Some sextics of genera five and seven attaining the Serre bound *

Motoko Qiu Kawakita

Department of Mathematics, Shiga University of Medical Science, Seta Tsukinowa-cho, Otsu, Shiga, 520-2192 Japan
kawakita@belle.shiga-med.ac.jp

Abstract. We define two families of sextics. By computer search on one family, we find new curves of genus 5 attaining the Hasse–Weil–Serre bound over $\mathbb{F}_{71}$, $\mathbb{F}_{191}$ and $\mathbb{F}_{11^5}$, and we update 3 entries of genus 5 in manYPoints.org. Among another family, we find new curves of genus 7 attaining the Hasse–Weil–Serre bound over $\mathbb{F}_{p^3}$ for some primes p. We determine the precise condition on the finite field over which the sextics attain the Hasse–Weil–Serre bound.

Keywords: Algebro-geometric codes · Rational points · Serre bound.

1 Introduction

Goppa discovered algebro-geometric codes in 1970s, where we can construct efficient codes from explicit curves with many rational points; see [11]. For a curve C of genus $g(C)$ over a finite field $\mathbb{F}_q$, we have the Hasse–Weil bound $\#C(\mathbb{F}_q) \leq q+1+2g(C)\sqrt{q}$. A curve attaining this bound is said to be maximal. Here p is a prime number and q is a power of p, $\#C(\mathbb{F}_q)$ is the number of rational points of C over $\mathbb{F}_q$. By a curve we mean a projective geometrically irreducible nonsingular curve. In 1983, Serre improved this bound as $\#C(\mathbb{F}_q) \leq q+1+g(C)\lfloor 2\sqrt{q}\rfloor$, which we call the Serre bound. Here $\lfloor\cdot\rfloor$ means round down.

Many properties of maximal curves have been widely investigated; see [2], [4] and references therein. However, this is not the case of non-maximal curves attaining the Serre bound with its genera ≥ 4. There are known only examples of genera 4 and 10 in [6], genus 6 in [7–9], genus 11 in [10].

The purpose of this research is to find more explicit examples. In the process of studying the sextics in [7, 8], we get an idea to define two families of sextics in Section 2 and 4. Among them by computer search, we find new non-maximal curves of genera 5 and 7 attaining the Serre bound in Section 3 and 5 respectively.

2 A family of sextics of genus ≤ 5

Let k be a field of characteristic $p \neq 2, 3, 5$ in this section, and $\bar{k}$ be its algebraic closure.

* Partially supported by JSPS Grant-in-Aid for Scientific Research (C) 17K05344.

Definition 1. *We set a sextic C over a field k with the following equation:*

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

where $a, b, c \in k$ and $c \neq 0$.

Let J_C be the Jacobian variety of a curve C. Theorem B of [5] plays an important role when we decompose a Jacobian variety of a curve in this article.

Theorem 1. (Theorem B, [5]) *Given a curve X, let $G \leq \mathrm{Aut}(X)$ be a finite group such that $G = H_1 \cup \cdots \cup H_m$ where the subgroups H_i satisfy $H_i \cap H_j = 1_G$ if $i \neq j$. Then we have the following isogeny relation*

$$J_X^{m-1} \times J_{X/G}^{g} \sim J_{X/H_1}^{h_1} \times \cdots \times J_{X/H_m}^{h_m}$$

where $g = |G|$ and $h_i = |H_i|$ and J_r means the product of J with itself r times.

Proposition 1. *Assume that there exists $\zeta \in k$, such that $\zeta^5 = 1$. The Jacobian variety of C decomposes over k have the following isogeny relation*

$$J_C \sim J_{C_\sigma}^2 \times J_{C_\tau},$$

where $C_\sigma : f(x, y) = 0$ and $C_\tau : y^2 = h(x)$ with

$$f(x, y) = x^5 - 5x^3y + 5xy^2 + y^3 + ay^2 + by + c,$$
$$h(x) = (x^3 + ax^2 + bx + c)^2 - 4x^5.$$

Proof. For $\sigma : (x, y) \mapsto (y, x)$, we have the quotient as

$$C/\langle\sigma\rangle : x^5 - 5x^3y + 5xy^2 + y^3 + ay^2 + by + c = 0.$$

For $\tau : (x, y) \mapsto (\zeta x, \zeta^{-1}y)$, we have

$$C/\langle\tau\rangle : x^2 + (y^3 + ay^2 + by + c)x + y^5 = 0,$$

which is birational equivalent to $y^2 = (x^3 + ax^2 + bx + c)^2 - 4x^5$.

Set $G = \langle\sigma, \tau\rangle$. We have $G = \langle\sigma\rangle \cup \langle\tau\rangle \cup \langle\sigma\tau\rangle \cup \langle\sigma\tau^2\rangle \cup \langle\sigma\tau^3\rangle \cup \langle\sigma\tau^4\rangle$. From Theorem 1,

$$J_C^5 \times J_{C/G}^{10} \sim J_{C/\langle\sigma\rangle}^2 \times J_{C/\langle\tau\rangle}^5 \times J_{C/\langle\sigma\tau\rangle}^2 \times J_{C/\langle\sigma\tau^2\rangle}^2 \times J_{C/\langle\sigma\tau^3\rangle}^2 \times J_{C/\langle\sigma\tau^4\rangle}^2.$$

The genus of C/G is 0. Further $C/\langle\sigma\tau^i\rangle$ for $i = 1, 2, 3, 4$ are birational equivalent to $C/\langle\sigma\rangle$, therefore $J_C \sim J_{C/\langle\sigma\rangle}^2 \times J_{C/\langle\tau\rangle}$. Setting $C/\langle\sigma\rangle$ and $C/\langle\tau\rangle$ as C_σ and C_τ respectively, which completes the proof.

Corollary 1. *Let $q = 1 (\bmod 5)$. We have that*

$$\#C(\mathbb{F}_q) = 2\#C_\sigma(\mathbb{F}_q) + \#C_\tau(\mathbb{F}_q) - 2q - 2.$$

Proof. It is well known that $\#C(\mathbb{F}_q) = q+1-t$, where t is the trace of Frobenius acting on a Tate module of J_C. Proposition 1 implies that this Tate module is isomorphic to a direct sum of two copies of the Tate module of J_{C_σ} and C_τ. Hence $t = 2t_1 + t_2$, where t_1 and t_2 are the trace of Frobenius on the Tate module of J_{C_σ} and C_τ respectively. Since $t_1 = q+1-\#C_\sigma(\mathbb{F}_q)$ and $t_2 = q+1-\#C_\tau(\mathbb{F}_q)$, the result follows.

For polynomials $u(x)$ and $v(x)$, we set the resultant $\mathrm{Res}(u, v)$ as the determinant of the Sylvester matrix.

Lemma 1. *Let α, β be roots of $1 - 3x + x^2 = 0$ in $\bar{k}$, $f_y(x, y)$ be the partial derivative of f with respect to y. Set $u_\alpha(x) = f(x, \alpha x^2)$, $v_\alpha(x) = f_y(x, \alpha x^2)$. If $\mathrm{Res}(u_\alpha, v_\alpha) = \mathrm{Res}(u_\beta, v_\beta) = 0$, then the genus $g(C_\sigma) \leq 2$.*

Proof. The infinity of C_σ is a singular point, hence the genus $g(C_\sigma) \leq 4$. If $\mathrm{Res}(u_\alpha, v_\alpha) = 0$, then there exists $s \in \bar{k}$, such that $u_\alpha(s) = v_\alpha(s) = 0$. It means that $f(s, \alpha s^2) = f_y(s, \alpha s^2) = 0$. The partial derivative of f with respect to x is $f_x(x, y) = 5(x^4 - 3x^2y + y^2)$. Thus $f_x(s, \alpha s^2) = 0$, which means that $(s, \alpha s^2)$ is a singular point on the affine piece. Similarly, if $\mathrm{Res}(u_\beta, v_\beta) = 0$ then there exists another singular point $(t, \beta t^2)$ on the affine piece. Therefore the genus $g(C_\sigma) \leq 2$.

Lemma 2. *Set $h'(x)$ as the differentiation of $h(x)$. If $\mathrm{Res}(h, h') = 0$, then the genus $g(C_\tau) \leq 1$.*

Proof. If $\mathrm{Res}(h, h') = 0$, then there exists $s \in \bar{k}$ such that $h(x) = (x-s)^2 h_1(x)$ where $\deg h_1 = 4$. Hence C_τ is birational to $y^2 = h_1(x)$, which means $g(C_\tau) \leq 1$.

Proposition 2. *If $\mathrm{Res}(u_\alpha, v_\alpha) = \mathrm{Res}(u_\beta, v_\beta) = \mathrm{Res}(h, h') = 0$, then the genus $g(C) \leq 5$.*

Proof. From Proposition 1, we have that $g(C) = 2g(C_\sigma) + g(C_\tau)$. Lemma 1 and 2 imply the result immediately.

We remark that the condition of Proposition 2 is simple to implement in computer search.

3 Curves of genus 5 attaining the Serre bound

We search by MAGMA [1] among C over $\mathbb{F}_q$ for $q \equiv 1 (\bmod 5)$, under the condition of Proposition 2, using Corollary 1. New curves of genus 5 are found, which update three entries in [3], whom we list in Table 1. In [3] the tables record for a pair (q, g) an entry $\alpha - \beta$ where β is the best upper bound for the maximum number of points of a curve of genus g over $\mathbb{F}_q$ and α gives a lower bound obtained from an explicit example of a curve defined over $\mathbb{F}_q$ with α (or at least α) rational points.

Example 1. $x^3y^3 + x^5 + y^5 + 2x^2y^2 + 4xy + 25 = 0$ has 82 rational points over $\mathbb{F}_{31}$.

Table 1. Curves of genus 5 with many points

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

Example 2. The sextic C attains the Serre bound over $\mathbb{F}_q$, when $(q, a, b, c) = (71, 4, 46, 36)$, $(191, 134, 126, 2)$, $(11^5, 10, 9, 10)$.

Simultaneously, we find maximal curves of genus 5.

Example 3. The sextic C is maximal over $\mathbb{F}_{p^2}$, when $(p, a, b, c) =$ $(29, 17, 28, 28)$, $(31, 1, 3, 7)$, $(41, 28, 29, 31)$, $(59, 9, 16, 28)$, $(61, 11, 9, 10)$, $(71, 0, 62, 64)$, $(79, 5, 10, 12)$, $(89, 8, 20, 8)$, $(101, 46, 89, 38)$, $(109, 4, 87, 7)$, $(131, 0, 107, 97)$, $(139, 2, 43, 122)$, $(149, 5, 43, 59)$, $(151, 5, 41, 115)$, $(179, 7, 152, 90)$, $(181, 67, 41, 18)$, $(191, 2, 9, 17)$, $(199, 17, 196, 24)$, etc.

We list them in Table 2. We note that we practice for $p \leq 269$ in this case.

Table 2. Maximal curves of genus 5 over $\mathbb{F}_{p^2}$

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

From Table 2, we have a conjecture.

Conjecture 1. Let $p > 23$. If $p \equiv \pm 1 (\bmod 5)$, then there exists a sextic C of genus 5, which is maximal over $\mathbb{F}_{p^2}$.

4 A family of sextics of genus 7

Let k be a field of characteristic $p \neq 2, 3$ in this section.

Definition 2. *We set a sextic W over k with the following equation:*

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

where $b \in k$.

We decompose the Jacobian variety, where the idea comes from Proposition 10 in [7].

Proposition 3. *The sextic W over a field k have the following isogeny relation:*

$$J_W \times H_2^2 \sim J_H^3,$$

where the curves are defined by

$$\begin{aligned} H_2 &: x^2y + y^2 + x + xy^2 + y + x^2 + bxy = 0, \\ H &: x^2y^2 + y^4 + x + xy^4 + y^2 + x^2 + bxy^2 = 0. \end{aligned}$$

Proof. Since $\sigma : (x, y) \mapsto (-x, y)$, $\tau : (x, y) \mapsto (x, -y)$ are automorphisms of W, from Theorem 1, we have that

$$J_W \times J^2_{W/\langle\sigma,\tau\rangle} \sim J_{W/\langle\sigma\tau\rangle} \times J_{W/\langle\sigma\rangle} \times J_{W/\langle\tau\rangle}.$$

$W/\langle\sigma, \tau\rangle$ is birational equivalent to H_2. Further, $W/\langle\sigma\tau\rangle$, $W/\langle\sigma\rangle$ and $W/\langle\tau\rangle$ are birational equivalent to H, which show the isogeny relation.

Afterward, set $b \neq 2, 3, -6$.

Proposition 4. *The jacobian variety of the curve H over a field k have the following isogeny relation:*

$$J_H \sim E_1 \times E_2 \times E_3,$$

where the elliptic curves $E_i : y^2 = xf_i(x)$ for $i = 1, 2, 3$ are given by

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

Proof. Since $\sigma : (x, y) \mapsto (x/y^2, 1/y)$, $\tau : (x, y) \mapsto (x, -y)$ are automorphisms of H, from Theorem 1, we have

$$J_H \times J^2_{H/\langle\sigma,\tau\rangle} \sim J_{H/\langle\sigma\tau\rangle} \times J_{H/\langle\sigma\rangle} \times J_{H/\langle\tau\rangle}.$$

Now, an explicit quotient map $H \to H/\langle\sigma\tau\rangle$ is given by

$$(x, y) \mapsto (x + x/y^2, y - 1/y),$$

where one gets

$$H/\langle\sigma\tau\rangle : x^2 + xy^2 + bx + 2x + y^2 + 4 = 0,$$

which is birational equivalent to E_1.

Next, an explicit quotient map $H \to H/\langle\sigma\rangle$ is given by

$$(x, y) \mapsto (x/y, y + 1/y),$$

where we have

$$H/\langle\sigma\rangle : -(x^3 + y^3 - 3y) + (x + y)(x^2 + y^2 - 2) + bx = 0,$$

which is birational equivalent to E_2.

$H/\langle\tau\rangle$ is birational equivalent E_3, and the genus of $H/\langle\sigma, \tau\rangle$ is 0, which give the desired result.

Theorem 2. *The sextic W over a field k have the following isogeny relation*

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

And the genus $g(W) = 7$.

Proof. H_2 is birational equivalent to E_3, hence Proposition 3 and 4 show the result. Moreover, E_1, E_2 and E_3 are nonsingular when $b \neq 2, 3, -6$.

Corollary 2. *We have that*

$$\#W(\mathbb{F}_q) = 3\#E_1(\mathbb{F}_q) + 3\#E_2(\mathbb{F}_q) + \#E_3(\mathbb{F}_q) - 6q - 6.$$

Proof. It is well known that $\#W(\mathbb{F}_q) = q+1-t$, where t is the trace of Frobenius acting on a Tate module of J_W. Theorem 2 implies that this Tate module is isomorphic to a direct sum of three copies of the Tate module of E_1, E_2 and E_3. Hence $t = 3t_1 + 3t_2 + t_3$, where t_1, t_2 and t_3 are the trace of Frobenius on the Tate module of E_1, E_2 and E_3 respectively. Since $t_i = q + 1 - \#E_i(\mathbb{F}_q)$ for $i = 1, 2, 3$, the result follows.

Note that the j-invariants of E_1, E_2, E_3 are respectively

$$\frac{2^8(b^2 + 3b - 9)^3}{(b-2)(b-3)^2(b+6)}, \quad \frac{2^8(b^2 - 5b + 7)}{(b-2)^2(b-3)^2}, \quad \frac{b^3(b^3 - 24b + 48)^3}{(b-2)^3(b-3)^2(b+6)}.$$

5 Curves of genus 7 attaining the Serre bound

We search by MAGMA [1] among W over $\mathbb{F}_q$, using Corollary 2. For an elliptic curve E, we implement the next algorithm to compute n_i with $i \geq 2$ from n_1, where $n_i = \#E(\mathbb{F}_{p^i})$. It is based on the theory of Zeta function.

Algorithm.

INPUT: n_1, i.
OUTPUT: $n_2, n_3, \cdots, n_i$.
1. $a_1 \leftarrow p+1-n_1$.
2. $a_2 \leftarrow a_1^2-2p$.
3. $n_2 \leftarrow p^2+1-a_2$.
4. for $j=3$ to i do:
   $a_j \leftarrow a_1 a_{j-1} - p a_{j-2}$
   $n_j \leftarrow p^j+1-a_j$.
5. Return $n_2, n_3, \cdots, n_i$.

We find curves of genus 7 attaining the Serre bound.

Example 4. The sextic W is maximal over $\mathbb{F}_{p^2}$, when $(p,b)=(23,13), (47,26), (71,1), (167,137), (191,45), (239,27), (263,87), (383,358), (431,267), (479,309)$, etc.

We note that we practice for $p \leq 99991$ in this case.

Afterward we consider the finite field $\mathbb{F}_p$ as $\mathbb{Z}/(p)$, which is the residue classes of the integers modulo the ideal generated by a prime p. Set $m=(p-1)/2$. Denote the coefficients of x^m in $f_i(x)^m$ by $\overline{A}_i$ for $i=1,2,3$, which means that

$$\overline{A}_1 = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m!}{(i!)^2(m-2i)!}(-1)^{m-i} b^{m-2i}(b-3)^i,$$

$$\overline{A}_2 = H_p(b-2) = \sum_{i=0}^{m} \binom{m}{i}^2 (b-2)^i,$$

$$\overline{A}_3 = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m!}{(i!)^2(m-2i)!}(-16)^i (b^2-12)^{m-2i}(b-3)^i.$$

Theorem 3. *Let $b \in \mathbb{F}_p$. W is maximal over $\mathbb{F}_{p^2}$ if and only if*

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

Proof. It follows from Section V.4 of [12] and Theorem 2.

Example 5. The sextic W attaining the Serre bound over $\mathbb{F}_{p^3}$, when $(p,b) = (21313, 3663), (30269, 10886), (61519, 56766), (76163, 6230)$, etc.

We note that we practice for $p \leq 131363$ in this case.

For $\overline{A} \in \mathbb{F}_p$, set A as the integer such that $\overline{A} \equiv A (\bmod p)$ and $0 \leq A < p$.

Theorem 4. *Let $p \geq 11$ and $b \in \mathbb{F}_p$. W over $\mathbb{F}_{p^3}$ attains the Serre bound if and only if*

$$A_1^3 - 3pA_1 = A_2^3 - 3pA_2 = A_3^3 - 3pA_3 = -\lfloor 2p\sqrt{p} \rfloor.$$

Proof. It follows from Theorem 4 in [7] and Theorem 2.

Acknowledgements

The author wishes to express her thanks to Massimo Giulietti, Gary McGuire, Maria Montanucci and Carlos Moreno for their valuable comments on this research.

References

1. Bosma, W., Cannon, J., Playoust C.: The Magma algebra system. I. The user language, J. Symbolic Comput. **24**, 235–265 (1997)
2. Garcia, A., Güneri, G., Stichtenoth, H.: A generalization of the Giulietti–Korchmáros maximal curve, Adv. Geom. **10**(3), 427–434 (2010)
3. van der Geer, G., Howe, E., Lauter, K., Ritzenthaler, C.: Table of curves with many points, http://www.manypoints.org
4. Giulietti, M., Montanucci, M., Zini, G.: On maximal curves that are not quotients of the Hermitian curve, Finite Fields Appl. **41**, 72-88 (2016)
5. Kani, E., Rosen, M.: Idempotent relations and factors of Jacobians, Math. Ann. **284**(2), 307–327 (1989)
6. Kawakita, M.Q.: On quotient curves of the Fermat curve of degree twelve attaining the Serre bound, Int. J. Math. **20**(5), 529-539 (2005)
7. Kawakita, M.Q.: Wiman's and Edge's sextic attaining Serre's bound II, Algorithmic arithmetic, geometry, and coding theory, Contemp. Math. **637** 191–203 (2015)
8. Kawakita, M.Q.: Certain sextics with many rational points, Adv. Math. Commun. **11**(2), 289-292 (2017)
9. Kawakita, M.Q.: Wiman's and Edge's sextic attaining Serre's bound, Euro. J. Math. **4**(1), 330–334 (2018)
10. Miura, S.: Algebraic geometric codes on certain plane curves (in Japanese), IEICE Trans. Fundam. **J75-A**(11), 17351745 (1992)
11. Moreno, C.: Algebraic curves over finite fields, Cambridge Tracts in Mathematics **97**, Cambridge University Press, Cambridege (1991)
12. Silverman, J.H: The arithmetic of elliptic curves, 2nd Edition, Graduate Texts in Mathematics**106**, Springer, Heidelberg (2009)