Advances in Mathematics of Communications
Volume X, No. 0X, 20xx, X–XX
doi:10.3934/amc.xx.xx.xx

CERTAIN SEXTICS WITH MANY RATIONAL POINTS

Motoko Qiu Kawakita

Department of Mathematics, Shiga University of Medical Science,
Seta Tsukinowa-cho, Otsu, Shiga, 520-2192 Japan

Abstract. We construct a family of sextics from the Wiman and Edge sextics. We find a curve over $\mathbb{F}_{5^7}$ attaining the Serre bound, and update 9 entries of genus 6 in manYPoints.org by computer search on these sextics.

1. Introduction

Goppa discovered algebro-geometric codes in 1970s, where we can construct efficient codes from explicit curves with many rational points; see [10]. For a curve C of genus g over a finite field $\mathbb{F}_q$, we have the Hasse–Weil bound $\#C(\mathbb{F}_q) \leq q+1+2g\sqrt{q}$. A curve attaining this bound is said to be maximal. Here p is a prime number and q is a power of p. By a curve we mean a projective geometrically irreducible nonsingular curve. In 1983, Serre improved this bound as $\#C(\mathbb{F}_q) \leq q+1+g\lfloor 2\sqrt{q}\rfloor$, which we call the Serre bound. Here $\lfloor\ \rfloor$ means round down.

There are many interesting researches in maximal curves; see [3], [5] and their references. However there are only a few examples of curves which attain the Serre bound but are not maximal. In [7], [8], we find such curves from families of Wiman and Edge sextics. A family of the Wiman sextics W in [11] is defined by

$$x^6+y^6+1+a(x^4y^2+x^2y^4+x^4+x^2+y^4+y^2)+bx^2y^2=0;$$

the Edge sextics E in [2] is defined by

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

It is natural to try to generalise these two families of sextics. The purpose of this paper is to find curves with many rational points among them.

2. Generalising defining equations

Define a sextic S with the following equation:

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

Immediately we can check that if $a=b$ then S are the Wiman sextics, and if $a=(1-\alpha)/2$, $b=(1+\alpha)/2$, $c=-6$ then S are the Edge sextics.

Afterward we set $c=-3(a+b+1)$ in this section. Set $\mathrm{Jac}(C)$ be the Jacobian variety of a curve C, and k be a field of characteristic $p\geq 5$.

2010 *Mathematics Subject Classification:* Primary: 11G20, 14G05; Secondary: 14G50.
Key words and phrases: Algebro-geometric codes, Rational points, Serre bound.
This research was partially supported by JSPS Grant-in-Aid for Young Scientists (B) 25800090.

Proposition 1. *The Jacobian variety of S decomposes over k as*

$$\mathrm{Jac}(S) \sim \mathrm{Jac}(D) \times \mathrm{Jac}(D')^2,$$

where $D\colon y^2 = f_{a,b}(x)$ and $D'\colon y^2 = f_{b,a}(x)$ with

$$f_{a,b}(x) = -(x^3 + bx^2 + ax + 1)((a+b+2)x^3 - (a+2b+3)x^2 + (b+3)x - 1).$$

The basic idea of the proof is the same as Proposition 10 in [8].

Proof. We have $\rho\colon (x,y) \mapsto (x,-y)$ and $\iota\colon (x,y) \mapsto (-x,y)$ in the automorphism group of the sextic S. By Theorem B of [6], the following isogeny relation is satisfied:

$$\mathrm{Jac}(S) \times \mathrm{Jac}(S/\langle \iota, \rho\rangle)^2 \sim \mathrm{Jac}(S/\langle\iota\rangle) \times \mathrm{Jac}(S/\langle\rho\rangle) \times \mathrm{Jac}(S/\langle\iota\rho\rangle),$$

where $S/\langle\rho\rangle$ is birational equivalent to D, $S/\langle\iota\rangle$ and $S/\langle\iota\rho\rangle$ are birational equivalent to D'. Since $c = -3(a+b+1)$, the genus of $S/\langle\iota,\rho\rangle$ is 0, which completes the proof. □

Corollary 2. $\#S(\mathbb{F}_q) = 3\#D(\mathbb{F}_q) - 2q - 2$.

Proof. Since $\#D(\mathbb{F}_q) = \#D'(\mathbb{F}_q)$, it follows from the trace of Frobenius action on a Tate module of Jacobians. □

Note that if $a+b+2$, $-4a^3+a^2b^2+18ab-4b^3-27$, the resultant of x^3+bx^2+ax+1 and $(a+b+2)x^3-(a+2b+3)x^2+(b+3)x-1$ are not 0 then the genus of D is 2. Now we search by the computer algebra package Magma [1] among them. We find maximal curves D over $\mathbb{F}_{p^2}$, which give us maximal sextics S of genus 6 over $\mathbb{F}_{p^2}$ simultaneously.

Example 3. The sextic S is maximal over $\mathbb{F}_{p^2}$ when (p,a,b) is $(37,9,13)$, $(43,2,5)$, $(53,13,46)$, $(67,27,48)$, $(97,80,86)$, $(113,50,91)$, $(137,60,130)$, $(151,12,149)$, $(163,15,155)$, $(173,5,111)$, $(181,3,49)$, $(197,68,102)$, $\cdots$.

In Table 1 we list prime numbers $p < 200$. If there is a maximal Wiman or Edge sextic over $\mathbb{F}_{p^2}$ in [8], then we write W or E under p respectively. If there is a maximal sextic over $\mathbb{F}_{p^2}$ in Example 3, we write S under p.

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				

TABLE 1. Maximal curves over $\mathbb{F}_{p^2}$ of genus 6

Next, for $a, b \in \mathbb{F}_p$ and $i \geq 3$, we can compute the number of rational points of $\#D(\mathbb{F}_{p^i})$ from $\#D(\mathbb{F}_p)$ and $\#D(\mathbb{F}_{p^2})$ by the theory of Zeta function. We list the

algorithm here, where we set $n_i = \#D(\mathbb{F}_{p^i})$.

Input n_1, n_2
  $a_1 \leftarrow n_1 - p - 1$
  $a_2 \leftarrow (n_2 - p^2 - 1 + a_1^2)/2$
  $\omega_1, \cdots, \omega_4 \leftarrow$ roots of $x^4 + a_1x^3 + a_2x^2 + pa_1x + p^2 = 0$
  $n_i \leftarrow p^i + 1 - \sum_{j=1}^{4} {\omega_j}^i$
Output n_i

We implement it by Magma, and find a curve attaining the Serre bound.

Example 4. The sextic

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

of genus 6 over $\mathbb{F}_{5^7}$ attains the Serre bound.

We note the assertion of Lauter from Theorem 1 in [9].

Theorem 5 ([9])**.** *The Serre bound cannot be met when $q = 5^7$ and $g \geq 7$.*

We note that the Jacobian of H decomposes over $\mathbb{F}_{5^7}$ as $\mathrm{Jac}(H) \sim E_1^3 \times E_2^3$, where $E_1\colon y^2 = x^3 + 3x + 2$ and $E_2\colon y^2 = x^3 + x^2 + 2$.

3. Updating Table of curves with many points

We also find new curves with many rational points of genus 6 by computer search on S using Magma, which we list in Table 2, 3. For example, S over $\mathbb{F}_{5^3}$ has 240 rational points when $a = \beta^4$, $b = \beta^{56}$ and $c = \beta^{38}$ where β is a root of $u^3+3u+3 = 0$ in $\mathbb{F}_{5^3}$. Here the best known lower bound is 210 and the upper bound is 255 in [4].

$\mathbb{F}_p$	(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	$[150 - 168]$

TABLE 2. S with many points over $\mathbb{F}_p$

$\mathbb{F}_q$	(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	$[512 - 564]$

TABLE 3. S with many points over $\mathbb{F}_q$

ACKNOWLEDGMENTS

The author wishes to express her thanks to Henning Stichtenoth and Gary McGuire for their valuable comments on her talk at Workshop on the occasion of Harald Niederreiter's 70th birthday.

REFERENCES

[1] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. **24**(1997), 235–265.

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

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

[4] G. van der Geer, E. W. Howe, K. E. Lauter, C. Ritzenthaler, Table of curves with many points, `http://www.manypoints.org`, Retrieved 23rd January 2016.

[5] M. Giulietti, M. Montanucci, G. Zini, On maximal curves that are not quotients of the Hermitian curve, preprint 2015, `arXiv:1511.05353`.

[6] E. Kani, M. Rosen, Idempotent relations and factors of Jacobians, Math. Ann. **284**(2)(1989), 307–327.

[7] M. Q. Kawakita, Wiman's and Edge's sextic attaining Serre's bound, preprint 2011. Available from: `http://www.manypoints.org/upload/kawakita.pdf`.

[8] M. Q. Kawakita, Wiman's and Edge's sextic attaining Serre's bound II, Algorithmic arithmetic, geometry, and coding theory, Contemp. Math. **637**(2015), 191–203.

[9] K. E. Lauter, Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields, J. Algebraic Geom. **10**(1)(2001), 19–36.

[10] C. Moreno, Algebraic curves over finite fields, Cambridge Tracts in Mathematics **97**, Cambridge University Press, 1991.

[11] A. Wiman, Ueber eine einfache Gruppe von 360 ebenen Collineationen, Math. Ann. **47**(4)(1896), 531–556.