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　２９　年　　５　月　３０　日現在

機関番号：　１４２０２
研究種目：　若手研究(B)
研究期間：　2013～2016
課題番号：　２５８０００９０

研究課題名（和文）符号理論のための代数曲線の研究

研究課題名（英文）Research on algebraic curves in coding theory

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）　　3,200,000円

研究成果の概要（和文）：　1970年代にGoppaが代数幾何符号を発見した．有限体上において多数の有理点を持つ代数曲線から，効率良い線形符号を構成できることを明らかにした．代数曲線論は数学において古くからある研究分野である．近年暗号理論でも代数曲線が応用されるようになった．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．符号理論の視点に立つと，最適曲線は代数幾何符号構成に最も有効である．最大曲線について既に多くの研究成果が出ている．けれども最大曲線でない最適曲線の性質は五里霧中である．本研究の最大の成果は，最大曲線でない代数曲線の中からSerre上界に達するものを発見したことである．

研究成果の概要（英文）：　In 1970's Goppa discovered algebro-geometric codes, where we need explicit curves with many rational points to construct good codes. A curve attaining the Hasse-Weil bound is called a maximal curve, and there are many interesting research on it. However we do not know the property of a curve attaining Serre's bound which is not maximal. Recently we found that the sextics, defined by Wiman in 1895 and by Edge in 1980, attain the Hasse-Weil-Serre bound over some finite fields. For some sextics among them, we determined the precise condition on the finite field over which the sextics attain the Hasse-Weil-Serre bound.

研究分野：　代数幾何符号

キーワード：　代数曲線　符号理論　有理点

様　式　C－19、F－19－1、Z－19　(共通)

１．研究開始当初の背景

1970 年代に Goppa が代数幾何符号を発見した．有限体上において多数の有理点をもつ代数曲線から，効率良い線形符号を構成できることを明らかにした．代数曲線論は数学において古くからある研究分野である．近年暗号理論でも代数曲線が応用されるようになった．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がメインテーマである．最適曲線は代数幾何符号構成に最も有効である．最大曲線について既に多くの研究成果が出ている．けれども最大曲線でない最適曲線の性質は五里霧中である．その中でターゲットを絞って，Serre 上界に達する最大曲線でない代数曲線の存在と性質を明らかにしたい．研究期間 4 年間において，全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られる．
(1) Serre 上界に達する代数曲線について種数 3 以上では，僅かな具体例しか知られていないので，まずコンピュータ探索で具体例を発見する．
(2) 発見した具体例の定義方程式を解析し，試行錯誤しながら予想を立てる．
(3) 最終的に予想を証明する．

４．研究成果

研究成果は 3 つの部分に分けられる．以下順番に解説する．

(1) Wiman 曲線

古典的な代数曲線の論文から Serre 上界に達するものを発見できた．1896 年に発表された Wiman の論文である．その代数曲線を Wiman の 6 次曲線と呼び，得られて研究成果を紹介する．

素数 $p > 5$ とし，k を標数 p の体とする．k 上の Wiman の 6 次曲線は次のように定義される．

$$\begin{aligned} W\colon\ & x^6+y^6+1 \\ & +a(x^4y^2+x^2y^4+x^4+x^2+y^4+y^2) \\ & +bx^2y^2=0. \end{aligned}$$

① Wiman の 6 次曲線のヤコビ多様体は以下のように k 上完全分解する．

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

楕円曲線は $E_1\colon y^2 = xf_1(x)$, $E_2\colon y^2 = xf_2(x)$,

$$\begin{aligned} f_1(x) &= x^2+(a-3)(7a+6)x-(a-3)(2a+3)^3, \\ f_2(x) &= x^2-(a-3)(a+2)x-(a-3)(2a+3) \end{aligned}$$

で定義される．

② 有限体 $\mathbb{F}_p$ 上で定義された Wiman の 6 次曲線を考える．$b=-6a-3$, $m=(p-1)/2$ とし，

$$\overline{A}_1 = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m!}{(i!)^2(m-2i)!} S_{i,a},$$

$S_{i,a} = (-1)^i(a-3)^{m-i}(7a+6)^{m-2i}(2a+3)^{3i}$,

$$\overline{A}_2 = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m!}{(i!)^2(m-2i)!} T_{i,a},$$

$T_{i,a} = (-1)^{m-i}(a-3)^{m-i}(a+2)^{m-2i}(2a+3)^i$
とする．

$p \geq 17$ のとき，有限体 $\mathbb{F}_p$ 上の Wiman の 6 次曲線 W が Serre 上界に達する必要十分条件は

$$\overline{A}_1 \equiv \overline{A}_2 \equiv -\lfloor 2\sqrt{p} \rfloor \pmod{p}$$

である．

③ $a \in \mathbb{F}_p$ とする．有限体 $\mathbb{F}_{p^2}$ 上の Wiman の 6 次曲線 W が最大曲線となる必要十分条件は

$$\overline{A}_1 \equiv \overline{A}_2 \equiv 0 \pmod{p}$$

である．

④ $p \geq 11$, $a \in \mathbb{F}_p$ とする．有限体 $\mathbb{F}_{p^3}$ 上の Wiman の 6 次曲線 W が Serre 上界に達する必要十分条件は

$$A_1^3 - 3pA_1 = A_2^3 - 3pA_2 = -\lfloor 2p\sqrt{p} \rfloor$$

である．

⑤ 論文発表時において，データベース
http://www.manypoints.org/
を以下のように更新できた．

下のテーブルは有限体 $\mathbb{F}_p$ 上で多数の有理点をもつ Wiman の 6 次曲線の記録である．

$\mathbb{F}_p$	(a,b)	$\#W(\mathbb{F}_p)$	old entry
17	$(1,8)$	54	– 60
29	$(6,19)$	78	– 90
37	$(35,9)$	86	80 – 104
41	$(35,33)$	102	90 – 114
47	$(18,30)$	120	90 – 126
59	$(21,48)$	132	120 – 150
61	$(38,13)$	134	110 – 152
73	$(34,12)$	170	140 – 174
79	$(57,50)$	176	170 – 182
89	$(79,57)$	186	150 – 198

下のテーブルは有限体 $\mathbb{F}_q$ 上で多数の有理点をもつ Wiman の 6 次曲線の記録である．

$\mathbb{F}_q$	$\#W(\mathbb{F}_q)$	old entry
7^2	110	– 134
11^2	254	230 – 254
7^3	512	500 – 564
11^3	1716	1680 – 1764
13^3	2714	2690 – 2756
11^5	165756	165720 – 165864
13^5	378506	– 378602
17^5	– 1434156	
19^5	– 2494982	

(2) Edge 曲線

1981 年に Edge が Wiman 曲線を研究して得た代数曲線である．

Edge の 6 次曲線は次のように定義される．

$$x^6+y^6+1+(x^2+y^2+1)(x^4+y^4+1) \\ -12x^2y^2+\alpha(y^2-1)(1-x^2)(x^2-y^2)=0.$$

① 素数 $p>3$ とし，k を標数が p の体とする．Edge の 6 次曲線は以下のように k 上でヤコビ多様体が分解する．

$$J_G \sim J_D \times J_{D'}^2,$$

ここで超楕円曲線は，

$D\colon y^2=f_\alpha(x)g_\alpha(x)$，$D'\colon y^2=f_{-\alpha}(x)g_{-\alpha}(x)$，

$$f_\alpha(x)=-6x^3+(9+\alpha)x^2-(\alpha+7)x+2,$$
$$g_\alpha(x)=2x^3+(1+\alpha)x^2+(1-\alpha)x+2$$

で定義される．

② Edge の 6 次曲線は $(p,\alpha)=(19,0)$, $(29,0)$, $(59,12)$, $(79,0)$, $(109,\beta^{715})$ $(139,12)$, $(149,33)$, $(179,42)$, $(199,0)$, $\cdots$ のとき有限体 $\mathbb{F}_{p^2}$ 上で最大曲線となる．

③ Edge の 6 次曲線は $(p,\alpha)=(67,0), (229,110)$, $(787,356)$, $(1021,230)$, $(1153,154)$, $(1229,67)$, $\cdots$ のとき有限体 $\mathbb{F}_{p^3}$ 上で Serre 上界に達する．

(3) ある種の 6 次曲線

Wiman の 6 次曲線と Edge の 6 次曲線を参考に以下のような代数曲線を定義した．

$$S: x^6+y^6+1 \\ +a(x^4y^2+x^2+y^4) \\ +b(x^2y^4+x^4+y^2) \\ +cx^2y^2=0.$$

① コンピュータ探索をした結果，有限体 $\mathbb{F}_{p^2}$ 上で最大曲線を得ることが出来た．下のテーブルにおいて，W は Wiman 曲線，E は Edge 曲線，S は曲線 S について有限体 $\mathbb{F}_{p^2}$ 上で最大曲線を得たことを意味する．

5	7	11	13	17	19	23	29
		W		W	W	W	W
31	37	41	43	47	53	59	61
W	S	W	S	W	S	W	
67	71	73	79	83	89	97	101
S	W		W	W	W	S	W
103	107	109	113	127	131	137	139
W	W	E	S	W	W	S	W
149	151	157	163	167	173	179	181
E	S		S	W	S	W	S
191	193	197	199				
W	W	S	W				

② 曲線 S をコンピュータ探索した結果，最大曲線でない最適曲線を得た．

種数 6 の代数曲線

$$x^6+y^6+1+(x^2y^4+x^4+y^2)-x^2y^2=0$$

は有限体 $\mathbb{F}_{5^7}$ 上で Serre 上界に達する.

③ 論文発表時において，データベース
`http://www.manypoints.org/`
を以下のように更新できた.

下のテーブルは有限体 $\mathbb{F}_p$ 上で多数の有理点をもつ曲線 S の記録である.

$\mathbb{F}_p$	(a,b,c)	$\#S(\mathbb{F}_p)$	old entry
19	$(13,6,16)$	56	$[50-68]$
37	$(29,28,14)$	98	$[86-104]$
43	$(2,4,2)$	104	$[100-116]$
53	$(51,36,1)$	132	$[120-138]$
61	$(42,54,17)$	140	$[134-152]$
67	$(65,2,45)$	152	$[140-164]$
71	$(29,65,70)$	156	$[150-168]$

下のテーブルは有限体 $\mathbb{F}_q$ 上で多数の有理点をもつ曲線 S の記録である.

$\mathbb{F}_q$	(a,b,c)	$\#S(\mathbb{F}_q)$	old entry
5^3	$(\beta^4,\beta^{56},\beta^{38})$ $u^3+3u+3=0$	240	$[210-255]$
7^3	$(\beta^{22},\beta^{94},\beta^8)$ $u^3-u^2+4=0$	542	$[512-564]$

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）

〔雑誌論文〕（計 2 件）

① 川北素子, Certain sextics with many rational points, Advances in Mathematics of Communications 11 (2017), no. 2, 289-292. 査読有

DOI:10.3934/amc.2017020

② 川北素子, Wiman's and Edge's sextic attaining Serre's bound II, Contemporary Mathematics 637 (2015), 191–203. 査読有

DOI:10.1090/conm/637/12758

〔学会発表〕（計 5 件）

① 川北素子, Certain sextics with many rational points, Workshop on Mathematics in Communications (WMC2016), スペイン・University of Cantabria, 2016 年 7 月.

② 川北素子, On certain sextics with many rational points, Workshop on Galois point and related topics, 神奈川大学, 2015 年 9 月.

③ 川北素子, Certain sextics with many rational points, Workshop on the Occasion of Harald Niederreiter's 70th Birthday: Applications of Algebra and Number Theory, オーストリア・Johann Radon Institute for Computational and Applied Mathematics, 2014 年 6 月.

④ 川北素子, Wiman's and Edge's sextic attaining Serre's bound, Workshop around Algebraic Combinatorics, 高知大学, 2014 年 1 月.

⑤ 川北素子, Wiman's and Edge's sextic attaining Serre's bound, Arithmetic, Geometry, Cryptography and Coding Theory, フランス・Centre International de Rencontres Mathmatiques, 2013 年 6 月.

〔その他〕
ホームページ等
`http://www.shiga-med.ac.jp/~kawakita/`

６．研究組織

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