Wiman's and Edge's sextic attaining Serre's bound II

Motoko Qiu Kawakita

Abstract. In 1970's Goppa discovered algebro-geometric codes, where we need explicit curves with many rational points to construct good codes. 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 of order p, p^2 or p^3, for a prime number p. For some sextics among them, we determined the precise condition on the finite field over which the sextics attain the Hasse–Weil–Serre bound. In addition we update 19 entries of genus 6 and 11 entries of genus 4 in manYPoints.org by computer search on these sextics.

1. Introduction

In 1970's Goppa discovered algebro-geometric codes. We can construct good codes by explicit curves with many rational points by his theory. For a curve C over a finite field $\mathbb{F}_q$ of genus g, we have the Hasse–Weil bound

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

which is proved for elliptic curves by Hasse in 1933, and for all curves by Weil in 1941. Here we set p as a prime number and q as a power of p, $\mathbb{F}_q$ as a finite field with q elements. By a curve we mean a projective geometrically irreducible nonsingular algebraic curve.

After Goppa's discovery, in 1983 Serre improved this bound in [**13**] as

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

where $\lfloor\rfloor$ means round down. We call it Serre's bound. A curve attains this bound have a very simple L-function as $(1 + \lfloor 2\sqrt{q}\rfloor T + qT^2)^g$.

A curve attaining the Hasse–Weil bound is called a maximal curve, and there are many interesting research on it; see [**3**], [**4**] and their references. However we do not know the property of a curve attaining Serre's bound which is not maximal when the genus ≥ 4. There are only a few examples of such curves; see [**9**], [**10**], [**11**].

In Section 2, we introduce Wiman's sextic from [**17**], where the geometry was researched in [**6**]. We determine the condition on $\mathbb{F}_p$ and $\mathbb{F}_{p^3}$ over which it attains Serre's bound, where we do it on $\mathbb{F}_{p^2}$ in [**10**]. In Section 3, from [**16**] we introduce a family of Wiman's sextic. We determine the condition on $\mathbb{F}_p$, $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^3}$ over which it attains Serre's bound when the coefficients of its defining equation are in

2010 *Mathematics Subject Classification.* Primary 11G20, 14G05; Secondary 14G50.
Key words and phrases. Algebro-geometric codes; Rational points; Serre's bound.

$\mathbb{F}_p$. We find 19 new curves of genus 6 with many rational points by computer search which can update manYPoints in [**5**]. In Section 4, we find Wiman's sextics of genus 4 attaining Serre's bound, where we determine the condition on $\mathbb{F}_p$, $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^3}$ over which it attains the bound when the coefficients of its defining equation are in $\mathbb{F}_p$. Also we find 11 new curves of genus 4 with many rational points. In Section 5, we find that Edge's sextics attain Serre's bound over $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^3}$ for some p, where we find it attains Serre's bound over $\mathbb{F}_p$ in [**10**]. We also give a conjecture of the condition on $\mathbb{F}_{p^2}$ over which it is maximal.

ACKNOWLEDGMENTS. I would like to thank Nils Bruin for his comment on the Jacobian decomposition of Edge's sextic, Arnaldo Garcia and Takayuki Oda for encouraging me to continue this research. This research was partially supported by JST PRESTO program and JSPS Grant-in-Aid for Young Scientists (B) 25800090.

2. Wiman's sextic I

In 1896 Wiman introduced the sextic

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

in [**17**]. We call it Wiman's sextic and we find it attains Serre's bound. Even the result of Wiman's sextic V is the special case of Wiman's sextic W in Section 3, however this section will show author's spirit to readers.

As preparation, we discuss about the conditions for elliptic curves attaining Serre's bound. 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. Let $p > 2$ and E be an elliptic curve with Weierstrass equation

$$E\colon y^2 = f(x),$$

where $f(x) \in \mathbb{F}_p[x]$ is a cubic polynomial with distinct roots. Set

$$\overline{A} = \text{coefficient of } x^{p-1} \text{ in } f(x)^{(p-1)/2}.$$

From Section V.4 of [**14**], we have the next proposition.

PROPOSITION 1 ([**14**]). *The number of rational points of E over $\mathbb{F}_p$*

$$\#E(\mathbb{F}_p) \equiv 1 - \overline{A} \pmod{p},$$

and E is supersingular if and only if

$$\overline{A} \equiv 0 \pmod{p}.$$

Note that Serre in [**13**] proved the lower bound $\#C(\mathbb{F}_q) \geq q + 1 - g\lfloor 2\sqrt{q}\rfloor$, which we call Serre's lower bound. We use it to prove our assertions afterwards. Now, we start to introduce our results.

THEOREM 2. *Let $p \geq 17$. E over $\mathbb{F}_p$ attains Serre's bound if and only if*

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

PROOF. We start from the "if" part. By Proposition 1, $\#E(\mathbb{F}_p) \equiv 1 - \overline{A} \equiv 1 + \lfloor 2\sqrt{p}\rfloor \pmod{p}$. Here $p+1-\lfloor 2\sqrt{p}\rfloor \leq \#E(\mathbb{F}_p) \leq p+1+\lfloor 2\sqrt{p}\rfloor$ from Serre's bounds. Since $p \geq 17$, we have $1 + \lfloor 2\sqrt{p}\rfloor < p + 1 - \lfloor 2\sqrt{p}\rfloor$. Hence $\#E(\mathbb{F}_p) \neq 1 + \lfloor 2\sqrt{p}\rfloor$, which means $\#E(\mathbb{F}_p) = p + 1 + \lfloor 2\sqrt{p}\rfloor$.

Next we prove the "only if" part. By the assumption, $\#E(\mathbb{F}_p) = p+1+\lfloor 2\sqrt{p}\rfloor$. Because $\#E(\mathbb{F}_p) \equiv 1 - \overline{A} \pmod{p}$, we obtain that $\overline{A} \equiv -\lfloor 2\sqrt{p}\rfloor \pmod{p}$. □

At this point we introduce an elementary lemma, where we require it to prove the next theorem. Let $\mathbb{R}$ be a field of real numbers.

LEMMA 3. *Let $p \geq 11$, and $h(x) = -x^3 + 3px$ be a polynomial in $\mathbb{R}[x]$. Then $h(x) = \lfloor 2p\sqrt{p} \rfloor$ has 3 roots in $\mathbb{R}$. They are ω_1, ω_2 and ω_3 with $\omega_1 < -\lfloor 2\sqrt{p} \rfloor$ and $0 < \omega_2 < \sqrt{p} < \omega_3 < \sqrt{p} + 0.3$.*

PROOF. Write the graphs of $y = h(x)$ and $y = \lfloor 2p\sqrt{p} \rfloor$ on a xy-plane. Since $h(-\lfloor 2\sqrt{p} \rfloor) = \lfloor 2\sqrt{p} \rfloor^3 - 3p\lfloor 2\sqrt{p} \rfloor < 4p\lfloor 2\sqrt{p} \rfloor - 3p\lfloor 2\sqrt{p} \rfloor = p\lfloor 2\sqrt{p} \rfloor < \lfloor 2p\sqrt{p} \rfloor$, one root of $h(x) = \lfloor 2p\sqrt{p} \rfloor$ is less than $-\lfloor 2\sqrt{p} \rfloor$. Because $(\sqrt{p}, 2p\sqrt{p})$ is a local maximum of $y = h(x)$, there are two roots near $\sqrt{p}$. □

For $\overline{A} \in \mathbb{F}_p$, set A as the integer such that $\overline{A} \equiv A \pmod{p}$ and $0 \leq A < p$ throughout this article.

THEOREM 4. *Let $p \geq 11$. With this notation, E over $\mathbb{F}_{p^3}$ attains Serre's bound if and only if*

$$A^3 - 3pA = -\lfloor 2p\sqrt{p} \rfloor.$$

PROOF. The Zeta function of the elliptic curve E over $\mathbb{F}_p$ is given by

$$Z(T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-pT)}.$$

Since $\#E(\mathbb{F}_p) = p + 1 - \alpha - \beta$, we have that $\alpha + \beta \equiv A \pmod{p}$ by Proposition 1. By Serre's bounds for E, we have that $\alpha + \beta$ should be either $A - p$, A or $A + p$. Suppose $\alpha + \beta = A + p$. Then $\#E(\mathbb{F}_p) = 1 - A \leq 1 < p + 1 - \lfloor 2\sqrt{p} \rfloor$ since $A \geq 0$, which gives us a contradiction. So $\alpha + \beta \neq A + p$.

Now we prove the "only if" part. $\#E(\mathbb{F}_{p^3}) = p^3 + 1 + \lfloor 2p\sqrt{p} \rfloor$ by the assumption. Because $\#E(\mathbb{F}_{p^3}) = p^3 + 1 - \alpha^3 - \beta^3$, we have that $-\alpha^3 - \beta^3 = \lfloor 2p\sqrt{p} \rfloor$. Hence $\alpha\beta = p$ implies that $-(\alpha + \beta)^3 + 3p(\alpha + \beta) = \lfloor 2p\sqrt{p} \rfloor$. Then $\alpha + \beta$ should be a root of $-x^3 + 3px = \lfloor 2p\sqrt{p} \rfloor$. Suppose that $\alpha + \beta = A - p$. Since $A < p$, we have $\alpha + \beta < 0$. Thus $\alpha + \beta < -\lfloor 2\sqrt{p} \rfloor$ from the above lemma. It means that $\#E(\mathbb{F}_p) > p + 1 + \lfloor 2\sqrt{p} \rfloor$, which gives us a contradiction to Serre's bound. Therefore we have $\alpha + \beta = A$, which means that $-A^3 + 3pA = \lfloor 2p\sqrt{p} \rfloor$.

Next we prove the "if" part. Suppose $\alpha + \beta = A - p$. By the above lemma, we know that $A < \sqrt{p} + 0.3$ when $p \geq 11$, hence we have that $\alpha + \beta < -2\sqrt{p}$. Thus $\#E(\mathbb{F}_p) = p + 1 - \alpha - \beta > p + 1 + 2\sqrt{p}$, which gives us a contradiction to Serre's bound. Therefore we have $\alpha + \beta = A$, which means that $\#E(\mathbb{F}_{p^3}) = p^3 + 1 - A^3 + 3pA = p^3 + 1 + \lfloor 2p\sqrt{p} \rfloor$. □

Now we come back to Wiman's sextic. Set $p > 5$ afterward in this section. We introduce its Jacobian decomposition from [**10**]. Let J_C be the Jacobian variety of a curve C, and k be a field of characteristic p.

PROPOSITION 5. [**10**] *The Jacobian variety of Wiman's sextic V over a field k decomposes completely as*

$$J_V \sim E_0^6$$

where the elliptic curve is defined by $E_0\colon y^2 = x(5x^2 - 95x + 2^9)$.

Similarly as Corollary 12, the following corollary is immediate.

COROLLARY 6. $\#V(\mathbb{F}_q) = 6\#E_0(\mathbb{F}_q) - 5q - 5$.

Set $m=(p-1)/2$, and the coefficient of x^m in $(5x^2-95x+2^9)^m$ by $\overline{A}_0$. From [**10**] we know that

$$\overline{A}_0=\sum_{i=0}^{\lfloor\frac{m}{2}\rfloor}\frac{m!}{(i!)^2(m-2i)!}\cdot 2^{9i}\cdot 5^{m-i}\cdot(-19)^{m-2i}.$$

Theorem 2 together with Corollary 6 gives the following result.

THEOREM 7. *Let $p\geq 17$. Wiman's sextic V over $\mathbb{F}_p$ attains Serre's bound if and only if*

$$\overline{A}_0\equiv-\lfloor 2\sqrt{p}\rfloor\pmod{p}.$$

Note that 5393, 10019609, 11926193, 14162263, 22861687, etc satisfy the condition of the theorem, where only the first one was introduced in [**10**] as a result of computer search on Wiman's sextic V.

The following theorem is obtained by Theorem 4 and Corollary 6.

THEOREM 8. *Let $p\geq 11$. Wiman's sextic V over $\mathbb{F}_{p^3}$ attains Serre's bound if and only if*

$$A_0^3-3pA_0=-\lfloor 2p\sqrt{p}\rfloor.$$

Note that 67, 28909, 61487, 1721371, 6461821, 48052531, etc satisfy the condition of the above theorem, where only the first one was introduced in [**10**] as a result of computer search on Wiman's sextic V.

3. Wiman's sextic II

In 1895, Wiman in [**16**] defined the sextic

$$W\colon x^6+y^6+1+a(x^4y^2+x^2y^4+x^4+x^2+y^4+y^2)+bx^2y^2=0.$$

When $a=1/2$ and $b=-6$, it is isomorphic to Wiman's sextic V in Section 2.

Remark that Theorem B of Kani and Rosen in [**7**] plays an important role when we decompose a Jacobian variety of a curve in this article. We sometimes use the next corollary which follows directly from Theorem B.

COROLLARY 9. [**12**] *Let C be a curve, $\sigma,\tau\in\mathrm{Aut}(C)$ where $\sigma\neq\tau$, $\sigma\tau=\tau\sigma$, $|\sigma|=|\tau|=|\sigma\tau|=2$. Then we have the isogeny relation*

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

Set $p>5$ in this section.

PROPOSITION 10. *The Jacobian variety of Wiman's sextic W over a field k have the following isogeny relation*

$$J_W\sim H_1^3\times H_2\times J^3_{H_3},$$

where the curves are defined by

$$H_1\colon y^2=((3a-b-3)x-a+3)(1+(a-3)x(1-x)),$$
$$H_2\colon x^3+y^3+1+a(x^2y+xy^2+x^2+x+y^2+y)+bxy=0,$$
$$H_3\colon y^2=-((a+1)x^3+(2a+b)x^2+4ax+4)(x^3+ax^2+ax+1).$$

Proof. The automorphism group of the sextic W contains $\iota\colon (x,y)\mapsto(-x,y)$ and $\rho\colon (x,y)\mapsto(x,-y)$. From Corollary 9, we have the following isogeny relation

$$J_W \times J^2_{W/\langle\iota,\rho\rangle} \sim J_{W/\langle\iota\rangle}\times J_{W/\langle\rho\rangle}\times J_{W/\langle\iota\rho\rangle},$$

while $W/\langle\iota\rangle$, $W/\langle\rho\rangle$ and $W/\langle\iota\rho\rangle$ are birational to

$$H\colon x^3+y^6+1+a(x^2y^2+xy^4+x^2+x+y^4+y^2)+bxy^2=0.$$

Here an explicit map $W\to H_2$ is given by $(x,y)\mapsto(x^2,y^2)$, hence $W/\langle\iota,\rho\rangle$ are birational to H_2. Therefore we have that $J_W\times H_2^2\sim J_H^3$.

Since $\sigma\colon (x,y)\mapsto(x/y^2,1/y)$ and $\tau\colon (x,y)\mapsto(x,-y)$ are automorphisms of H, from Corollary 9 we have that

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

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

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

where we have that

$$H/\langle\sigma\rangle\colon (1-a)(x^3+y^3-3y)+a(x+y)(x^2+y^2-2)+bx=0.$$

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 we have that $H/\langle\sigma\tau\rangle$ is defined by

$$(1-a)(x^3+(y^2+1)(y^2+4)^2)+a(x+y^2+4)(x^2+(y^2+2)(y^2+4))+bx(y^2+4)=0.$$

After transformation on their defining equations, we yield that $H/\langle\sigma\rangle$ and $H/\langle\sigma\tau\rangle$ are birational to H_1 and H_3 respectively. Since the genus of $H/\langle\sigma,\tau\rangle$ is 0 and $H/\langle\tau\rangle$ is isomorphic to H_2, we have

$$J_H\sim H_1\times H_2\times J_{H_3}.$$

Thus we have the isogeny relation $J_W\times H_2^2\sim H_1^3\times H_2^3\times J_{H_3}^3$, and this proves the assertion. □

Afterward, set $b=-6a-3$ and $a(a-3)(a+1)(2a+3)\neq 0$ throughout this section. The following theorem is obtained directly.

Theorem 11. *The Jacobian variety of Wiman's sextic W over a field k has the following isogeny relation*

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

where the elliptic curves are defined by $E_1\colon y^2=xf_1(x)$ and $E_2\colon y^2=xf_2(x)$ with

$$f_1(x)=x^2+(a-3)(7a+6)x-(a-3)(2a+3)^3,$$
$$f_2(x)=x^2-(a-3)(a+2)x-(a-3)(2a+3).$$

Proof. Since $b=-6a-3$, the point $(1,1)$ on H_2 is a singular point. Thus the genus of H_2 is 0. H_1 and H_3 in Proposition 10 are birational to E_1 and E_2 respectively. Hence we have $J_W\sim E_1^3\times E_2^3$. Moreover, E_1 and E_2 are nonsingular when $a(a-3)(a+1)(2a+3)\neq 0$. □

Remark that Wiman's sextic V in Section 2 is a case when E_1 and E_2 are isogenous.

Corollary 12. *If $b=-6a-3$ then $\#W(\mathbb{F}_q)=3\#E_1(\mathbb{F}_q)+3\#E_2(\mathbb{F}_q)-5q-5$.*

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 11 implies that this Tate module is isomorphic to a direct sum of three copies of the Tate module of E_1 and E_2. Hence $t = 3t_1 + 3t_2$, where t_1, t_2 are the trace of Frobenius on the Tate module of E_1 and E_2 respectively. Since $t_1 = q + 1 - \#E_1(\mathbb{F}_q)$ and $t_2 = q + 1 - \#E_2(\mathbb{F}_q)$, the result follows. □

Note that the j-invariants of E_1 and E_2 are respectively

$$\frac{2^8(73a^3 + 45a^2 - 54a - 27)^3}{3^4a^2(a + 1)(2a + 3)^6}, \qquad \frac{2^8(a^3 + a^2 - 2a - 3)^3}{a^2(a + 1)(2a + 3)^2}.$$

Denote the coefficients of x^m in $f_1(x)^m$ and $f_2(x)^m$ by $\overline{A}_1$ and $\overline{A}_2$ respectively, which means that

$$\overline{A}_1 = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m!}{(i!)^2(m-2i)!}(-1)^i(a-3)^{m-i}(7a+6)^{m-2i}(2a+3)^{3i},$$

$$\overline{A}_2 = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m!}{(i!)^2(m-2i)!}(-1)^{m-i}(a-3)^{m-i}(a+2)^{m-2i}(2a+3)^{i}.$$

Theorem 13. *Let $p \geq 17$. Wiman's sextic W over $\mathbb{F}_p$ attains Serre's bound if and only if*

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

Proof. Since we have the isogeny relation $J_W \sim E_1^3 \times E_2^3$, Wiman's sextic W over $\mathbb{F}_p$ attains Serre's bound if and only if both E_1 and E_2 do it by Corollary 12. By Theorem 2 we can prove the condition for E_1 and E_2. □

Note that the pairs (p, a) satisfying these conditions are $(503, 104)$, $(1873, 1026)$, $(2069, 907)$, $(2437, 1009)$, $(5393, 2697)$, $(6131, 2638)$, $(7309, 4030)$, $(8369, 6752)$, etc.

Next we determine the conditions of Wiman's sextic to be maximal, which is defined in the introduction.

Theorem 14. *Let $a \in \mathbb{F}_p$. Wiman's sextic W is maximal over $\mathbb{F}_{p^2}$ if and only if*

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

Proof. Wiman's sextic W over $\mathbb{F}_{p^2}$ is maximal if and only if both E_1 and E_2 are maximal by Corollary 12. From Proposition 1, the elliptic curves E_1 and E_2 over $\mathbb{F}_p$ is supersingular if and only if the coefficients of x^m in $f_1(x)^m$ and $f_2(x)^m$ are zero. Hence we can prove it by the definitions of $\overline{A}_1$ and $\overline{A}_2$. □

Note that (p, a) satisfying these conditions are $(11, 9)$, $(17, 8)$, $(19, 10)$, $(23, 7)$, $(29, 5)$, $(31, 4)$, $(41, 15)$, $(47, 34)$, $(59, 34)$, $(71, 7)$, $(79, 1)$, $(83, 30)$, etc.

Theorem 15. *Let $p \geq 11$ and $a \in \mathbb{F}_p$. Wiman's sextic W over $\mathbb{F}_{p^3}$ attains Serre's bound if and only if*

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

Proof. W over $\mathbb{F}_{p^3}$ attains Serre's bound if and only if both elliptic curves E_1 and E_2 do it by Corollary 12. Theorem 4 gives the condition for E_1 and E_2. □

Note that (p, a) satisfying these conditions are $(67, 34)$, $(97, 35)$, $(101, 22)$, $(103, 100)$, $(193, 101)$, $(673, 340)$, $(677, 40)$, $(787, 98)$, $(1153, 57)$, $(1607, 467)$, etc.

Here, we find new curves of genus 6 by computer search on Wiman's sextic W using MAGMA computational algebra system. Table 1 is the results of W over $\mathbb{F}_p$. For example, when $(a, b) = (34, 12)$, W over $\mathbb{F}_{73}$ has 170 rational points, where the best known lower bound is 140 and the upper bound is 174 by manYPoints in [**5**].

$\mathbb{F}_p$	(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

TABLE 1. W with many points over $\mathbb{F}_p$

When $b = -6a - 3$, we implement Corollary 12 by MAGMA, where Table 2 is our results. For example, W over $\mathbb{F}_{7^3}$ has 512 rational points when $a = \beta^{81}$ where β is a root of $u^3 + 6u^2 + 4 = 0$ in $\mathbb{F}_{7^3}$ and $b = -6a - 3$. Here the best known lower bound is 500 and the upper bound is 564 in [**5**].

$\mathbb{F}_q$	a	primitive poly.	$\#W(\mathbb{F}_q)$	old entry
7^2	4		110	– 134
11^2	9		254	230 – 254
7^3	β^{81}	$u^3 + 6u^2 + 4$	512	500 – 564
11^3	β^{157}	$u^3 + 2u + 9$	1716	1680 – 1764
13^3	β^{425}	$u^3 + 2u + 11$	2714	2690 – 2756
11^5	β^{16525}	$u^5 + 10u^2 + 9$	165756	165720 – 165864
13^5	2		378506	– 378602
17^5	β^{115551}	$u^5 + u + 14$	1434006	– 1434156
19^5	β^{992900}	$u^5 + 5u + 17$	2494688	– 2494982

TABLE 2. W with many points over $\mathbb{F}_q$ when $b = -6a - 3$

4. Wiman's sextic of genus 4

We research on Wiman's sextic W for $a = -1$, 3, where we exclude them in Section 3. Set $p > 3$ in this section.

THEOREM 16. *Let $a = -1$ and $b \neq -6, -2, 2, 3$. The Jacobian variety of Wiman's sextic W over a field k have the following isogeny relation*

$$J_W \sim E_3 \times E_4^3,$$

where the elliptic curves are defined by $E_3\colon y^2 = xf_3(x)$ *and* $E_4\colon y^2 = xf_4(x)$ *with*

$$f_3(x) = x^2 - 2(b+2)^2(b+6)^2(b^2-12)x + (b-2)^3(b+2)^4(b+6)^5,$$
$$f_4(x) = x^2 + 2bx + (b-2)(b+6).$$

PROOF. From Proposition 10, when $a = -1$, the Jacobian variety of Wiman's sextic W over a field k have the following isogeny relation

$$J_W \sim H_2 \times H_3^3,$$

where we have $H_2\colon x^3 + y^3 + 1 - (x^2y + xy^2 + x^2 + x + y^2 + y) + bxy = 0$ and $H_3\colon y^2 = -((b-2)x^2 - 4x + 4)(x+1)$. Actually, H_2 and H_3 are birational to E_3 and E_4 respectively, and E_3 and E_4 are nonsingular when $b \neq -6, -2, 2, 3$. □

Similarly as Corollary 12, the following corollary is immediate.

COROLLARY 17. *If* $a = -1$ *then* $\#W(\mathbb{F}_q) = \#E_3(\mathbb{F}_q) + 3\#E_4(\mathbb{F}_q) - 3q - 3$.

Note that the j-invariants of E_3 and E_4 are respectively

$$-\frac{(b-6)^3(b^3+6b^2+12b-120)^3}{(b-2)^6(b-3)(b+6)^2}, \qquad -\frac{2^4(b-6)^6}{(b-2)^2(b-3)(b+6)^2}.$$

Denote the coefficients of x^m in $f_3(x)^m$ and $f_4(x)^m$ by $\overline{A}_3$ and $\overline{A}_4$ respectively, which means that

$$\overline{A}_3 = (b+2)^{2m} \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m!}{(i!)^2(m-2i)!}(-2(b^2-12))^{m-2i}(b-2)^{3i}(b+6)^{2m+i},$$

$$\overline{A}_4 = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m!}{(i!)^2(m-2i)!}(2b)^{m-2i}(b-2)^i(b+6)^i.$$

THEOREM 18. *Let* $a = -1$ *and* $b \in \mathbb{F}_p \backslash \{-6, -2, 2, 3\}$. *The following hold for Wiman's sextic* W.

(i) *Let* $p \geq 17$. W *over* $\mathbb{F}_p$ *attains Serre's bound if and only if*

$$\overline{A}_3 \equiv \overline{A}_4 \equiv -\lfloor 2\sqrt{p} \rfloor \pmod{p}.$$

(ii) W *over* $\mathbb{F}_{p^2}$ *is maximal if and only if*

$$\overline{A}_3 \equiv \overline{A}_4 \equiv 0 \pmod{p}.$$

(iii) *Let* $p \geq 11$. W *over* $\mathbb{F}_{p^3}$ *attains Serre's bound if and only if*

$$A_3^3 - 3pA_3 = A_4^3 - 3pA_4 = -\lfloor 2p\sqrt{p} \rfloor.$$

PROOF. We can prove (i), (ii) and (iii) similarly as Theorem 13, 14 and 15 respectively. □

Note that the pairs $(p, b) = (541, 6)$, $(853, 6)$, $(1237, 6)$, $(1693, 6)$, $(2221, 6)$, $(2857, 6)$, $(3529, 6)$, $(4273, 6)$, $(7933, 6)$, $(9311, 2982)$, etc satisfy the condition of (i) in the above theorem. The pairs $(p, b) = (5, 1)$, $(11, 0)$, $(17, 6)$, $(23, 0)$, $(29, 6)$, $(41, 6)$, $(47, 0)$, $(53, 6)$, $(59, 0)$, $(71, 0)$, $(83, 0)$, etc satisfy the condition of (ii). The pairs $(p, b) = (61, 5)$, $(67, 19)$, $(193, 1)$, $(199, 82)$, $(397, 66)$, $(673, 51)$, etc satisfy the condition of (iii).

When $a = -1$ and $b = 6$, Wiman's sextic W have an interesting relation with the quotient curve of the Fermat curve in [**9**]. Let the elliptic curves $E_5\colon y^2 = x^3 + 1$ and $E_6\colon y^2 = x^3 - 1$ over a field k.

PROPOSITION 19. [**9**] *Consider the curve* $C\colon y^6 = x^2(4-4x^2)$.

(i) *The Jacobian variety of C over k have the following isogeny relation*

$$J_C \sim E_5^3 \times E_6.$$

(ii) *The curve C over $\mathbb{F}_p$ attains Serre's bound if and only if* $p \equiv 1 \pmod{12}$, $\lfloor\sqrt{p}\rfloor \equiv 2 \pmod 3$, $\lfloor 2\sqrt{p}\rfloor \equiv 1 \pmod 3$ *and there is an integer n such that* $p = \lfloor\sqrt{p}\rfloor^2 + 3n^2$.

THEOREM 20. *Let $a = -1$ and $b = 6$. The following hold for Wiman's sextic W.*

(i) *The Jacobian variety of W over a field k have the following isogeny relation*

$$J_W \sim E_5 \times E_6^3.$$

(ii) *W over a finite field $\mathbb{F}_p$ attains Serre's bound if and only if* $p \equiv 1 \pmod{12}$, $\lfloor\sqrt{p}\rfloor \equiv 2 \pmod 3$, $\lfloor 2\sqrt{p}\rfloor \equiv 1 \pmod 3$ *and there is an integer n such that* $p = \lfloor\sqrt{p}\rfloor^2 + 3n^2$.

(iii) *W over $\mathbb{F}_{p^2}$ is maximal if and only if* $p \equiv 2 \pmod 3$.

PROOF. (i) Since E_3 and E_4 are isogeneous to E_5 and E_6 respectively, it follows from Theorem 16.
(ii) Using (i), we can prove it by the same method as the proof of (ii) of the above proposition in [**9**].
(iii) From Example 4.4 in Chapter V of [**14**], E_5 over $\mathbb{F}_{p^2}$ is maximal if and only if $p \equiv 2 \pmod 3$. By the same method, this condition also holds for E_6. Therefore the result follows from (i). □

Note that the prime numbers 541, 853, 1237, 1693, 2221, 2857, 3529, 4273, 7933, 11497, etc satisfy the condition in (ii) of the above theorem.

THEOREM 21. *Let $a = 3$ and $b \neq -21, 6$. The Jacobian variety of Wiman's sextic W over a field k have the following isogeny relation*

$$J_W \sim E_7 \times E_8^3,$$

where the elliptic curves are defined by $E_7\colon y^2 = f_7(x)$ *and* $E_8\colon y^2 = f_8(x)$ *with*

$$f_7(x) = x^3 - 3^3(b+18)(b-6)^3x + 2\cdot 3^3(b^2+24b+36)(b-6)^4,$$
$$f_8(x) = x^3 - (b-6)x^2 - 2^2(b-6)^2.$$

PROOF. From Proposition 10, the Jacobian variety of Wiman's sextic W over a field k have the following isogeny relation when $a = 3$.

$$J_W \sim H_2 \times H_3^3,$$

where we have that $H_2\colon x^3 + y^3 + 1 + 3(x^2y + xy^2 + x^2 + x + y^2 + y) + bxy = 0$ and $H_3\colon y^2 = -(4x^3 + (b+6)x^2 + 12x + 4)(x+1)$. Actually, H_2 and H_3 are birational to E_7 and E_8 respectively, and E_7 and E_8 are nonsingular when $b \neq -21, 6$. □

Similarly as Corollary 12, the following corollary is immediate.

COROLLARY 22. *If $a = 3$ then* $\#W(\mathbb{F}_q) = \#E_7(\mathbb{F}_q) + 3\#E_8(\mathbb{F}_q) - 3q - 3$.

Note that the j-invariants of E_7 and E_8 are respectively

$$-\frac{(b-6)(b+18)^3}{b+21}, \qquad -\frac{2^4(b-6)^2}{b+21}.$$

Denote the coefficients of x^{p-1} in $f_7(x)^m$ and $f_8(x)^m$ by $\overline{A}_7$ and $\overline{A}_8$ respectively, which means that

$$\overline{A}_7 = \sum_{i=\lceil \frac{p-1}{4} \rceil}^{\lfloor \frac{p-1}{3} \rfloor} \frac{m!\ 2^{2i-m}3^{3m-3i}}{i!(2i-m)!(2m-3i)!}(-b-18)^{2m-3i}(b-6)^{2m-i}(b^2+24b+36)^{2i-m},$$

$$\overline{A}_8 = \sum_{i=0}^{\lfloor \frac{\lfloor \frac{p-1}{3} \rfloor}{2} \rfloor} \frac{m!\ (-1)^{m-2i}2^{2i}}{i!(2i)!(m-3i)!}(b-6)^{m-i}.$$

Here $\lceil\rceil$ means round up.

Theorem 23. *Let $a = 3$ and $b \in \mathbb{F}_p \backslash \{-21, 6\}$. The following hold for Wiman's sextic W.*

(i) *Let $p \geq 17$. W over $\mathbb{F}_p$ attains Serre's bound if and only if*

$$\overline{A}_7 \equiv \overline{A}_8 \equiv -\lfloor 2\sqrt{p} \rfloor \pmod p.$$

(ii) *W over $\mathbb{F}_{p^2}$ is maximal if and only if*

$$\overline{A}_7 \equiv \overline{A}_8 \equiv 0 \pmod p.$$

(iii) *Let $p \geq 11$. W over $\mathbb{F}_{p^3}$ attains Serre's bound if and only if*

$$A_7^3 - 3pA_7 = A_8^3 - 3pA_8 = -\lfloor 2p\sqrt{p} \rfloor.$$

Proof. We can prove (i), (ii) and (iii) similarly as Theorem 13, Theorem 14 and Theorem 15 respectively. □

Note that the pairs satisfy the condition in (i) of the above theorem are (p, b)= $(9311, 7969)$, $(13751, 1913)$, $(19181, 1245)$, $(23057, 9510)$, $(37243, 4693)$, etc. The pairs satisfy (ii) are $(p, b) = (11, 7)$, $(23, 21)$, $(29, 11)$, $(41, 17)$, $(47, 46)$, $(59, 11)$, $(71, 7)$, $(83, 35)$, etc. The pairs satisfy (iii) are $(p, b) = (11, 9)$, $(61, 17)$, $(67, 25)$, $(83, 41)$, $(193, 72)$, $(199, 192)$, $(397, 125)$, $(443, 62)$, etc. Here, we implement Corollary 17 and 22 by MAGMA, and find new curves of genus 4, which we list in Table 3. For example, W over $\mathbb{F}_{5^3}$ has 198 rational points when $a = 3$ and $b = \beta^{11}$ where β is a root of $u^3 + 3u + 3 = 0$ in $\mathbb{F}_{5^3}$. Here the best known lower bound is 196 and the upper bound is 211 in [**5**].

$\mathbb{F}_q$	(a, b)	primitive poly.	$\#W(\mathbb{F}_q)$	old entry
5^3	$(3, \beta^{11})$	$u^3 + 3u + 3$	198	196 – 211
7^3	$(-1, 4)$		480	454 – 489
11^3	$(3, 9)$		1620	1580 – 1620
13^3	$(-1, \beta^{87})$	$u^3 + 2u + 11$	2538	2510 – 2570
17^3	$(3, \beta^{956})$	$u^3 + u + 14$	5430	5414 – 5474
19^3	$(3, 11)$		7500	7470 – 7520
7^5	$(-1, \beta^{3519})$	$u^5 + u + 4$	17784	17780 – 17840
11^5	$(-1, \beta^{35534})$	$u^5 + 10u^2 + 9$	164196	– 164260
13^5	$(3, \beta^{11241})$	$u^5 + 4u + 11$	376086	– 376166
17^5	$(3, \beta^{573629})$	$u^5 + u + 14$	1429254	– 1429390
19^5	$(-1, \beta^{634132})$	$u^5 + 5u + 17$	2488608	– 2488688

Table 3. W of genus 4 with many points

5. Edge's sextic

In 1980 Edge introduced a family of sextics in [**2**] to research on Wiman's sextic V. It is defined by the following defining equation

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

We denote it by G, and call it Edge's sextic; see also [**1**] for its geometrical properties. It is Wiman's sextic V in Section 2 when $\alpha=0$.

Set $p>3$ in this section.

Proposition 24. *The Jacobian variety of Edge's sextic over a field k have the following isogeny relation*

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

where $D\colon y^2=h_\alpha(x)$ *and* $D'\colon y^2=h_{-\alpha}(x)$ *with*

$$h_\alpha(x)=(-6x^3+(9+\alpha)x^2-(\alpha+7)x+2)(2x^3+(1+\alpha)x^2+(1-\alpha)x+2).$$

Proof. We have $\sigma\colon (x,y)\mapsto(-x,y)$ and $\tau\colon (x,y)\mapsto(x,-y)$ as automorphisms of the sextic G. Applying Corollary 9 to G we obtain that

$$J_G\times J^2_{G/\langle\sigma,\tau\rangle}\sim J_{G/\langle\sigma\rangle}\times J_{G/\langle\tau\rangle}\times J_{G/\langle\sigma\tau\rangle},$$

Here $G/\langle\sigma\rangle$ is birational to

$$x^3+y^6+1+(x+y^2+1)(x^2+y^4+1)-12xy^2+\alpha(y^2-1)(1-x)(x-y^2)=0.$$

After we set $y^2=uX+1$ and $x=X+1$, we can denote this equation as

$$X^2((2u^3+(1+\alpha)u^2+(1-\alpha)u+2)X+8(u^2-u+1))=0.$$

Since $y^2=uX+1$, we have that

$$y^2=1-8u(u^2-u+1)/(2u^3+(1+\alpha)u^2+(1-\alpha)u+2).$$

Therefore, it is birational to $D\colon y^2=h_\alpha(x)$.

Similarly, we have that $G/\langle\tau\rangle$ and $G/\langle\sigma\tau\rangle$ are birational to D'. Since the genus of $G/\langle\sigma,\tau\rangle$ is 0, we can prove the assertion. □

Corollary 25. $\#G(\mathbb{F}_q)=3\#D(\mathbb{F}_q)-2q-2$.

Proof. It is well known that $\#G(\mathbb{F}_q)=q+1-t$, where t is the trace of Frobenius acting on a Tate module of J_G. Theorem 24 implies that this Tate module is isomorphic to a direct sum of the Tate modules of J_D and two copies of the Tate module of $J_{D'}$. Hence $t=t_1+2t_2$, where t_1 and t_2 are the traces of Frobenius on the Tate modules of J_D and $J_{D'}$ respectively. Since we have $\#D(\mathbb{F}_q)=\#D'(\mathbb{F}_q)$, $t_1=q+1-\#D(\mathbb{F}_q)$ and $t_2=q+1-\#D'(\mathbb{F}_q)$, the result follows. □

We implement Corollary 25 by KASH/KANT computational algebra system, and find maximal curves.

Example 26. Edge's sextic G is maximal over $\mathbb{F}_{p^2}$ for (p,α) is equal to $(19,0)$, $(29,0)$, $(59,12)$, $(79,0)$, $(109,\beta^{715})$ where β is a root of $u^2-u+6=0$ in $\mathbb{F}_{109^2}$, $(139,12)$, $(149,33)$, $(179,42)$, $(199,0)$, etc.

Next, let

$$h_\alpha(x)^m=\sum_{j=0}^{N}c_j(\alpha)x^j,\quad M(\alpha)=\begin{pmatrix} c_{p-1}(\alpha) & c_{p-2}(\alpha)\\ c_{2p-1}(\alpha) & c_{2p-2}(\alpha)\end{pmatrix}.$$

Here, $M(\alpha)^{(1/p)}$ is called the Hasse–Witt matrix of the curve D.

Proposition 27. *If Edge's sextic G over $\mathbb{F}_{p^2}$ is maximal then $M(\alpha) = 0$.*

Proof. If G is maximal then D is maximal by Corollary 25. When D is maximal, we can prove it by Theorem 4.1 of [**15**]. □

Here, we have a conjecture.

Conjecture 28. *Edge's sextic G over $\mathbb{F}_{p^2}$ is maximal if and only if*

$$c_{p-1}(\alpha) = c_{p-2}(\alpha) = 0.$$

Assume $\alpha \in \mathbb{F}_p$. We make computer search on D over $\mathbb{F}_{p^3}$ to find G over $\mathbb{F}_{p^3}$ attains Serre's bound by Corollary 25. To reduce the computational complexity, we use the numbers of rational points of D over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ to compute them over $\mathbb{F}_{p^3}$. We list the algorithm here, which induces from the theory of Zeta function; see 5.2. of [**8**] for example. Here we set $n_i = \#D(\mathbb{F}_{p^i})$ for $i = 1, 2, 3$.

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 $x^4 + a_1x^3 + a_2x^2 + pa_1x + p^2 = 0$
  $n_3 \leftarrow p^3 + 1 - \sum_{i=1}^4 {\omega_i}^3$
Output n_3

We implement it by KASH/KANT, and find curves attaining Serre's bound.

Example 29. Edge's sextic G over $\mathbb{F}_{p^3}$ attains Serre's bound when (p, α) is equal to $(67, 0)$, $(229, 110)$, $(787, 356)$, $(1021, 230)$, $(1153, 154)$, $(1229, 67)$, etc.

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. Güneri, H. Stichtenoth, A generalization of the Giulietti–Korchmáros 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.

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

[8] T. Katsura, Introduction to algebraic geometry (in Japanese), Kyoritsu shuppan 1998.

[9] 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.

[10] M. Q. Kawakita, Wiman's and Edge's sextic attaining Serre's bound, submitted to Appl. Algebra Engrg. Comm. Comput..

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

[12] J. Paulhus, Jacobians of curves with extra automorphisms, Acta Arith. **132**(3)(2008), 231–244.

[13] 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.

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

[15] S. Tafazolian, On supersingular curves over finite field, PhD Thesis, IMPA 2008.

[16] A. Wiman, Ueber eine einfache Gruppe von 360 ebenen Collineationen, Math. Ann. **48**(1896), 531–556.

[17] A. Wiman, Zur Theorie der endlichen Gruppen von birationalen Transformationen in der Ebene, Math. Ann. **48**(1896), 195–240.

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

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