WIMAN'S AND EDGE'S SEXTIC ATTAINING SERRE'S BOUND

MOTOKO QIU KAWAKITA

Abstract. We find new explicit algebraic curves of genus 6 over the finite field $\mathbb{F}_{67^3}$, $\mathbb{F}_{5393}$ and $\mathbb{F}_{9173}$ attaining Serre's bound. They are Wiman's and Edge's sextic. Also we obtain the condition of p for Wiman's sextic over the finite field $\mathbb{F}_{p^2}$ to be maximal, and give new entries of genus 6 for the tables manYPoints.org [5] by computing search on Edge's sextics.

1. Introduction

For the number of rational points of an algebraic curve C of genus g over a finite field $\mathbb{F}_q$, we have Hasse–Weil's bound

$$\#C(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q},$$

which is proved by Hasse for elliptic curves in 1933, and extended to all algebraic curves by Weil in 1941. The algebraic curve is said to be maximal if it attains this bound. Here p is a prime and q is its power.

In 1970's Goppa discovered algebro-geometric codes, where we can construct efficient codes from algebraic curves with many rational points. In 1983 Serre improved Hasse–Weil bound as

$$\#C(\mathbb{F}_q) \leq q + 1 + g\lfloor 2\sqrt{q}\rfloor,$$

which we call Serre's bound. Here $\lfloor\rfloor$ denotes the round down. An algebraic curve attains this bound has a very simple L-function as $(1 + \lfloor 2\sqrt{q}\rfloor t + qt^2)^g$; see [7].

We know many properties for maximal curves; see [3], [4] and their references. However we do not know about the property of non-maximal curves attaining Serre's bound when its genera ≥ 4. Since we only know some examples over prime fields of genus 4 in [8], and one example over the finite field 2^{11} of genus 11 in [9].

2. Wiman's sextic

In 1895 Wiman introduced the sextic

$$W: \; x^6 + y^6 + 1 + (x^2 + y^2 + 1)(x^4 + y^4 + 1) - 12x^2y^2 = 0$$

2000 *Mathematics Subject Classification.* Primary 11G20, 14G05; Secondary 14G50.

Key words and phrases. Algebro-geometric codes; sextics; rational points.

in [12], where we call it Wiman's sextic and you can see its beautiful geometrical properties in [2] and [6]. We find the following example by computing search.

Example 1. Wiman's sextic W attains Serre's bound over the finite field $\mathbb{F}_{67^3}$ and $\mathbb{F}_{5393}$.

We also have the next proposition.

Proposition 2. Wiman's sextic over the finite field $\mathbb{F}_{p^2}$ is maximal if and only if

$$\sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m!}{(i!)^2(m-2i)!} \cdot 2^{9i} \cdot 5^{m-i} \cdot (-19)^{m-2i} \equiv 0 \mod p,$$

where $m := \frac{p-1}{2}$.

Proof. We can prove it from the following lemma. □

Lemma 3. Wiman's sextic W over $\mathbb{F}_p$ is supersingular if and only if p satisfies the condition in the above proposition.

Proof. Let $p \neq 2, 3, 5$. We have the Jacobian of W decomposes completely as

$$J_W \sim \epsilon^6$$

where the elliptic curve is defined by

$$\epsilon : \ y^2 = x(5x^2 - 95x + 2^9).$$

From Theorem 4.1. in [11], we have that this elliptic curve over $\mathbb{F}_p$ is supersingular if and only if the coefficient of x^{p-1} in $(x(5x^2 - 95x + 2^9))^{(p-1)/2}$ is zero. Here by compute the coefficient of $x^{\frac{p-1}{2}}$ in $(5x^2 - 95x + 2^9)^{(p-1)/2}$, we can prove it. □

We note that $19, 29, 79, 199, 269, 359, 439, 499, 509, 599, 919, 1279, \cdots$ are such primes.

3. Edge's sextics

From Wiman's sextic, in 1981 W. L. Edge found a family of sextics in [2], which is defined by the equation

$$E_\alpha : \ T + \alpha S = 0$$

where

$$\begin{aligned} T &:= x^6 + y^6 + 1 + (x^2 + y^2 + 1)(x^4 + y^4 + 1) - 12x^2y^2, \\ S &:= (y^2 - 1)(1 - x^2)(x^2 - y^2). \end{aligned}$$

We call it Edge's sextic; see also [1] for its geometrical properties.

We obtain the next example by computing search.

Example 4. Edge's sextic E_{1403} attains Serre's bound over the finite field $\mathbb{F}_{9173}$.

We also obtain Edge's sextic with many rational points which give new entries for the tables manYPoints.org in [5] for the case of genus 6. We list them in the following tables.

TABLE 1

$\mathbb{F}_p$	α	new entry	old entry
13	0	$[50-52]$	$[50-52]$
19	2	$[50-68]$	-68
23	10	$[60-78]$	-78
31	0	$[80-96]$	-96
37	8	$[80-108]$	-108
41	8	$[90-114]$	-114
47	10	$[90-126]$	-126
53	21	$[120-138]$	-138
59	16	$[120-150]$	-150
61	6	$[110-152]$	-152
67	9	$[140-164]$	-164
71	49	$[150-168]$	-168
73	5	$[140-174]$	-174
79	3	$[170-182]$	-182
83	14	$[180-190]$	-190
89	0	$[150-198]$	-198
97	7	$[200-212]$	-212

The first line of Table 1 means that Edge's sextic E_0 over the finite field $\mathbb{F}_{13}$ have 50 rational points, where the old entry does not give an equation of the algebraic curve. The third line of Table 2 means that Edge's sextic $E_{\beta^{37}}$ over the finite field $\mathbb{F}_{5^5}$ have 3750 rational points, where $\beta \in \mathbb{F}_{5^5}$ satisfies $\beta^5 + 4\beta + 3 = 0$.

Acknowledgements. The author would like to express her appreciation to Shinji Miura for discussion, and the authors of KASH/KANT. This work was supported by JST PRESTO program.

REFERENCES

[1] G. Cornelissen, F. Kato, Mumford curves with maximal automorphism group II, Lamé type groups in genus 5–8, Geom. Dedicata **102**(2003), 127–142.

[2] W. L. Edge, A pencil of four-nodal plane sextics, Math. Proc. Cambridge Philos. Soc. **89**(3)(1981), 413–421.

[3] A. Garcia, H. Stichtenoth, C. P. Xing, On subfields of the Hermitian function field, Comp. Math. **120**(2000), 137–170.

[4] A. Garcia, G, Guneri, H. Stichtenoth, A generalization of the Giulietti-Korchmaros maximal curve, Adv. Geom. **10**(3) (2010), 427–434.

[5] G. van der Geer, E. Howe, K. Lauter, C. Ritzenthaler, Table of curves with many points. URL http://www.manypoints.org

[6] N. Inoue, F. Kato, On the geometry of Wiman ' s sextic, J. Math. Kyoto Univ. **45**(4)(2005), 743–757.

TABLE 2

$\mathbb{F}_q$	α		new entry	old entry
5^2	1		$[80-82]$	-82
5^3	1		$[210-255]$	-255
5^5	β^{37}	$\beta^5+4\beta+3=0$	$[3750-3792]$	-3792
7^3	β^{29}	$\beta^3+6\beta^2+4=0$	$[500-564]$	-564
7^5	0		$[18260-18360]$	-18360
11^2	0		$[230-254]$	-254
11^3	0		$[1680-1764]$	$[1668-1764]$
11^4	β^{732}	$\beta^4+8\beta^2+10\beta+2=0$	$[16070-16094]$	$[15350-16094]$
11^5	β^{8087}	$\beta^5+10\beta^2+9=0$	$[165720-165864]$	-165864
13^3	β^{159}	$\beta^3+2\beta+11=0$	$[2690-2756]$	-2756
17^3	β^{268}	$\beta^3+\beta+14=0$	$[5700-5752]$	-5752
19^3	β^{2315}	$\beta^3+4\beta+17=0$	$[7820-7850]$	-7850
19^4	β^{25702}	$\beta^4+2\beta^2+11\beta+2=0$	$[134630-134654]$	-134654

[7] K. Lachaud, Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis, C. R. Acad. Sci. Paris, Sér. I Math. **305**(16)(1987), 729–732.

[8] M. Q. Kawakita, On quotient curves of the Fermat curve of degree twelve attaining the Serre bound, Internat. J. Math. **20**(5) (2009), 529–539.

[9] S. Miura, Algebraic geometric codes on certain plane curves (in Japanese), IEICE Trans. Fundamental **J75-A**(11)(1992), 1735–1745.

[10] J. -P. Serre, Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, C. R. Acad. Sci. Paris Sér. I Math. **296**(9)(1983), 397–402.

[11] J. H. Silverman, The arithmetic of elliptic curves, 2nd Edition, Graduate Texts in Mathematics**106**(2009).

[12] A. Wiman, Zur Theorie der endlichen Gruppen von birationalen Transformationen in der Ebene, Math. Ann. **48**(1897), 195–240.

DEPARTMENT OF MATHEMATICS, SHIGA UNIVERSITY OF MEDICAL SCIENCE, SETA TSUKINOWA-CHO, OTSU, SHIGA, 520-2192 JAPAN

E-mail address: `kawakita@belle.shiga-med.ac.jp`