2024年度共同利用研究報告書

2024年12月19日

所属・職名 日本文理大学工学部・准教授

黒田 匡迪

		整理番号	2024a017	
1.研究計画題目	Generalized Almost Perfect Nonlinear関数とFermat曲線についての研究討論			
2.新規・継続	新規			
3.種別	一般研究			
4.種目	短期共同研究			
5.開催方法	対面開催			
6.研究代表者	氏名	黒田 匡迪		
	所属 部局名	日本文理大学工学部	職名	准教授
7.研究実施期間	2024年09月20日(金曜日)～2024年09月24日(火曜日)			
8.キーワード	APN関数，GAPN関数，幾何学的既約，Fermat曲線			
9.参加者人数	6人			

10.本研究で得られた成果の概要

有限体上の非線形性が高い関数としてAlmost Perfect Nonlinear（APN）関数が研究されており，標数2の場合に暗号理論や符号理論へ応用されている．例えば，符号理論では，標数2の例外的APN関数の完全分類を与えることで例外的数の系列を決定した．一方で，奇標数の場合には，基礎研究が十分ではなく，これらの分野へ応用されていない．このことは，標数2の場合のある代数的性質が，奇標数の場合の既存の定義では成立しないことに起因していると考える．近年，標数2の場合の代数的性質を保つ奇標数への一般化であるGeneralized APN（GAPN）関数が定義され，国内外で研究されはじめている．本研究では，例外的GAPN関数の分類に関する研究の深化を目的とする．上記の通り，標数2の例外的APN関数は暗号理論・符号理論へと応用されているため，本研究で得られた結果を基に，これらの応用を一般化する形でGAPN関数の暗号理論・符号理論への応用に期待できる．

三井健太郎氏（琉球大学）とのこれまでの共同研究の中で，MAGMAを用いた数値実験により，標数3の特殊性を観察しており，主に標数3の場合に研究を行ってきた．これまでの研究において，例外的GAPN関数の特徴付けを次のように与えた：単項関数が例外的GAPN関数であるための必要十分条件は，その単項関数が定めるある代数曲線が基礎体上で定まる幾何学的既約成分をもたないことである．この特徴付けにより，例外的GAPN関数の分類に関する研究は，代数曲線の幾何学的既約成分の研究へと帰着できる．代数曲線が基礎体上で定まる幾何学的既約成分をもつか否かの判定は，この代数曲線の特異点の個数評価の問題に帰着できる．この問題は，有限体上のFermat曲線の有理点の個数評価の問題へと部分的に帰着できる．必要な個数評価の予想は既に見出しており，数値実験では予想成立の確らしさを確認できている．この予想の解決を目標に，新たに星明考氏（新潟大学）を加え，3名での短期共同研究を実施した．

採択から研究討論までの間も上記予想の解決に取り組んできた．本研究討論の直前に実施した研究集会において，深澤知氏 (山形大学) から頂戴したアイディアにより，上記予想の部分的解決が得られている．本研究討論においては，星明考氏からFermat曲線の有理点の個数とJacobi和や円

成果報告書：Generalized Almost Perfect Nonlinear関数とFermat曲線についての研究討論

研究代表者：黒田　匡迪　(日本文理大学)
参加者：三井　健太郎　(琉球大学)
星　明考　(新潟大学)

1. 本研究討論の目的と期待される成果

有限体上の非線形性が高い関数としてAlmost Perfect Nonlinear（APN）関数が研究されており，標数2の場合に暗号理論や符号理論へ応用されている．例えば，暗号理論では，差分解読法や線形解読法などの攻撃方法に対して高い耐性を有するブロック暗号アルゴリズムを構築する上で重要な部品の1つであるとされている．また，符号理論では，標数2の例外的APN関数の完全分類を与えることで例外的数の系列を決定した[2]．一方で，奇標数の場合には，基礎研究が十分ではなく，これらの分野へ応用されていない．このことは，標数2の場合のある代数的性質が，奇標数の場合の既存の定義では成立しないことに起因していると考える．近年，標数2の場合の代数的性質を保つ奇標数への一般化であるGeneralized APN（GAPN）関数が定義された[3]．標数2のAPN関数でないものも奇標数のGAPN関数になり得る．特に，応用上このような生成関数が多く得られることは利点であり，産業への応用も期待できる．GAPN関数は，国内外で研究されはじめており，暗号理論の専門誌に掲載された学術論文もある．本研究では，例外的GAPN関数の分類に関する研究の深化を目的とする．上記の通り，標数2の例外的APN関数は暗号理論・符号理論へと応用されているため，本研究で得られた結果を基に，これらの応用を一般化する形でGAPN関数の暗号理論・符号理論への応用に期待できる．

共同研究者の三井健太郎氏（琉球大学）とのこれまでの研究の中で，MAGMA[1]を用いた数値実験により，標数3の特殊性を観察している．例えば，標数5以上の場合には例外的GAPN関数のいくつかの族が構成されており，現時点では体系的研究の困難が見込まれるが，標数3の例外的GAPN関数は1つの族しか見つかっておらず，この族以外には存在しないと予想している．加えて，標数3の場合はFermat曲線と関係しているため，学際的研究の推進も期待できる．そのため，主に標数3の場合に研究を行ってきた．これまでの研究において，例外的GAPN関数の特徴付けを次のように与えた：単項関数が例外的GAPN関数であるための必要十分条件は，その単項関数が定めるある代数曲線が基礎体上で定まる幾何学的既約成分をもたないことである．この特徴付けにより，例外的GAPN関数の分類に関する研究は，代数曲線の幾何学的既約成分の研究へと帰着できる．

代数曲線が基礎体上で定まる幾何学的既約成分をもつか否かの判定は，この代数曲線の特異点の個数評価の問題に帰着できる．必要な個数評価の予想は既に見出しており，数値実験では予想成立の確らしさを確認できている．この問題は有限体上定義されたFermet曲線の有理点の個数と密接に関係しており，代数幾何・数論・数論幾何においても興味深い内容である．この特異点の個数評価に関する研究について，新たに星明考氏（新潟大学）を加え，3名での短期共同研究を実施した．

2. 採択から会合までの準備段階で得られた成果

本研究では主に，標数3の例外的単項GAPN関数の分類問題に取り組んでいる．この問題は，Feramt 曲線 $C(u)\colon x^u + y^u + z^u = 0$ の $\mathbb{F}_{3^f}$ 上の有理点 $C(u)(\mathbb{F}_{3^f})$ (ただし，$u \mid (3^f - 1)$) の個数評価の問題へと部分的に帰着できる．具体的には，次の不等式を満たす u の条件を決定したい：

$$\#C(u)(\mathbb{F}_{3^f}) < \frac{u^2(v+4)}{4} \qquad (\text{ただし，} v \coloneqq (3^f-1)/u). \tag{1}$$

MAGMA[1] を用いた数値実験により，次を予想している．

予想 2.1. $v \not\equiv 0 \mod 3$ に対して，f を $3 \in (Z/vZ)^\times$ の位数，$u \coloneqq (3^f-1)/v$，e を $3 \in (Z/uZ)^\times$ の位数とする．以下の場合を除いて，不等式 (1) が成り立つ：

(i) $u = 1$，2；

(ii) $u = 4$ (このとき $e = 2$) かつ $\dfrac{f}{2}$ が奇数；

(iii) $e = f$ のとき，$e = f$ は偶数，かつ，$\dfrac{3^{f/2}+1}{u} = 2$，4.

採択から会合までの間も三井健太郎氏と共に上記予想の解決に取り組んできた．予想 2.1 (i)–(iii) のとき，不等式 (1) が成立しないことは証明できているが，逆については部分的解決にとどまっていた．本会合の直前に実施した研究討論において，深澤知氏 (山形大学) から頂戴したアイディアにより，予想 2.1 の部分的解決が得られている：

定理 2.2. $u \notin \{1, 2\}$ とし，$r \in \mathbb{Z}_{>0}$ を次で定める：

$u \equiv 1 \mod 3$ の場合，$3^r \mid (u-1)$ かつ $3^{r+1} \nmid (u-1)$
$u \equiv 2 \mod 3$ の場合，$3^r \mid (u-2)$ かつ $3^{r+1} \nmid (u-2)$

このとき，次が成り立つ：

$$\#C(u)(\mathbb{F}_{3^f}) \le \begin{cases} \dfrac{u^2(v+2)}{3^r} & (u \equiv 1 \mod 3), \\ \dfrac{2u^2(v+1)}{3^r} & (u \equiv 2 \mod 3). \end{cases}$$

特に，$r \ge 2$ のとき，不等式 *(1)* が成り立つ．

3. 本研究討論で得られた成果

本研究討論は，2024年9月20日から9月24日の間に実施された（9月20日は公開プログラム，9月21日～9月24日は非公開プログラム）．公開プログラムでは，星明考氏を含む参加者に向けて下記内容で講演を行い，本研究討論における目的や到達目標 (予想 2.1 の解決) について共有した：

- 講演タイトル：3-exceptional monomial GAPN functions
  （講演者：三井 健太郎（琉球大学））
- 講演タイトル：3-例外的単項GAPN関数の分類に関係するFermat曲線について
  （講演者：黒田 匡迪（日本文理大学））

上記講演では，先行研究である APN 関数の導入から始め，GAPN 関数の研究へと広がった背景や上記 Fermat 曲線の有理点の個数評価との関係などについて網羅的に解説を行った．星明考氏の他に，落合啓之氏 (九州大学)，片桐宥氏 (九州大学)，岡田拓三氏 (九州大学) の 3 名にご聴講いただき，本研究へのコメントや質問を頂戴した．特に，星明考氏からは Jacobi 和や円分数との関係をご指摘いただき，非公開プログラムにおける研究討論へと発展していった．

非公開プログラム（9 月 21 日〜9 月 24 日）では，黒田匡迪，三井健太郎氏，星明考氏の 3 名で上記の Fermat 曲線の有理点の個数評価について研究討論を行った．各参加者の主な役割は下記の通りである．

1. 黒田匡迪：全体の統括を行った．研究討論を進めていく中で必要に応じて GAPN 関数についての解説を行い，議論が円滑に進むように努めた．

2. 三井健太郎氏：代数曲線の特異点や有理点の個数評価といった本研究と関係する代数幾何に関する専門知識について適宜，解説していただいた．加えて，計算機による数値実験を担当していただいた．

3. 星明考氏：Fermat 曲線の有理点の個数と Jacobi 和や円分数との関係についてご指摘いただき，これらの専門知識を集中講義形式で解説していただいた．

本研究討論の到達目標である予想 2.1 の解決には至っていないが，星明考氏に Jacobi 和や円分数との関係について解説していただくことで，本研究の問題や関連する内容の理解を深めることができた．特に，Fermat 曲線の有理点の個数を円分数を用いて記述することで，任意の奇標数の場合に問題を拡張することができる．三井健太郎氏は，この問題について数値実験を行い，奇標数の場合に不等式 (1) が成り立たないような系列を予想するなど興味深い新たな課題を見出すことができた．今後の共同研究への発展にも期待ができる．

参考文献

[1] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR 1484478

[2] Fernando Hernando and Gary McGuire, *Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions*, J. Algebra **343** (2011), 78–92. MR 2824545

[3] Masamichi Kuroda and Shuhei Tsujie, *A generalization of APN functions for odd characteristic*, Finite Fields Appl. **47** (2017), 64–84. MR 3681081

[4] Ana Sălăgean and Ferruh Özbudak, *Further constructions and characterizations of generalized almost perfect nonlinear functions*, Cryptography and Communications **15** (2023), no. 6, 1117–1127.

九州大学 IMI 共同利用・短期共同研究　公開プログラム

Generalized Almost Perfect Nonlinear関数とFermat曲線についての研究討論

Workshop on Generalized Almost Perfect Nonlinear functions and Fermat curves

9月20日（金）

13:00-14:00

講演者：三井　健太郎（琉球大学）

講演タイトル：3-exceptional monomial GAPN functions

14:30-16:00

講演者：黒田　匡迪（日本文理大学）

講演タイトル：3-例外的単項 GAPN 関数の分類に関係する Fermat 曲線について

※研究実施期間：2024 年 9 月 20 日(金)～9 月 24 日(火)

※公開日：2024 年 9 月 20 日(金)

ＨＰ掲載用英文

Speaker: Kentaro Mitsui (University of the Ryukyus)

Title: 3-exceptional monomial GAPN functions

Speaker: Masamichi Kuroda (Nippon Bunri University)

Title: On Fermat curves related to the classification of 3-exceptional monomial GAPN functions