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　５ 年　 ４ 月 ２７ 日現在

機関番号：１４２０２
研究種目：基盤研究(C)（一般）
研究期間：2017～2022
課題番号：１７Ｋ０５３４４

研究課題名（和文）符号構成のための代数曲線の探求とその規則性の解明

研究課題名（英文）Algebraic curves for coding theory and their properties

研究代表者
川北　素子（Kawakita, Motoko）

滋賀医科大学・医学部・准教授

研究者番号：８０４６７３７３

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：有限体上において多数の有理点をもつ代数曲線を発見した。種数５について、最大曲線でないセール上界に達する代数曲線と最大曲線を見つけた。種数６について、最大曲線となるWimanの６次曲線の性質を調べた。種数７について、最大曲線でないセール上界に達する代数曲線と最大曲線を見つけた。種数１０について、新しい最大曲線を発見した。また、データベースhttp://www.manypoints.org/を更新した。

研究成果の学術的意義や社会的意義
ICT 社会基盤の正確性を保つため、誤り訂正符号の理論は不可欠である。 1970年代にゴッパが代数幾何符号を発見した。その理論を用いると、有限体上において多数の有理点をもつ代数曲線から、効率のよい符号が構成できる。本研究の成果は、有限体上において多数の有理点をもつ代数曲線にあり、将来的に実用への貢献が期待できる。また代数曲線論は古くからある純粋数学の研究分野である。存在が知られていない代数曲線を、本研究において具体的に定義方程式を与えたので、数学としても意義がある。

研究成果の概要（英文）：We find algebraic curves over finite fields with many rational points. For genus 5, we find maximal curves and algebraic curves attaining the Serre bound which are not maximal. For genus 6, we analyze the property of the maximal curves of the Wiman sextics. For genus 7, we find maximal curves and algebraic curves attaining the Serre bound which are not maximal. For genus 10, we find new maximal curves and compute their Jacobian decompositions. Also, we update the database http://www.manypoints.org/.

研究分野：多数の有理点をもつ代数曲線

キーワード：代数曲線　有理点　符号理論

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　(共通)

１．研究開始当初の背景

ICT 社会基盤の正確性を保つため、誤り訂正符号の理論は不可欠である。1970 年代にゴッパが代数幾何符号を発見した。その理論を用いると、有限体上において多数の有理点をもつ代数曲線から効率のよい符号が構成できる。代数曲線論は古くからある数学の研究分野である。しかし有限体上の代数曲線について未知の部分が多く残されている。

２．研究の目的

本研究は、有限体上の代数曲線の中で、効率のよい符号を構成するものの発見と規則性の解明を目指す。具体的に述べると、セール上界に達するものをターゲットに絞っている。最大曲線とそうでないものがあるが、それぞれの特徴を明らかにしたい。研究期間中に、すべてを解明することが困難なため、種数が比較的小さいものに重点を置く。

３．研究の方法

本研究は 3 つの段階に分けて進めた。
(1) 色々な代数曲線についてヤコビアン分解を計算する。
(2) ヤコビアン分解できた代数曲線についてコンピュータ探索を行い、セール上界に達するで具体例を発見する。
(3) 最大曲線とそうでないものに分けて、それぞれの特徴を解析する。

４．研究成果

研究成果を種数ごとに分類して、以下順番に抜粋して解説する。

(1) 種数 5 の代数曲線
k を標数 p の体とし、$p \neq 2, 3, 5$ とする。次のような 6 次代数曲線 C を k 上に定義した。

$$C : x^3y^3 + x^5 + y^5 + ax^2y^2 + bxy + c = 0,$$

ただし $a, b, c \in k$ and $c \neq 0$。
ヤコビアン分解を計算し、コンピュータ探索した結果、以下の具体例を得た。

$$x^3y^3 + x^5 + y^5 + 2x^2y^2 + 4xy + 25 = 0$$

は有限体 $\mathbb{F}_{31}$ 上で 82 個の有理点をもつ。
さらに C は $(q, a, b, c) \in \{(71, 4, 46, 36), (191, 134, 126, 2), (11^5, 10, 9, 10)\}$ のとき有限体 $\mathbb{F}_q$ 上でセール上界に達する。加えて、データベース `http://www.manypoints.org/` を右表のように更新できた。

$\mathbb{F}_q$	$\#C(\mathbb{F}_q)$	old entry
31	82	-82
71	152	-152
11^5	165062	-165062

次に、最大曲線に関する結果を紹介する。
$(p, a, b, c) \in \{(29, 17, 28, 28), (31, 1, 3, 7), (41, 28, 29, 31),$
$(59, 9, 16, 28), (61, 11, 9, 10), (71, 0, 62, 64), (79, 5, 10, 12),$
$(89, 8, 20, 8), (101, 46, 89, 38), (109, 4, 87, 7), (131, 0, 107, 97),$
$(139, 2, 43, 122), (149, 5, 43, 59), (151, 5, 41, 115), (179, 7, 152, 90), (181, 67, 41, 18), (191, 2, 9, 17),$
$(199, 17, 196, 24)\}$ のとき、C が有限体 $\mathbb{F}_{p^2}$ 上で最大曲線となる。ここから予想を与えた:
$p > 23$、$p \equiv \pm 1 \pmod 5$ のとき、種数 5 の代数曲線 C が存在し、有限体 $\mathbb{F}_{p^2}$ 上で最大曲線となる。まだ証明できていない。

(2) 種数 7 の代数曲線

$p \neq 2, 3$ とし、k を標数 p の体とする。k 上で代数曲線 W を定義した。

$$W : x^4y^2 + y^4 + x^2 + x^2y^4 + y^2 + x^4 + bx^2y^2 = 0,$$

ただし $b \in k$。

楕円曲線を $E_i : y^2 = xf_i(x)$ $(i = 1, 2, 3)$

$$\begin{aligned} f_1(x) &= x^2 - bx - (b-3), \\ f_2(x) &= (x-1)(x-(b-2)), \\ f_3(x) &= x^2 + (b^2-12)x - 16(b-3) \end{aligned}$$

とすると、代数曲線 W のヤコビアンは体 k 上で完全分解する:

$$J_W \sim E_1^3 \times E_2^3 \times E_3$$

つまり、種数 7 である。また、

$$\begin{aligned} \overline{A}_1 &= \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m!}{(i!)^2(m-2i)!}(-1)^{m-i}b^{m-2i}(b-3)^i, \\ \overline{A}_2 &= H_p(b-2) = \sum_{i=0}^{m} \binom{m}{i}^2 (b-2)^i, \\ \overline{A}_3 &= \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m!}{(i!)^2(m-2i)!}(-16)^i(b^2-12)^{m-2i}(b-3)^i \end{aligned}$$

とおくと、定理を得る: $b \in \mathbb{F}_p$ のとき、代数曲線 W が有限体 $\mathbb{F}_{p^2}$ 上で最大曲線であることと

$$\overline{A}_1 \equiv \overline{A}_2 \equiv \overline{A}_3 \equiv 0 (\bmod p)$$

は必要十分である。

最後に、$(p, b) \in \{(21313, 3663), (30269, 10886), (61519, 56766), (76163, 6230)\}$ のとき、代数曲線 W は有限体 $\mathbb{F}_{p^3}$ 上で Serre 上界に達する。

(3) 種数 10 の代数曲線

有限体 $\mathbb{F}_{p^2}$ 上で代数曲線 $U_{p,b}$ を定義した。

$$U_{p,b} : x^6 + y^6 + 1 + bx^2y^2 = 0$$

$p \geq 5$ のとき、 代数曲線 $U_{p,b}$ は種数が 10 であり、ヤコビアン分解は

$$Jac(U_{p,b}) \simeq_{\mathbb{F}_{p^2}} E_1^3 \times E_2 \times E_3^3 \times E_4^3$$

となる。ただし、楕円曲線は

$$\begin{aligned} E_1 : y^2 &= x^3 + 3(b+6)x^2 + 3(b+3)(b+12)x + 27(b+3)^2, \\ E_2 : y^2 &= x^3 - 3^3b^2x^2 + 2^33^3b(b^3+27)x - 3^32^4(b^3+27)^2, \\ E_3 : y^2 &= x^3 + 2bx^2 + b^2x - 2^2, \\ E_4 : y^2 &= x^3 - 48b^2x^2 + 768b(b^3+27)x - 4096(b^3+27)^2 \end{aligned}$$

である。

さらに、$(p, b) \in \{(89, 58), (101, 96), (131, 100), (191, 116), (227, 69), (239, 94), (251, 3)\}$ のとき、代数曲線 $U_{p,b}$ は有限体 $\mathbb{F}_{p^2}$ 上で最大曲線となる。

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4件／うち国際共著　2件／うちオープンアクセス　0件）

１．著者名 M. Giulietti, M. Kawakita, S. Lia, M. Montanucci	４．巻 21
２．論文標題 An Fp2-maximal Wiman sextic and its automorphisms	５．発行年 2021年
３．雑誌名 Advances in Geometry	６．最初と最後の頁 451-461
掲載論文のDOI（デジタルオブジェクト識別子） 10.1515/advgeom-2020-0012	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 該当する

１．著者名 D. Bartoli, M. Giulietti, M. Kawakita, M. Montanucci	４．巻 68
２．論文標題 New examples of maximal curves with low genus	５．発行年 2020年
３．雑誌名 Finite Fields and Their Applications	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.ffa.2020.101744	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 該当する

１．著者名 M. Kawakita	４．巻 11321
２．論文標題 Some sextics of genera five and seven attaining the Serre bound	５．発行年 2018年
３．雑誌名 Lecture Notes in Computer Science	６．最初と最後の頁 264-271
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-05153-2_15	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 M. Kawakita	４．巻 4
２．論文標題 Wiman's and Edge's sextic attaining Serre's bound	５．発行年 2018年
３．雑誌名 European Journal of Mathematics	６．最初と最後の頁 330-334
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s40879-017-0147-3	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 －

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 M. Kawakita
２．発表標題 Some sextics of genera five and seven attaining the Serre bound
３．学会等名 International Workshop on the Arithmetic of Finite Fields（国際学会）
４．発表年 2018年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

SUMS -Math- http://www.shiga-med.ac.jp/~kawakita/

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			
イタリア	University of Perugia			
デンマーク	Technical University of Denmark			