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

平成　３０　年　　６　月　　７　日現在

機関番号：　３４４１９
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2017
課題番号：　２６４０００２８

研究課題名（和文）暗号および符号に関連する数論的関数とゼータ関数の研究

研究課題名（英文）A Study of arithmetic functions and zeta functions related to the cryptography and coding theory

研究代表者

知念　宏司（CHINEN, Koji）

近畿大学・理工学部・准教授

研究者番号：３０４１９４８６

交付決定額（研究期間全体）：（直接経費）　　1,800,000円

研究成果の概要（和文）：情報通信に不可欠な「誤り訂正符号」には、純粋数学と関連をもつテーマがいくつかある。本研究期間においては、そのようなテーマの一つである「線型符号のゼータ関数」および関連する数学について研究を行なった。これは誤り訂正符号の理論と整数論の境界に位置するテーマである。具体的には、線型符号に対して定義される「重み多項式」に類似の多項式である "formal weight enumerator" の探索とそのゼータ関数の性質を調べることであり、新しい多項式の系列発見などの成果が得られた。

研究成果の概要（英文）：The error-correcting codes, which are indispensable for the communication, have several aspects related to pure mathematics. In this study, the author investigates one such aspect, "zeta functions for linear codes" and related topics. More precisely, the author finds new families of divisible formal weight enumerators and studies their properties.

研究分野：　整数論

キーワード：　ゼータ関数　リーマン予想　数論的関数

１．研究開始当初の背景

線型符号のゼータ関数は 1999 年に Iwan Duursma により導入された。それは符号の重み多項式の母関数という形で定義され、符号の重み分布に関するいろいろな情報を保持していると考えられている。また符号が自己双対である場合、そのゼータ関数は、代数曲線のゼータ関数と全く同じ形の関数等式をもつことから、リーマン予想も同じ形で定義するのが妥当と考えられる。このように、（自己双対）符号のリーマン予想は、代数曲線のリーマン予想の形式的類似として導入された面があるが、ただそれだけではなく、符号の何らかの性能を表しているのではないか、具体的には「リーマン予想を満たすのは性能のよい符号はではないか」という期待とともに導入された。こうした観点から、Duursma は extremal code に注目した。Extremal code とは, 体 $\mathbf{F}_2$, $\mathbf{F}_3$, $\mathbf{F}_4$ 上の自己双対符号であって、与えられた符号長 n に対して、最小距離 d が最も大きく取れるもの、より正確に言うと、Mallows-Sloane bound において等号が成立するもののことである。一般に符号の最小距離は大きいほど誤り訂正能力が高いため、extremal code は性能の良い符号であると言うことができる。Duursma はこの extremal code の系列に対して様々な観察、理論的考察、数値実験等を行ない、「『extremal code はリーマン予想を満たす』は正しいか」という問題提起を行なっている（2001 年)。そして Type IV と呼ばれる $\mathbf{F}_4$ 上の自己双対符号の系列のうち、ある部分系列について、この問題を肯定的に解決している（2003 年)。その後、Type IV の別のある部分系列に対しても肯定的に解決された（Okuda, 2008 年)。しかし、他の自己双対符号の系列（Type I から Type III および Type IV の残りの系列）に対しては、この問題は未解決である。ただし反例は見つかっておらず、恐らく正しいものと予想される。

このように、Duursma の問題は、符号の性能という応用上重要な側面と整数論的対象である符号のゼータ関数との関連を窺わせ、まさに応用数学と純粋数学の境界に位置する大変重要な問題である。ところで、extremal であることがリーマン予想を満たすための必要十分条件ではないことも、すでにわかっている。例えば、$\mathbf{F}_2$ 上の長さ 32 の extremal でない自己双対符号でリーマン予想を満たす例が見つかっている（Komichi, 2005 年、九州大学修士論文)。他にも同様の例が、符号長が小さいところで存在することがわかっている。

ここで一つ注意すべきことがある。それは、「符号のゼータ関数」は、必ずしも符号が実在しなくても定義可能だということである。このゼータ関数は符号の重み多項式の母関数であることをすでに述べたが、実際、それは重み多項式そのものに対して定義されるものであり、その重み分布を実現する符号が存在するかどうかには無関係に定義されるのである。このことは例えば、MDS 符号のゼータ関数という形で理論の核心部分で使われている他、$\mathbf{F}_2$ 上の長さ 72 の extremal code （実在するかどうかは未解決）の重み多項式がリーマン予想を満たすことを、Duurma は確かめている。したがって、この問題は、符号そのものよりも、重み多項式型の斉次多項式（その中で特に、いわゆる MacWilliams 変換で不変となるもの）に対する問題であると考えるべきものである。

筆者はこの点に特に注目し、符号とは必ずしも関連をもたない多項式も含む形での一般化を考察してきた。対象とするのは、重み多項式型の斉次多項式 $W(x,y)$ で、いわゆる MacWilliams 変換で不変に保たれるか、または $-W(x,y)$ に変換されるものである。前者を「不変式」、後者を "formal weight enumerator" と呼ぶことにする。この場合、符号の長さに対応するのは $W(x,y)$ の次数であり、最小距離に対応するのは、$W(x,y)$ における y の最小次数である。

筆者は 2008 年の論文で、このように考察の対象を最大限広げた不変式を考察したが、その結果、リーマン予想を満たす不変式が大量に存在し、しかも最小距離には関係せず広範囲の n, d の組に対して存在すること（実際、可能なすべての n, d の組に対してリーマン予想を満たす不変式が存在すること）がわかった。そのような不変式は、MDS 符号の重み多項式とその双対の重み多項式を、ある方法で組み合わせることで得られた。したがってこれは、具体的構成によって示された結果である。

筆者は他にも、小関氏の formal weight enumerator （Type II code の重み多項式に近縁の多項式）に対して、実在の Type II code の重み多項式と類似の現象も発見している（2005 年)。すなわち、この場合にも符号の場合に似た関数等式が成立し、その結果リーマン予想も同様に定式化できる。そして extremal の概念も定義できて、extremal な多項式はリーマン予想を満たすであろうことが数値実験の結果、観察されたのである。

符号のゼータ関数のリーマン予想に関する他の特筆すべき結果として、種数 1 の場合の Nishimura の結果がある。それは、種数 1 の自己双対重み多項式がリーマン予想を満たすための必要十分条件を与えたものである（2008 年)。種数 1 は大変限られた場合であるが、必要十分という形で条件が与えられた意義は大きく、しかもその条件が非常に簡単な形をしていることも興味深い。その論文ではさらに（形は幾分複雑にはなるが）種数 3 未満（半整数の種数も導入されている）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を導出しており、このテーマに関する重要な貢献となっている。

このように、符号のゼータ関数に関しては、Duursma の発見以来、いくつかの重要な展開が見られるものの、リーマン予想を満たすための必要十分条件を完全に求めるという重要な目標には未だ届いていないというのが現状であり、依然としてこれは解決が強く望まれる問題である。

２．研究の目的

本研究の究極の目標は、符号のゼータ関数がリーマン予想を満たすための必要十分条件を完全に求めるということであり、その実現に向けて、符号のゼータ関数の性質をより多角的に、詳細に解明していくことである。筆者による上述の 2008 年の結果、つまり、パラメーター d の大きさに関係なく、リーマン予想を満たす不変式が広範囲に存在するという現象は、幾分病的な現象と考えられる。筆者はこの病的な現象がなぜ生じたかを考察し、それは divisible という条件が欠落しているためではないかと予想した。ここで divisible というのは、符号で言えば、すべての符号語の重みが一定の数 c で割り切れることである（このとき符号は divisible by c であると言う）。また重み多項式の言葉で言えば、y の次数が c で割り切れるような項のみで重み多項式が表せているということである。実は、Duursma の問題に登場する自己双対符号の系列はこの divisible という性質をもっている。実際、Type I, IV code は divisible by 2 であり、Type II code は divisible by 4, Type III code は divisible by 3 である。古典的な Gleason-Pierce の定理により、実在の自己双対符号で divisible であるものは（自明なもの以外）これらの場合に限られることが知られている。したがって、実在の自己双対符号のみを考察の対象としていたのでは、これ以上新しいことは得られないと考えられる。そこで、これまで未発見の不変式または formal weight enumerator で divisible なものを探索する必要に迫られた。本研究の目的は、上述の状況に鑑み、新しい divisible な不変式または formal weight enumerator を構成し、その性質、特にそのゼータ関数のリーマン予想に関する知見を得ることにある。

３．研究の方法

研究の道具として用いるのは、重み多項式の moment 公式である。これは、重み多項式の係数と、双対重み多項式の係数の間の関係を与えるもので、符号理論における古典的な道具であるが、先述の Nishimura の結果においても有効に用いられるなど、今なお利用価値のある概念である。特に、考えている斉次多項式が自己双対な重み多項式（つまり上の意味での不変式）や formal weight enumerator の場合、その斉次多項式の係数たちが満たすべき連立 1 次方程式を与えるという側面をもっている。そこで筆者は、この連立 1 次方程式という意味付けに注目して、moment 公式を新しい斉次多項式系列探索の道具として用いるという方法を考えた。

４．研究成果

本研究では主に、divisible by 2 であるような formal weight enumerator の探索を行なった。つまり、

$$W(x,y)=x^n+A_d x^{n-d}y^d+\cdots$$

の形で、ある q に対する Macwilliams 変換で $-W(x,y)$ に移されるような多項式である。Formal weight enumerator で divisible by 2 という場合は、すでに述べたように moment 公式を係数の連立 1 次方程式と考えた場合、未知数の個数（n+1 個）と方程式の個数が一致する。しかも $W(x,y)$ においては x^n の係数 A_0 はつねに 1 でなければならない。つまり、係数の連立 1 次方程式は必ず非自明な解をもつのである。このことから、各次数 n に対して、このような formal weight enumerator が存在するための必要条件として、問題の連立 1 次方程式の係数行列の行列式が 0 であること、という簡明な条件が得られる。この係数行列は q を含んでいるので、（行列式）＝0 を q について解くことにより、各次数に対して formal weight enumerator が存在する q の候補が得られる。こうして、q の候補を求める方法が、アルゴリズムとして確立されることになる。ここで、一般的には（行列式）＝0 を解くことは大きな計算量を伴うことが多いが、本計算においては、ある次数 n （偶数）に対して q が求まった場合、その q はそれより大きな偶数次数の計算においても必ず解として現れる。その理由は、ある次数の divisible by 2 である formal weight enumerator $W(x,y)$ が見つかれば、$W(x,y)(x^2+(q-1)y^2)$ も formal weight enumerator divisible by 2 となるからである。そのため、数式処理ソフトなどによって q を求める計算は、比較的先の方まで大きな困難なく進めることができる。

なお、各 q に対して、divisible by c である formal weight enumerator のなす環（存在するならば）は、MacWilliams 変換で不変な式をも含んでいる。したがって、divisible by 2 において、 q=2,4 の場合は実在の自己双対符号（Type I, IV）の重み多項式も含まれる。このように、本研究は、必ずしも符号と関連しない斉次多項式を扱いながらも、応用上重要な不変式をも含む形で実行されている。

この点に関連して、実在の自己双対符号で divisible なものが存在するための必要十分条件（q の値）は、すでに述べた通り Gleason-Pierce の定理によって得られているが、Sloane によるその証明（1979 年）の

うち必要条件の部分は、論理的には formal weight enumerator 存在の場合も含んでいるものの、条件としては弱く、q の値の候補をこの条件によって絞り込むことはできない。われわれの方法は古典的方法よりはるかに強く、効率的に q の値の候補を求めることができるようになっている。これは本研究で得られた重要な成果の一つである。

実際の探索は、 $W(x,y)$ の次数の偶奇によって場合分けをして行なった。まず偶数次数の場合を述べる。deg $W(x,y)=2$ の場合には上に述べた連立 1 次方程式の係数行列はつねに正則であり、したがって divisible by 2 である formal weight enumerator は存在しない。deg $W(x,y)=4$ の場合には（行列式）$=0$ の解は $q=2$ のみである。そして実際、この場合には divisible by 2 である formal weight enumerator が存在する。それは $x^4-6x^2y^2+y^4$ である。これと、不変式である x^2+y^2 を合わせることで、$q=2$ に対する formal weight enumerator divisible by 2 の環が得られることになる。なお、この環は Type I 自己双対符号の重み多項式も含んでおり、本研究が実在の符号をも対象としていることを示している。deg $W(x,y)=6$ の場合には（行列式）$=0$ の解は $q=2$ の他に $q=4/3$ がある。つまり、$q=4/3$ のときに divisible by 2 である formal weight enumerator が存在する（具体形は省略する）。他にも q が 2 次無理数で divisible by 2 である formal weight enumerator が存在するようなものがいくつか発見された。これは大変驚くべきことで、 Gleason-Pierce の定理にとらわれていては気づかないことである。本研究におけるこの発見の意義は大変大きいと考えている。

さらに、今回発見した divisible formal weight enumerator の一部には、exremal と言うべき性質をもちながらリーマン予想を満たさないものが発見された。これは Duursma の問題の意義を考え直すべきであることを示唆していると思われ、今後のこの分野の研究に大きな影響を与える可能性のある発見であると考えている。

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）

〔学会発表〕（計３件）

① 知念　宏司：Divisible formal weight enumerator に対する Mallows-Sloane bound の類似, 日本数学会, 2018 年.
② 知念　宏司：Riemann 予想を満たさない extremal な多項式の構成, 日本数学会, 2017 年.
③ 知念　宏司：Divisible formal weight enumerator の構成, 日本数学会, 2017 年.

６．研究組織

(1)研究代表者

知念　宏司（CHINEN, Koji）
近畿大学・理工学部・准教授
研究者番号：30419486