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 ２４ 日現在

機関番号：３３３０２
研究種目：挑戦的萌芽研究
研究期間：2016～2018
課題番号：１６Ｋ１２３９５

研究課題名（和文）円分体の相対類数の行列式公式による実験計画の最適化

研究課題名（英文）Optimization of the experimental design by the determinant formula of the relative class numbers of cyclotomic field

研究代表者

谷口　哲也（Taniguchi, Tetsuya）

金沢工業大学・基礎教育部・講師

研究者番号：９０６２５５００

交付決定額（研究期間全体）：（直接経費）　　2,400,000円

研究成果の概要（和文）：新たな相対類数の行列式公式に関して，0,±1成分を持つ行列，Demjanenko 行列と2次指標を組み合わせた行列を構成した．
円分体の相対類数の計算を21円分体などに対して行った．これは約5億次行列の行列式を計算したことに相当し，行列式として直接計算するのは非常に困難な対象でも計算可能であることを実証した．素数p円分体の場合のDemjanenko行列式の桁数およびD-efficiencyの漸近的挙動の予想を定式化し，前者は特別の仮定なしに示し，後者はKummer予想の下で示した．

研究成果の学術的意義や社会的意義
一般に，組み合わせ最適化に関連した計算の計算量はNP 困難問題であることが多い．本研究で提案する相対類数計算はO(n の多項式時間で実行可能であり，その計算量の評価も行っている．従って相対類数を表現する±1成分の行列式の値も同計算量で求まり，その結果D-optimal design の近似解も多項式時間で得られる．純粋な整数論的対象である円分体の相対類数およびその行列式公式と，具体的な応用の計算の対象であるD-optimal design の間をつなぐ，最初の一歩を本研究では踏み出した．

研究成果の概要（英文）：With regard to the new relative class number determinant formula, we have constructed a matrix with 0, ± 1 components, and a matrix combining the Demjanenko matrix and the secondary index.
We calculated the relative class numbers of 21th cyclotomic field etc. This corresponds to the fact that the determinant of about 500 million-order matrix is calculated, and it has been demonstrated that it is possible to calculate objects that are very difficult to calculate directly as the determinant.
We have formulated the prediction of the asymptotic behavior of the Demjanenko matrix and the asymptotic behavior of the D-efficiency in the case of prime p-circles, the former is shown without any special assumptions, the latter under Kummer conjectures.

研究分野：代数学，整数論，計算数論

キーワード：円分体　相対類数　行列式　実験計画法　組み合わせ最適化　ランダム行列

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

実験計画法においては，実験効率を上げるために，±1 成分の行列 X で行列式 det(X) の値が大きいものを構成することが求められている．成分が±1 である n 次正方行列全体の集合の中で，行列式の値が最大となる行列 Xmax を D-optimal design とよぶ．行列式の値の上限は Hadamard や Ehlich によって与えられているが，Hadamard 行列（その成分の n 個の列ベクトルが n 次元超立方体をなす．すなわち行列式が最大となる）は，N = 2 や N = 4n(1　n < 167) の範囲では具体的に存在が知られており，一般の N = 4n でも存在するであろうという Sylvester 予想があるが，これは未解決である．

一方，円分体の相対類数の行列式公式のうち，成分が 0，1 のみのもの，±1 のみのものがあるが，これらの行列式の値の大きさが極端な大きさであり偶然とは考えにくいことを数値的に観察していた．このような背景のもと，円分体の相対類数の行列式公式が実験計画法などに応用できる可能性があるとの仮説をもって，研究を開始した．

２．研究の目的

本研究の目的は，成分が±1 である n 次正方行列全体の集合の中で，行列式の値が大きくなるような行列を具体的に構成すること，および値が大きくなる理由の解明である．この様な行列は実験計画法において実験を効率よく行うために用いられる．本研究では，その構成方法として円分体の相対類数の行列式公式の利用を提案する．相対類数の行列式公式は Demjanenko 行列（成分が 0, 1）など多く知られているが，これらの行列式の値は，係数をランダムに生成した行列式に比べて非常に大きな値をとることを応募者は数値実験にて観察している．本研究ではこの様な性質をもつ行列を特徴づけ，行列式の大きな行列を具体的に構成することを目標とする．

３．研究の方法

主に(a)，(b)，(c)の 3 項目を考察してゆく：

(a) 相対類数の行列式公式の構成：

±1 成分の行列式で相対類数を表現する新たな公式を構成する．

(b) 数値実験による行列式公式の評価：

(a) で得られた公式による数値実験および，同じ型のランダム行列式を大量に生成し，その分布状況を推定するための基礎データの蓄積および，それぞれの公式がどれだけ大きな値を出力するかの測定・評価を行う．

(c) 相対類数の大きさ，±1 係数の行列式の大きさの評価の考察：

ランダム行列や実験計画法，D-optimal design に関する文献を調査し，(a) の相対類数の行列式表示との関係を考察する．

(a) 相対類数の行列式公式の構成，

相対類数の行列式公式の既知のものを整理し，±1 を成分とする行列式の公式を複数構成する．この構成は連携研究者とともに行う．既知の公式としては Funakura-Tsumura による構成

$$\det\left((-1)^{R_p(uv^{-1})}\right)_{1\le u,v\le (p-1)/2} = (\text{初等因子}) \times h_p^- \quad (1)$$

があり，この行列式を用いて数値実験をするとランダムに作成した±1 成分の行列式より異常に大きな値をとっていることが確認できている．例えば次の表の様な結果は課題応募時に得られていた：

相対類数の行列式公式による値と Hadamard の上界との関係の例

p	行列の次数(a)	ランダム行列式(b)	行列式公式(c)	Hadamard の上界	比(b)/(c)
499	49	244 桁程度	287 桁	299 桁	96.2%
997	498	562 桁程度	649 桁	672 桁	96.6%
1433	716	867 桁程度	990 桁	1023 桁	96.8%

±1 以外を成分としてもつ行列式公式についても同様の結果がいくつか得られている．例えば Demjanenko Matrix（各成分が 0, 1）についても同様の結果が出ている（課題応募時の計算機資源ではさほど大規模な結果までは到達できていなかった）．

(a) 相対類数の大きさに関する文献調査．

まず，相対類数の大きさの評価，D-optimal design，ランダム行列に関する文献を調査し整理して理解しておく．ランダム±1 成分行列の期待値（平均）に関する文献として，Terence Tao, Van Vu による″On random ±1 matrices: Singularity and Determinant″については詳しく調べる．この論文では，行列の要素が±1 でそれぞれの確率が 1/2 であるようなランダム行列の行列式の期待値が $\sqrt{n!}\exp(O\sqrt{n\log n})$ であることを示している．

(b) 相対類数計算に関する計算プログラムの開発．

±1 成分のランダム行列の行列式の値を，いろいろなサイズに対して膨大に計算し，行列式の

値の分布の具体例を蓄積する必要があるため，そのためのプログラムを開発する．以前作成した相対類数計算プログラムが流用可能であり,それを用いた行列式計算は可能ではある.ただ,このプログラムは 1 億桁レベルの多倍長計算にチューニングしたものであり，小さな桁では却ってオーバーヘッドが大きいので，小さいサイズの行列式計算に向けて最適化したプログラムも新たに開発して能率的に行列式の値を計算し，基礎データを蓄積する．

(b) 相対類数の計算プログラムの改良.
当初は p ～ 数十万程度を想定しており，億のオーダーの p に対する相対類数計算は想定していなかったため，メモリの使い方に無駄がある．データ構造の見直しが必要となる．

現状では大きな乗算をブロック分割して Karatsuba 乗算に落とし込み，当面不要なメモリ領域は Disk に逃しているが，計算量は大きくなる．Karatsuba 乗算の代わりにブロックを一つの要素とみた「大 FFT 乗算」と，要素内の「小 FFT 乗算」による 2 段階 FFT 乗算を検討する．これは円周率の世界記録の計算が参考になると考えられる．
現状では複素数体上の FFT 乗算を用いており，整数データを double 型に変換するためメモリ使用効率が悪い．2011 年の応用数理学会で発表した「nega-cyclic convolution」を推し進めれば，整数のみで FFT 乗算が実現できる可能性がある．

(b) 相対類数計算の実行.
プログラム改良を踏まえ，行列式の計算を実行し，更なるデータの蓄積を行う．これはできるだけ早い段階で行いたい．行列式の値の生データは今回のデータの解析の中心となるためである．
現状のプログラムを早い段階から動かしておくことには意味がある．現状プログラムでもまだ計算しきれていない領域が沢山あること，プログラム改良がうまく行かなかった場合を想定しての対策，うまくいった場合の「検算」を兼ねる，などの理由による．また，新たに構成した行列式公式が出来次第，追加計算も実施する．

(c) 相対類数の大きさ，±1 係数の行列式の大きさの評価の考察.
新たに構成した相対類数の行列式公式とその数値実験結果の結果から，より大きな行列式の値を出力する公式を選出する．以上の結果をデータベースとしてまとめ，今後の研究のための基礎データとする．

４．研究成果
2016 年度，2017 年度，2018 年度，全体のまとめの流れで報告する．
■2016 年度
1. 成分が 0-1 タイプ，±1 のタイプ Demjanenko 行列（Hazama の 1990 年の論文）について数値実験を行い，いずれも「行列式の値が極端に大きい」という観察結果を得られた．比較対象として，ランダムな 0-1 成分・±1 成分の対称・非対称行列（計 4 種）を選び，それぞれの行列式値の度数分布の中で Demjanenko 行列式の値を位置づけた．その結果から±1 成分の Demjanenko 行列の方が，Hadamard の上界に近い値を取ることが確認できた．具体的には「±1 成分の Demjanenko 行列式の桁数と，Hadamard の上界の桁数の比は，（数値実験した範囲では）96%以上」であり，行列サイズを大きくしてゆくと，桁数の比は 96%からさらに上昇傾向にあることが数値的に確認できた．
ここに，「0-1 成分・±1 成分の対称・非対称行列，計 4 種の条件下で生成したランダムな行列式」の統計情報を p=499 の場合について記す．平均，分散等の数値は各条件下において 10 万件以上行列式を生成し，その $\log_2$ の値に関する統計情報であり，**行列式公式**の数値は各条件に合致するような円分体の相対類数の行列式公式の $\log_2$ の値である：

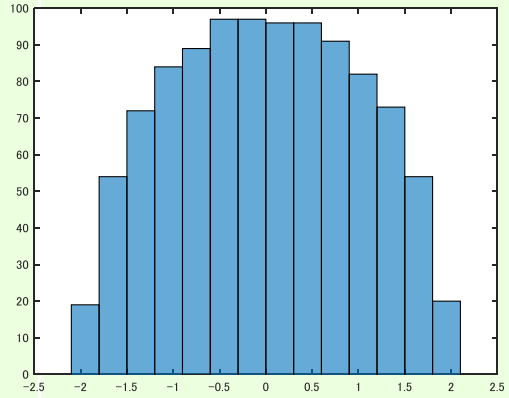
p =499	非対称		対称	
0，1 成分	平均： 分散： **行列式公式：**	565.036 7.41675 **705.388**	平均： 分散： **行列式公式：**	566.937 11.6786 **705.388**
±1 成分	平均： 分散： **行列式公式：**	810.005 7.57272 **953.388**	平均： 分散： **行列式公式：** **Hadamard の上限：991.02**	811.914 11.3971 **953.388**

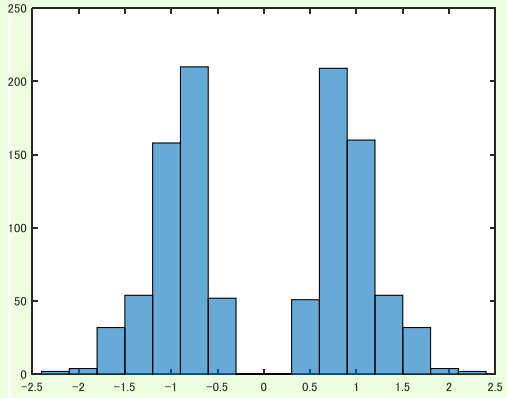
このように，p=499 の時点で Hadamard の上限が 2 進数で約 990 桁であるのに対して，行列式公式の 2 進桁数は約 950 桁以上もあることがわかる．

2. ±1 成分の Demjanenko 行列は実対称行列であり，固有値がすべて実数値であるが Weegner

の半円則から大きく外れた分布をするという観察結果を得た.

p=2047	Random±1 成分行列の固有値分布の例	Demjanenko 行列の固有値分布





Demjanenko 行列式の値が極端に大きくなる現象と固有値の分布状況の関係は数値的には見いだせたが，固有値分布のゆがみの原因は依然未解明であり，この分布を近似する分布が何であるかの特定も課題である．また，Demjanenko 行列の固有値と一般ベルヌーイ数の間の関係は，「複素共役の積」といった単純な関係ではないことが確認できている．試験的に BLAS・LAPACK を用いて固有値計算の数値実験を行ったところ，当該の行列に関しては，2 万次程度の行列の固有値計算が実用的な時間で実行可能であることは確認している．今後の数値実験の参考とする．

■2017 年度

1. Demjanenko 行列式の大きさに関する前年度までの観察結果を踏まえ，本年度は合成数分体の場合の Demjanenko 行列（Hirabayashi による一般化された公式を合成数円分体に制限したケース）と，素数 p 分体の場合とを比較した．その観察結果から素数 p 分体の場合の Demjanenko 行列式の桁数の漸近的な挙動について一つの予想を提案し，その予想が正しいことの証明にめどをつけた．Demjanenko 行列式の値が極端な大きさになる原因は，L 関数の特殊値（整数論）と結びついていることにあると考えられる．素数 p 円分体の場合の今後証明を完成し，論文として発表予定であり，合成数円分体に関しては数学的な予想として定式化し，証明する．

2. Demjanenko 行列は実対称行列であり固有値がすべて実数値であるが，その分布は Weegner の半円則から大きく外れており，絶対値が小さい固有値が極端に少ないという「Demjanenko 行列式の極端な大きさ」の傍証を得ていた．また Demjanenko 行列のその他いくつかの性質も特異であることは数値実験により観察している．今後の研究課題とする．

■2018 年度

Kummer 予想の仮定の下，素数 p 円分体の場合について±1 成分 Demjanenko 行列の D-efficiency の極限値を求めた．Kummer 予想の仮定を外して無条件に成立主張を構成するために，相対類数の評価式を踏まえて詳細を検討中である．また，合成数 n 円分体の場合に対応する予想を定式化することも課題である．

2019 年 10 月 31 日～11 月 3 日の実験計画法の研究集会「実験計画法ならびに情報数理と関連する組合せ構造 2018」に参加し，講演発表を行った．会場にて知り合った研究者たちからコメントやアドバイスをいただき，組み合わせ論の観点やグラフ理論の観点，確率分布の観点，実学への応用の観点からこの行列を解釈する必要があると判明した．

■全体のまとめ

(a) 相対類数の行列式公式の構成： 新たなタイプの行列式公式の作成について：
研究協力者（連携研究者）平林教授により，

- 新たなタイプの行列式公式（-1，0，1 成分）のものが得られている．成分に 0 も含んでいる関係で，行列式の値は±1 成分のものほどは大きくない．従って更なる改良の余地があると認識している．
- Demjanenko 行列と 2 次指標を組み合わせた行列

も候補として提案している．

(b) 数値実験による行列式公式の評価：
研究期間中に次の円分体の相対類数の計算を行い，基礎データの充実を図った：

- 2^{31} 円分体の相対類数計算を遂行した
- 素数 p 円分体の相対類数計算を p<30 万まで拡張した

新たに計算した 2^{31} 円分体の相対類数の値の桁数は，10 進数で 20 億桁程度である．対応する

行列式の値を,行列式のまま計算することは速度面でも記憶領域の面でも極めて困難であるが,本手法では行列式を経由することなく高速に計算を遂行できている.

(c) 相対類数の大きさ，±1 係数の行列式の大きさの評価の考察.

- Demjanenko 行列式の値の漸近的挙動について.
  - 素数 p 円分体の場合：
    - Demjanenko 行列式の桁数の漸近的挙動の予想を定式化し，証明した.
    - Demjanenko 行列の D-efficiency の値の漸近的挙動の予想を定式化し，Kummer 予想の仮定の下で証明した．Kummer 予想の仮定を外して証明することが課題である.
  - 合成数 n 円分体の場合：
    - Demjanenko 行列式の桁数の漸近的挙動の予想を定式化する必要がある.
    - Demjanenko 行列の D-efficiency の値の漸近的挙動の予想を定式化する必要がある.
- (a)で得られた公式については漸近的挙動が未解明である.
- 数値実験結果のデータについて
  - 相対類数の値： 研究期間中に 2^{31} 円分体の相対類数計算を遂行したこと，素数 p 円分体の相対類数計算を p<30 万まで拡張するなど，基礎データの充実を図った．公開方法は検討中である.
  - 行列式公式の固有値分布： 行列サイズ数千程度まで，Demjanenko 行列の固有値分布は計算し保存してある.
  - Demjanenko 行列に対して距離行列を計算し，固有値の分布も計算し保存してある.

●相対類数の行列式公式の解釈について今後の課題

今後，次のような観点で相対類数の行列式公式を解釈する必要がある.

- 組み合わせ論の観点： 特に球面上の代数的組み合わせ論.
- グラフ理論の観点： これらの行列に対応するグラフの特性の調査.
- 確率分布の観点： 固有値分布を記述するような確率分布の特定.
- 実学への応用の観点： 具体的にどの程度の程度のサイズの行列がどの分野で求められているかの調査.

５．主な発表論文等

〔雑誌論文〕（計 １件）

1. 谷口哲也,「円分体の相対類数の行列式公式の値の大きさの特異性について」, 第 16 回北陸数論研究集会（数論における行列式表示), 北陸数論研究集会報告集, 査読なし, 第 16 回, 2019, pp.28-34

〔学会発表〕（計１２件）

1. 第 197 回北陸数論セミナー

氏名：谷口哲也, 題目：円分体の相対類数の行列式公式の値の大きさと，その応用についての問題提起, 会場：金沢大学サテライトプラザ 2 階講義室, 日時：2016 年 11 月 10 日

2. 研究集会「九州代数的整数論 2017(KANT2017)」

氏名：谷口哲也, 題目：円分体の相対類数の行列式公式の値の大きさの特異性とその応用について, 会場：九州大学伊都キャンパス, 日時：2017 年 3 月 10 日

3. 第 203 回北陸数論セミナー

氏名：谷口哲也, 題目：円分体の相対類数の行列式公式の値の大きさについて, 会場：金沢大学サテライトプラザ 2 階講義室, 日時：2017 年 5 月 9 日

4. 香川セミナー

氏名：谷口哲也, 題目：円分体の相対類数の行列式公式の値の大きさと，その応用について, 会場：香川大学 教育学部, 日時：2017 年 10 月 28 日

5. 第 212 回北陸数論セミナー

氏名：谷口哲也, 題目：円分体の相対類数の行列式公式の値の大きさ，特に Demjanenko 行列と距離行列について, 会場：金沢大学サテライトプラザ 2 階講義室, 日時：2017 年 11 月 9 日

6. 第 16 回北陸数論研究集会

氏名：谷口哲也，題目：円分体の相対類数の行列式公式の値の大きさの特異性について，会場：富山大学理学部，日時：2017 年 12 月 26 日

7.　九大代数学セミナー

氏名：谷口哲也，題目：円分体の相対類数の行列式公式の値の大きさの特異性について，会場：九州大学伊都キャンパス，日時： 2018 年 2 月 16 日

8.　日本応用数理学会 「数論アルゴリズムとその応用」研究部会（JANT）

氏名：谷口哲也，題目：円分体の相対類数の行列式公式の値の大きさの特異性について，会場：大阪大学吹田キャンパス，日時：2018 年 3 月 16 日

9.　第 216 回北陸数論セミナー

氏名：谷口哲也，題目：Demjanenko 行列式の値の大きさの漸近的挙動について，会場：金沢大学サテライトプラザ 2 階講義室，日時：2018 年 5 月 10 日

10. 研究集会「実験計画法ならびに情報数理と関連する組合せ構造 2018」

氏名：谷口哲也，題目：「円分体の相対類数の行列式公式の値の大きさの特異性について」，会場：神戸大学，日時：2018 年 10 月 31 日

11. 日本応用数理学会 「数論アルゴリズムとその応用」研究部会（JANT）

氏名：谷口哲也，題目：「円分体の相対類数の行列式公式の値の大きさの特異性と D-efficiency について」，会場：筑波大学筑波キャンパス，日時：2019 年 3 月 4 日

12. 第 4 回 組合せ論・モデル理論セミナー【招待講演】

氏名：谷口哲也 ，題目：「円分体の相対類数の行列式公式の値の大きさの特異性について」，会場：神戸大学，日時：2019 年 3 月 8 日

〔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，該当なし

６．研究組織
(1)研究分担者：該当なし

(2)研究協力者
研究協力者氏名：平林 幹人
ローマ字氏名：Hirabayashi Mikihito

研究協力者氏名：藤井 俊
ローマ字氏名：Fujii Satoshi