１０３
研究種目：基盤研究(C)（一般）
研究期間：2015～2018
課題番号：１５Ｋ０４９０４

研究課題名（和文）有限体上における可積分系の探索

研究課題名（英文）Searching for integrable systems over finite fields

研究代表者
由良　文孝（Yura, Fumitaka）

公立はこだて未来大学・システム情報科学部・教授

研究者番号：９０４０４８０５

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：本研究においては、有限体上に値をとる格子模型に付随する力学系を主に構築した。そこで得られた有限体上におけるソリトン系は孤立波を保存し、多項式表示を持つ新規な力学系である。また楕円数列とそれに付随するSomos数列の一般解のHankel行列式表示のもつ性質を調べた。楕円数列は楕円曲線上の点列に等価なものであり、楕円曲線暗号や代数幾何において本質的である。さらには有限体上におけるソリトン系を与える枠組みに現れる代数系の暗号理論への応用に対して基本的な考察を行った。

研究成果の学術的意義や社会的意義
まず、有限体上において孤立波を保存するようなソリトン系は従来得られていなかったと思われるため、新規な力学系である。また多項式表示を持つ点は、従来の実数あるいは複素数上の可積分系には見られない大きな特徴であり、離散的な系との比較は可積分系に対する新しい視点となりうる。また、ここに現れる枠組みは平方剰余と関係することから、力学系として新規なモデルを与える可能性だけではなく、代数系を基にした暗号理論への応用が今後期待される。

研究成果の概要（英文）：In this research, I have mainly constructed the dynamical systems related to the lattice model that take a value on finite fields. The solitonic systems obtained there over finite fields conserves solitary waves, and have polynomial representations, which are novel dynamical systems. The properties of the general solutions of the elliptic sequences and the Somos sequences as a special case are also considered through Hankel determinants. The elliptic sequence is equivalent to the sequence of points on an elliptic curve, and fundamental object for the elliptic curve cryptography and the algebraic geometry. Furthermore, a basic application to cryptography of algebraic systems connected with dynamical systems that support a soliton equation over finite fields are considered.

研究分野：離散可積分系

キーワード：soliton　finite field

様　式　Ｃ－１９，Ｆ－１９－１，Ｚ－１９，ＣＫ－１９（共通）

１．研究開始当初の背景

箱玉系とセルオートマトン系について触れる．箱玉系は従属変数が 0 と 1 からなる可積分な離散力学系であり，1990 年に高橋大輔，薩摩順吉，両氏によって発見された．以来，この離散的状態における可積分系が注目を集め続けてきた．その理由としてはいくつか挙げられるが，

(1) 1996 年に発見された箱玉系の保存量と，超離散化と呼ばれる極限操作によって，非線形可積分系に結び付けられ，ソリトン系であることが示されたこと
(2) 箱玉系は組み合わせ論的な Yang-Baxter 関係式を満たすが，これが量子群におけるクリスタルの表現論と，そこにおける可解格子模型に由来していること

などが数理的な背景として挙げられる．一方，類似している系としてセルオートマトンが存在する. これまでセルオートマトン系については, 複雑系研究の中で多くの研究がなされてきた．厳密な意味において箱玉系は，いわゆるセルオートマトンではないことに注意する．状態空間は同じであるが，満たすべきルールはセルオートマトンでは局所的であるのに対し，箱玉系では非局所的である(かつフィルター型と呼ばれる発展則に分類される)．箱玉系とセルオートマトン系は共に離散値を値に取る力学系である．しかしながら前者は可積分系，後者は主に複雑系と，その出自は違い，また満たすべきルールも全く異なる力学系である．これまで両者を共に含む枠組みを模索し，通常のセルオートマトンではなく，順序セルオートマトン上にソリトン解をもつモデルを構築してきた.

２．研究の目的

箱玉系は Yang-Baxter 方程式を満たす．現在，Yang-Baxter 方程式は格子模型における可解性(Ising 模型など) や力学系の可積分性(離散 KdV 方程式など) の十分条件であると考えられている．そこで本研究では，上述のフィルター型セルオートマトンの構築のため，有限体上に値をとる Yang-Baxter map を適用することを試みる.

現在，一般論としてセルオートマトンの「可積分性」はよくわかっていない．得られた系は格子模型の観点から構築したものであるが，保存量に関してはいまのところ自明なものを除き不明である．通常 Yang-Baxter 方程式が成立することは，パラメータ付きの転送行列が存在し，系が無限個の保存量を持つことを意味する．しかし有限体上に値を取るパラメータでは，明らかに無限個の保存量を与えない．この点については，代数的エントロピーによる可積分系の特徴づけと関連することが予想されるため，今後も数値実験を通して研究を行いたい．ところで, KdV 方程式などを含む QRT 写像は楕円関数によりパラメトライズされる不変曲線を持ち，Painlevé 方程式などとの関連からも近年盛んに研究されている．また，この QRT 写像の超離散版についても研究は進んでいる．このような(トロピカルも含む) 代数曲線を与える理論へ発展させることが可能であれば符号や暗号といった理論を含む，大変広い応用を持つことが期待できる.

３．研究の方法

一般的な状況においてセルオートマトンを 1+1 次元離散力学系として見たとき，その可積分性あるいは非可積分性はよくわかっていない．具体的な系に限っても，その保存量などについてよくわからないことが多い．そのため格子模型の探索そのものだけではなく，その保存量の探索にも数値実験が欠かせない．これを踏まえて，小さな有限体においてブルートフォース探索を数値的に行った．また理論的には，1 次元離散力学系としての integrality や Laurent 性などといった著しい特徴を持つ楕円数列と Somos 数列について考察した．その結果，暗号理論への応用が期待されることが示唆された.

４．研究成果

本研究においては，有限体上に値をとる格子模型に付随する力学系を主に構築した．そこで得られた有限体上におけるソリトン系は孤立波を保存し, 多項式表示を持つ新規な力学系である．また楕円数列とそれに付随する Somos 数列の一般解の Hankel 行列式表示のもつ性質を調べた．楕円数列は楕円曲線上の点列に等価なものであり，楕円曲線暗号や代数幾何において本質的である．さらには有限体上におけるソリトン系を与える枠組みに現れる代数系の暗号理論への応用に対して基本的な考察を行った.

５．主な発表論文等

〔雑誌論文〕（計 4 件）

(1) K Matsuya, F Yura, J Mada, H Kurihara and T Tokihiro, "A Discrete Mathematical Model for Angiogenesis", SIAM J. Appl. Math., 76(6), 2243--259 (2016). （査読あり）

(2) 間田潤，松家敬介，由良文孝，栗原裕基，時弘哲治，「血管新生の数理モデル」日本応用数理学会論文誌 26(1)，105-123（2016）．（査読あり）

(3) F YURA, "Hankel determinant solution for elliptic sequence", Linear Algebra and its Applications 484, 27-45 (2015). （査読あり）

(4) 由良文孝，「楕円曲線と Hankel 行列式」，九州大学応用力学研究所講究録 26AO-S2，163-169，2015．（査読あり）

〔学会発表〕（計 5 件）

(1) 由良文孝,「大域的 2 次元セルオートマトンのある拡張について」，日本応用数理学会(2018)．

(2) 由良文孝，田久保直子，林達也，間田潤，栗原裕基，時弘哲治,「排除体積効果を伴う 2 体相互作用におけるパターン形成について」，日本応用数理学会(2018)．

(3) 林達也，由良文孝，間田潤，時弘哲治，礪波一夫，栗原裕基,「血管新生における血管内皮細胞の基本動態に関する数理モデル」，日本応用数理学会(2018)．

(4) 間田潤，松家敬介，由良文孝，時弘哲治，栗原裕基，由良文孝,「血管新生の数理モデルについて」日本応用数理学会(2015)．

(5) 由良文孝,「楕円数列の Hankel 行列式解について」日本応用数理学会(2015)．

〔図書〕（計 0 件）

特になし

〔産業財産権〕

○出願状況（計 0 件）

特になし

○取得状況（計 0 件）

特になし

〔その他〕

特になし

６．研究組織

(1) 研究分担者

特になし

(2)研究協力者

特になし

※科研費による研究は，研究者の自覚と責任において実施するものです．そのため，研究の実施や研究成果の公表等については，国の要請等に基づくものではなく，その研究成果に関する見解や責任は，研究者個人に帰属されます．