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　６ 年　 ５ 月 ２０ 日現在

機関番号：３４４１９
研究種目：基盤研究(C)（一般）
研究期間：2020～2023
課題番号：２０Ｋ０３５２４

研究課題名（和文）ゼータ関数を用いた符号と不変式および暗号の数論的構造の研究

研究課題名（英文）Research of arithmetical structures of codes, invariant polynomials and cryptography using zeta functions

研究代表者

知念　宏司（Chinen, Koji）

近畿大学・理工学部・教授

研究者番号：３０４１９４８６

交付決定額（研究期間全体）：（直接経費）　　1,400,000円

研究成果の概要（和文）：本研究では、不変式のゼータ関数について研究を行ない、以下の２つの問題について結果を得た：(i) ある種の divisible な多項式系列に対するリーマン予想、(ii) 種数 3 および 4 の重み多項式に対するリーマン予想。問題 (i) では、 Type I, III, IV という、実在の符号の重み多項式に非常に近いが、変換規則が異なる divisible な多項式系列について考察した。その結果、Mallows-Sloane 限界式の類似が得られ、ある複数系列のリーマン予想が互いに同値であることがわかった。問題 (ii) では、種数 3、4 の場合に、リーマン予想の一つの同値条件を得た。

研究成果の学術的意義や社会的意義
線型符号のゼータ関数は 1999 年に導入され、符号の重み分布の情報を含んでいることから、符号理論、整数論両方の研究者の関心を集めてきた。特に「よい符号はリーマン予想を満たす」のではないかと考えられている。その後、研究代表者はその本質に迫ることを目指して、考察対象を広げて拡張を行なってきた。本研究期間においては、実在の符号の重み多項式に近い不変式においては、符号と類似の構造が見られることがわかった。また、実在の符号に関連する場合には、種数 3, 4 のときにリーマン予想の一つの同値条件が得られた。この方向はさらに大きな種数へ拡張できる可能性があり、今後の研究にもつながるものであると考えられる。

研究成果の概要（英文）：In this research, we investigated the zeta functions of invariant polynomials and obtained results on the following two problems: (i) the Riemann hypothesis for some families of divisible polynomials, (ii) the Riemann hypothesis for weight enumerotors of genera three and four. On the problem (i), we consider the families of invariant polynomials which are similar to the weight enumerators of existing codes (Types I, III and IV), but the transformation rule is a little different. We deduced the following results: analogs of the Mallows-Sloane bound, the fact that the Riemann hypothesis of certain sequences are equivalent. We also investigated a certain family of divisible polynomials, and we found that they satisfied similar properties to divisible weight enumerators of existing self-dual codes. On the problem (ii), we consider the weight enumerators of existing codes of genera three and four. we obtained a equivalent condition to the Riemann hypothesis in these cases.

研究分野：整数論、符号理論

キーワード：ゼータ関数　符号理論　整数論

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

本研究期間においては、線型符号のゼータ関数とそのリーマン予想について研究を行なった。線型符号のゼータ関数は、1999 年に導入された。これは符号の重み多項式の母関数となっているものであり、このことから線型符号の重み分布に関する情報を含んでいるものと考えられる。特に「extremal 自己双対符号はリーマン予想を満たすか？」という問題がある。Extremal 自己双対符号は誤り訂正能力が高い符号であるため、これは「よい符号はリーマン予想を満たす」というのが正しいかどうかを問う問題とも考えられる。このことから符号理論、整数論両方の研究者の注目を集めてきた問題である。なお、整数論分野で知られている多くのゼータ関数とは異なり、線型符号のゼータ関数には、リーマン予想を満たすものと満たさないものの両方が存在しており、リーマン予想を満たす線型符号の特徴づけという問題は、さらに大きな問題である。研究開始当初の状況では、上記の extremal 自己双対符号に関する問いは、一部の系列を除いて未解決であった（現在もそう）。他に、必ずしも符号とつながりのない、重み多項式型斉次多項式への拡張が行なわれ、そのリーマン予想へのアプローチが行なわれていた。そこでは、考察の対象を最大限広げると、リーマン予想を満たす重み多項式型斉次多項式が広い範囲に存在することがわかっている（Chinen 2008）。他に、自己双対符号の重み多項式に似るが異なる変換公式を満たす formal weight enumerator と呼ばれる多項式のある族では、実在の自己双対符号の場合と似た状況が起きていることがわかっている（Chinen 2005, 2019）。これとは別方向として、リーマン予想の必要十分条件を探る研究も存在していた。研究開始当初の先行研究としては、種数が 3 未満の自己双対重み多項式に対するリーマン予想の必要十分条件が得られていた（Nishimura 2008）。

２．研究の目的

上記のような状況のもと、本研究では、符号の重み多項式や、重み多項式型斉次多項式がどのような場合にリーマン予想を満たすのか、という問題に可能な限り迫る、ということを目的とした。そのために、まだ手掛けていない多項式系列のゼータ関数について、extremal という性質が定義できるかどうかを調べ、リーマン予想に関する考察を行なった。また、リーマン予想の必要十分条件を求めることも大きな目標であり、先行研究を、さらに種数の大きい場合に拡張する試みも行なった。

３．研究の方法

本研究で扱った問題は、2 つの系統に分かれる。一つは、実在の自己双対符号の重み多項式に似るが、変換規則が異なる多項式（以後 pseudo-invariant 多項式と呼ぶ）に関する問題、もう一つは通常の自己双対符号の重み多項式である。前者に対しては、実在の自己双対符号の場合と並行に議論が進むかどうか、違いは何か、といった点に注目して研究を進める方法を採った。後者に対しては、先行研究であるリーマン予想の必要十分条件を拡張すること（種数を大きくすること）が、どこまで可能かを探るという方法を採った。

４．研究成果

まず第一の場合、つまり pseudo-invariant 多項式の場合についての結果を述べる。このあと、変換規則（いわゆる MacWilliams 変換）に現れるパラメーターを q で表す。これは、実在の符号の場合には、考えている符号が定義される有限体の元の個数を表すパラメーターであり、その場合は素数のべきとなる数である。ただし、われわれは必ずしも実在の符号とは関連をもたない、重み多項式型の多項式を考察の対象としているため、素数べきという制限を取り除き、q は 1 と異なる正の実数というところまで拡張して議論を進める。このとき、q に対する MacWilliams 変換で、もとの式の -1 倍に変換される重み多項式型の多項式を pseudo-invariant 多項式と呼ぶことにする（研究代表者の以前の論文では formal weight enumerator と呼んでいた場合がある）。考察する q の値は、まず q=2,4 である。これは実在の自己双対符号の場合に、divisible code と呼ばれる重要な符号の族が存在する場合である。ここで divisible code とは、すべての符号語のハミング重みが、ある一定の数 c で割り切れるものをいう。これを重み多項式の言葉で言い換えると、0 でない項の y の指数がすべて c で割り切れること、となり、多項式の簡単な特徴で言い表すことができる。そのため pseudo-invariant 多項式に対しても、divisible という概念をそのまま持ち込むことができる。q=2,4 の場合には c=2 に対して divisible な自己双対符号の系列が存在する。そして、これと並行する形で、q=2,4, c=2 に対して divisible pseudo-invariant 多項式が存在するのである。なお、q=2 のときには c=4 に対しても divisible 自己双対符号が存在し、対応する pseudo-invariant 多項式も存在するが、その場合の一連の考察は、研究代表者による以前の研究で行なわれているため（Chinen 2005）、本研究期間では対象としていない。ここでもう一つ、divisible 自己双対符号で実在するものは有限個であることが古くから知られていることには注意を要する。しかしながら、divisible 自己双対重み多項式は、それが重み分布を表現する符号の存在、非存在にかかわらず、無限系列となっているので、

われわれはそうした多項式の無限列を考察の対象としているのである。したがってこの問題は実在の符号というよりも、重み多項式型多項式の無限列を対象としているものと言える。

まず $q=2$, $c=2$ の場合には $x^4-6x^2y^2+y^4$ という pseudo-invariant 多項式が存在する。これと x^2+y^2 という多項式を組み合わせることによって、$q=2$, $c=2$ に対するすべての pseudo-invariant 多項式が得られる。ここで x^2+y^2 は実在の自己双対符号の重み多項式として現れる多項式なので、この族は実在の自己双対符号に近いことがわかる。より詳しく、この族は Type I code と呼ばれる実在の自己双対符号の重み多項式をすべて含み、さらに広い「不変式環」を形成する。この族に対する最初の結果は Mallows-Sloane 限界式の類似である。Mallows-Sloane 限界式は、divisible 自己双対符号の場合に最小距離を符号長の式で上から評価するものであり、評価式で等号が成立するものは extremal code と呼ばれる。これらの評価式、概念は重み多項式の言葉で記述できる。実際に、符号長は重み多項式の次数であり、最小距離は、重み多項式における y の 0 でない最小次数である。こうしたことから、これらの概念は、符号と関連をもたない divisible pseudo-invariant 多項式にも容易に拡張できる。このことをふまえて、$q=2$, $c=2$ に対する pseudo-invariant 多項式の族に対して、Mallows-Sloane 限界式の類似を導出することを試み、成功した。証明には Duursma 2003 で導入された、偏微分作用素を利用する方法を採用した。

次に $q=4$, $c=2$ の場合には x^3-9xy^2 という pseudo-invariant 多項式が存在する。これと x^2+3y^2 という多項式を組み合わせることによって、$q=4$, $c=2$ に対するすべての pseudo-invariant 多項式が得られる。ここで x^2+3y^2 は実在の自己双対符号の重み多項式として現れる多項式なので、この族も実在の自己双対符号に近く、この系列は Type IV code と呼ばれる実在の自己双対符号の重み多項式をすべて含み、さらに広い「不変式環」を形成する。この族に対しても、$q=2$, $c=2$ の場合と同様に、Mallows-Sloane 限界式の類似を導出することに成功した。証明も同様に偏微分作用素を利用する方法である。

以上 2 つの族に対するリーマン予想を調べた。技術的な障害があり、以上 2 つの族で extremal なものに対するリーマン予想を証明するには至らなかったが、各族において、2 つの系列の extremal な多項式のリーマン予想が互いに同値であることがわかった。つまり、一方の系列のリーマン予想が正しいならば、他方も正しいということである。これは Okuda 2008 の pseudo-invariant 多項式における類似である。数値実験では、「extremal な pseudo-invariant 多項式はリーマン予想を満たすだろう」ということを窺わせる結果が出ている。

次にわれわれが考えたのは $q=4/3$ に対する pseudo-invariant 多項式である。4/3 は素数べきではないため、実在の符号とは関連をもたない。しかし $c=2$ に対して divisible pseudo-invariant 多項式が存在することが、研究代表者の以前の研究によりわかっている（Chinen 2019）。本研究期間においては、この多項式族のより詳細な研究を行なった。この族は 2 つの生成元をもつ。それらは $x^6-5x^4y^2+(5/3)x^2y^4-(1/27)y^6$ と $x^2+(1/3)y^2$ である。この族は従来符号の枠組みで研究されてきたものではないので、まず Molien 級数の計算から始めた。それによって pseudo-invariant 多項式の不変式環、そしてその部分環である、$q=4/3$ の MacWilliams 変換で不変な多項式のなす環が決定できた。そこでこれらの Mallows-Sloane 限界式の類似に取り組んだ。MacWilliams 変換で不変な多項式に対しては、実在の自己双対符号の場合に類似の不等式が得られた。しかし pseudo-invariant 多項式全体については、技術的困難により、多項式の次数が 12 を法として 6 に合同な系列に対してのみ証明ができた。証明の方法は、比較的古くから知られていた、解析学を援用する手法を採った。なお、$q=2,4$ の場合に用いた偏微分作用素を利用する手法は、$q=4/3$ では得られる不等式が弱く、適用できなかった。Mallows-Sloane 限界式が証明できた多項式族に対しては extremal という性質が定義できるため、リーマン予想の考察ができる。この場合も、リーマン予想自体の証明は不可能であったが、extremal pseudo-invariant 多項式の 2 つの系列に対して、リーマン予想が同値であることが示された。またこの場合にも数値実験では、「extremal な pseudo-invariant 多項式はリーマン予想を満たすだろう」ということを窺わせる結果が出ている。

他に、$c=3$ に対する divisible pseudo-invariant 多項式の族について研究を行なった。q の値としてはまず $q=3$ がある。これは Type III code と呼ばれる実在の自己双対符号の重み多項式をすべて含む環で、環自体すでに知られていたものであるが、今回 Mallows-Sloane 限界式の類似を証明した。これによって、Type I から IV までの divisible pseudo-invariant 多項式に対する Mallows-Sloane 限界式の類似がすべて出そろうこととなった。証明には偏微分作用素を利用する手法が適用可能であった。これによって、この族にも extremal という概念が導入でき、リーマン予想の考察を行なった、その結果、extremal pseudo-invariant 多項式の 2 つの系列のリーマン予想が互いに同値であることが示された。さらに、$c=3$ に対する divisible pseudo-invariant 多項式で、$q=3/2$ という値に対するものが見つかった。種々の計算の結果、実在の自己双対符号の重み多項式がなす環と同様の性質をもつと推定されるが、技術的困難があり、性質の理論的証明には至らなかった。数値実験では、リーマン予想を満たすと予想される実例が見つかっている。

続いて第二の場合、つまり、実在の自己双対符号の重み多項式に関するリーマン予想の同値条件について探る問題についての成果を述べる。われわれは種数が 3 および 4 の場合に同値条件を得ることができた。先行研究では 3 未満であったので、拡張に成功したことになる。証明手法であるが、先行研究では binomial moment を用いているため、計算はかなり複雑だったが、本

研究ではそれを回避する方法を開発したため、証明は大幅に簡易化された。従来より大きな種数まで計算ができたのも、この新しい方法によるところが大きい。この方法は先行研究で扱われている場合にも適用できるため、その簡単な別証明も得られた。

全体として、比較的多くの事実が判明したと言える。

5．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　2件）

1．著者名 Koji Chinen and Yuki Imamura	4．巻 57-1
2．論文標題 On the Riemann hypothesis for self-dual weight enumerators of genera three and four	5．発行年 2021年
3．雑誌名 SUT J. Math.	6．最初と最後の頁 55-75
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 CHINEN Koji	4．巻 43
2．論文標題 On Some Families of Certain Divisible Polynomials and Their Zeta Functions	5．発行年 2020年
3．雑誌名 Tokyo Journal of Mathematics	6．最初と最後の頁 1-23
掲載論文のDOI（デジタルオブジェクト識別子） 10.3836/tjm/1502179317	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 CHINEN Koji	4．巻 63
2．論文標題 On Some Families of Invariant Polynomials Divisible by Three and Their Zeta Functions	5．発行年 2021年
3．雑誌名 Mathematical Journal of Okayama University	6．最初と最後の頁 175-182
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計0件

〔図書〕　計0件

〔産業財産権〕

〔その他〕

－

6．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関