An $\mathbb{F}_{p^2}$-maximal Wiman's sextic and its automorphisms

Massimo Giulietti, Motoko Kawakita, Stefano Lia and Maria Montanucci

Keywords: Hermitian curve, Unitary groups, Quotient curves, Maximal curves, Wiman's sextic
2000 MSC: 11G20, 14H37

Abstract

In 1895 Wiman introduced a Riemann surface $\mathcal{W}$ of genus 6 over the complex field $\mathbb{C}$ defined by the homogeneous equation $\mathcal{W} : X^6+Y^6+Z^6+(X^2+Y^2+Z^2)(X^4+Y^4+Z^4)-12X^2Y^2Z^2 = 0$, and showed that its full automorphism group is isomorphic to the symmetric group S_5. In [23] the curve $\mathcal{W}$ was studied as a curve defined over a finite field $\mathbb{F}_{p^2}$ where p is a prime, and necessary and sufficient conditions for its maximality over $\mathbb{F}_{p^2}$ were obtained. In this paper we first show that the result of Wiman concerning the automorphism group of $\mathcal{W}$ holds also over an algebraically closed field $\mathbb{K}$ of positive characteristic p, provided that $p \geq 7$. For $p = 2, 3$ the polynomial $X^6+Y^6+Z^6+(X^2+Y^2+Z^2)(X^4+Y^4+Z^4)-12X^2Y^2Z^2$ is not irreducible over $\mathbb{K}$, while for $p = 5$ the curve $\mathcal{W}$ is rational and $Aut(\mathcal{W}) \cong \mathrm{PGL}(2, \mathbb{K})$. We also show that the $\mathbb{F}_{19^2}$-maximal Wiman's sextic $\mathcal{W}$ is not Galois covered by the Hermitian curve $\mathcal{H}_{19}$ over $\mathbb{F}_{19^2}$.

1 Introduction

For q a prime power, let $\mathbb{F}_{q^2}$ be the finite field with q^2 elements and $\mathcal{C}$ be a projective, absolutely irreducible, non-singular algebraic curve of genus g defined over $\mathbb{F}_{q^2}$. The curve $\mathcal{C}$ is called $\mathbb{F}_{q^2}$-maximal if the number $|\mathcal{C}(\mathbb{F}_{q^2})|$ of its $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil upper bound

$$q^2 + 1 + 2gq.$$

Surveys on maximal curves are found in [6, 7, 8, 10, 34, 35] and [19, Chapter 10]. By a result commonly referred as the Kleiman-Serre covering result, see [24] and [25, Proposition 6], a curve $\mathcal{C}$ defined over $\mathbb{F}_{q^2}$ which is $\mathbb{F}_{q^2}$-covered by an $\mathbb{F}_{q^2}$-maximal curve is $\mathbb{F}_{q^2}$-maximal as well. In particular, $\mathbb{F}_{q^2}$-maximal curves can be obtained as Galois $\mathbb{F}_{q^2}$-subcovers of an $\mathbb{F}_{q^2}$-maximal curve $\mathcal{C}$, that is, as quotient curves $\mathcal{C}/G$ where G is a finite automorphism group of $\mathcal{C}$ defined over $\mathbb{F}_{q^2}$. Most of the known $\mathbb{F}_{q^2}$-maximal curves are Galois covered by the Hermitian curve $\mathcal{H}_q : X^q + X = Y^{q+1}$; see e.g. [12, 3, 13] and the references therein.

The first example of a maximal curve which is not Galois covered by the Hermitian curve was discovered by Garcia and Stichtenoth [11]. This curve is $\mathbb{F}_{3^6}$-maximal and it is not Galois covered by $\mathcal{H}_{27}$. It is a special case of the $\mathbb{F}_{q^6}$-maximal GS curve, which was later shown not to be Galois covered by $\mathcal{H}_{q^3}$ for any $q > 3$, [17, 27]. Giulietti and Korchmáros [15] provided an $\mathbb{F}_{q^6}$-maximal curve, nowadays referred to as the GK curve, which is not covered by the Hermitian curve $\mathcal{H}_{q^3}$ for any $q > 2$. Two generalizations of the GK curve were introduced by Garcia, Güneri and Stichtenoth [9] and by Beelen and Montanucci in [1]. Both these two generalizations are $\mathbb{F}_{q^{2n}}$-maximal curves, for any q and odd $n \geq 3$. Also, they are not Galois covered by the Hermitian curve $\mathcal{H}_{q^n}$ for $q > 2$ and $n \geq 5$, see [5, 1]; the Garcia-Güneri-Stichtenoth's generalization is also

not Galois covered by $\mathcal{H}_{2^n}$ for $q = 2$, see [17]. The existence of infinite families of $\mathbb{F}_{p^2}$-maximal curves that are not Galois covered by $\mathcal{H}_p$ is an interesting open problem.

In 1895 Wiman [36] introduced a Riemann surface $\mathcal{W}$ over the complex field $\mathbb{C}$ defined by the homogeneous equation of degree 6

$$\mathcal{W} : X^6 + Y^6 + Z^6 + (X^2 + Y^2 + Z^2)(X^4 + Y^4 + Z^4) - 12X^2Y^2Z^2 = 0,$$

whose full automorphism group is isomorphic to the symmetric group S_5. The Jacobian of $\mathcal{W}$ decomposes completely as the product of the Jacobian of an elliptic curve ϵ six times. This fact, together with the nice projective model of $\mathcal{W}$, stimulated the investigation of the reduction mod p of the curve $\mathcal{W}$ and its properties over finite fields of characteristic p. Indeed Kawakita [23] used the complete decomposition of the Jacobian of $\mathcal{W}$ to apply Kani-Rosen Theorem [22], and obtained necessary and sufficient conditions for the maximality of $\mathcal{W}$ over $\mathbb{F}_{p^2}$. In particular, $\mathcal{W}$ is $\mathbb{F}_{p^2}$-maximal for infinite primes p; see also Section 2.

In this paper the result of Wiman concerning the structure of the full automorphism group of $\mathcal{W}$ is extended to any algebraically closed field of characteristic $p \geq 7$. For $p = 2, 3$ the homogeneous polynomial defining $\mathcal{W}$ is not irreducible, while for $p = 5$ the curve $\mathcal{W}$ is rational.

We also show that the $\mathbb{F}_{19^2}$-maximal curve $\mathcal{W}$ is not Galois covered by the Hermitian curve $\mathcal{H}_{19}$ over $\mathbb{F}_{19^2}$. This makes the Wiman sextics a natural candidate to provide the first example of an infinite family of $\mathbb{F}_{p^2}$-maximal curves that are not covered by the Hermitian curve.

The paper is organized as follows. Section 2 provided a collection of preliminary results on the Hermitian curve and its automorphisms, on the Wiman's sextic $\mathcal{W}$ and on automorphism groups of algebraic curves in characteristic $p > 0$. In Section 3 the full automorphism group of $\mathcal{W}$ is computed over algebraically closed field of characteristic $p \geq 7$, extending the result of Wiman [36] to the positive characteristic case. Finally, in Section 4, the $\mathbb{F}_{19^2}$-maximal Wiman's sextic $\mathcal{W}$ is shown not to be Galois covered by the Hermitian curve $\mathcal{H}_{19}$ over $\mathbb{F}_{19^2}$.

2 Preliminary results

2.1 The Wiman's sextic $\mathcal{W}$

In 1895 Wiman introduced in [36] a Riemann surface $\mathcal{W}$ over the complex field $\mathbb{C}$ defined by the homogeneous equation of degree 6

$$\mathcal{W} : X^6 + Y^6 + Z^6 + (X^2 + Y^2 + Z^2)(X^4 + Y^4 + Z^4) - 12X^2Y^2Z^2 = 0. \tag{1}$$

The irreducible curve $\mathcal{W}$ has genus 6 and 4 ordinary double points, namely $[1 : 1 : 1]$, $[1 : -1 : 1]$, $[-1 : 1 : 1]$, $[-1 : -1 : 1]$.

In [23] the curve $\mathcal{W}$ is studied as a curve defined over a finite field $\mathbb{F}_{p^2}$, where p is a prime. Primes p for which $\mathcal{W}$ is $\mathbb{F}_p$-maximal are characterized by applying the Kani-Rosen Theorem [22], taking into account that the Jacobian $J_{\mathcal{W}}$ of $\mathcal{W}$ decomposes completely as $J_{\mathcal{W}} \sim \epsilon^6$ where ϵ is the elliptic curve defined by the homogeneous equation $\epsilon : Y^2Z - X(5X^2 - 95XZ + 2^9Z^3)$. It turns out that $\mathcal{W}$ is $\mathbb{F}_{p^2}$-maximal if and only if the characteristic p satisfies the equation:

$$\sum_{i=0}^{\lfloor m/2 \rfloor} \frac{m!}{(i!)^2(m-2i)!} 2^{9i} 5^{-m-i} (-19)^{m-2i} \equiv 0 \pmod{p}. \tag{2}$$

Explicit values of p for which Equation (2) is satisfied are also found in [23]:

$$p = 19, 29, 79, 199, 269, 359, 439, 499, 509, 599, 919, 1279.$$

Wiman showed that the automorphism group $Aut(\mathcal{W})$ of $\mathcal{W}$ over $\mathbb{C}$ is isomorphic to S_5, the symmetric group on 5 letters.

In Section 3 we show that the same result holds true over an algebraically closed field of positive characteristic $p \geq 7$. The reason why p has to be at least 7 is that for $p = 2, 3$ the polynomial (1) is reducible, while for $p = 5$ the curve $\mathcal{W}$ is rational and hence its full automorphism group is the projective general linear group over the algebraic closure of $\mathbb{F}_5$.

2.2 The Hermitian curve and its automorphism group

Throughout this section, $q = p^n$, where p is a prime number, n is a positive integer and $\mathbb{K}$ is the algebraic closure of the finite field with q elements $\mathbb{F}_q$. The Deligne-Lusztig curves defined over $\mathbb{F}_q$ were originally introduced in [4]. Other than the projective line, there are three families of Deligne-Lusztig curves, named Hermitian curves, Suzuki curves and Ree curves. The Hermitian curve $\mathcal{H}_q$ arises from the algebraic group ${}^2A_2(q) = \mathrm{PGU}(3, q)$ of order $(q^3 + 1)q^3(q^2 - 1)$. It has genus $q(q-1)/2$ and is $\mathbb{F}_{q^2}$-maximal. This curve is isomorphic to the curves listed below:

$$X^{q+1} + Y^{q+1} + Z^{q+1} = 0; \tag{3}$$

$$X^q Z + X Z^q - Y^{q+1} = 0; \tag{4}$$

$$XY^q - YX^q + \omega Z^{q+1} = 0, \tag{5}$$

where ω is a fixed element of $\mathbb{K}$ such that $\omega^{q-1} = -1$;

$$XY^q + YZ^q + \omega ZX^q = 0. \tag{6}$$

Each of the models (3),(4) and (5) is $\mathbb{F}_{q^2}$-isomorphic to $\mathcal{H}_q$, while the model (6) is $\mathbb{F}_{q^6}$-isomorphic to $\mathcal{H}_q$, since for a suitable element $a \in \mathbb{F}_{q^6}$, the projective map

$$k : \mathbb{P}^2(\mathbb{K}) \to \mathbb{P}^2(\mathbb{K}),\ (X : Y : Z) \mapsto (aX + Y + a^{q^2+1}Z : a^{q^2+1}X + aY + Z : x + a^{q^2+1}Y + aZ),$$

changes (3) into (6), see [2, Proposition 4.6].

The automorphism group $\mathrm{Aut}(\mathcal{H}_q)$ is isomorphic to the projective unitary group $\mathrm{PGU}(3, q)$, and it acts on the set $\mathcal{H}_q(\mathbb{F}_{q^2})$ of all $\mathbb{F}_{q^2}$-rational points of $\mathcal{H}_q$ as $\mathrm{PGU}(3, q)$ in its usual 2-transitive permutation representation. The combinatorial properties of $\mathcal{H}_q(\mathbb{F}_{q^2})$ can be found in [21]. The size of $\mathcal{H}_q(\mathbb{F}_{q^2})$ is equal to $q^3 + 1$, and a line of $\mathrm{PG}(2, q^2)$ has either 1 or $q + 1$ common points with $\mathcal{H}_q(\mathbb{F}_{q^2})$. In the former case the line is said to be a 1-secant or tangent, in the former case a $(q + 1)$-secant or chord. A unitary polarity is associated with $\mathcal{H}_q(\mathbb{F}_{q^2})$; its isotropic points are those in $\mathcal{H}_q(\mathbb{F}_{q^2})$, and its isotropic lines are the 1-secants of $\mathcal{H}_q(\mathbb{F}_{q^2})$, that is, the tangents to $\mathcal{H}_q$ at the points of $\mathcal{H}_q(\mathbb{F}_{q^2})$.

A useful tool in our investigation is the classification of maximal subgroups of the projective special subgroup $\mathrm{PSU}(3, q)$ of $\mathrm{PGU}(3, q)$, going back to Mitchell and Hartley; see [28], [18], [20].

Theorem 2.1. *Let $d = \gcd(3, q + 1)$. Up to conjugacy, the subgroups below give a complete list of maximal subgroups of* $\mathrm{PSU}(3, q)$.

(i) the stabilizer of an $\mathbb{F}_{q^2}$-rational point of $\mathcal{H}_q$. It has order $q^3(q^2 - 1)/d$;

(ii) the stabilizer of an $\mathbb{F}_{q^2}$-rational point off $\mathcal{H}_q$ (equivalently the stabilizer of a chord of $\mathcal{H}_q(\mathbb{F}_{q^2})$). It has order $q(q-1)(q+1)^2/d$;

(iii) the stabilizer of a self-polar triangle with respect to the unitary polarity associated to $\mathcal{H}_q(\mathbb{F}_{q^2})$. It has order $6(q+1)^2/d$;

(iv) the normalizer of a (cyclic) Singer subgroup. It has order $3(q^2-q+1)/d$ and preserves a triangle in $\mathrm{PG}(2,q^6)\setminus\mathrm{PG}(2,q^2)$ left invariant by the Frobenius collineation $\Phi_{q^2}:(X,Y,T)\mapsto(X^{q^2},Y^{q^2},T^{q^2})$ of $\mathrm{PG}(2,\mathbb{K})$;

for $p>2$:

(v) $\mathrm{PGL}(2,q)$ preserving a conic;

(vi) $\mathrm{PSU}(3,p^m)$ with $m \mid n$ and n/m odd;

(vii) subgroups containing $\mathrm{PSU}(3,p^m)$ as a normal subgroup of index 3, when $m \mid n$, n/m is odd, and 3 divides both n/m and $q+1$;

(viii) the Hessian groups of order 216 when $9 \mid (q+1)$, and of order 72 and 36 when $3 \mid (q+1)$;

(ix) $\mathrm{PSL}(2,7)$ when $p=7$ or -7 is not a square in $\mathbb{F}_q$;

(x) the alternating group A_6 when either $p=3$ and n is even, or 5 is a square in $\mathbb{F}_q$ but $\mathbb{F}_q$ contains no cube root of unity;

(xi) the symmetric group S_6 when $p=5$ and n is odd;

(xii) the alternating group A_7 when $p=5$ and n is odd;

for $p=2$:

(xiii) $\mathrm{PSU}(3,2^m)$ with $m \mid n$ and n/m an odd prime;

(xiv) subgroups containing $\mathrm{PSU}(3,2^m)$ as a normal subgroup of index 3, when $n=3m$ with m odd;

(xv) a group of order 36 when $n=1$.

In the following, a subgroup $G \le \mathrm{PGU}(3,q)$ is said to be *tame* if its order is coprime to p and *non-tame* otherwise.

In our investigation it is also useful to know how an element of $\mathrm{PGU}(3,q)$ of a given order acts on $\mathrm{PG}(2,\mathbb{K})$, and in particular on $\mathcal{H}_q(\mathbb{F}_{q^2})$. This is stated in Lemma 2.2 with the usual terminology about collineations of projective planes; see e.g. [21]. In particular, a linear collineation σ of $\mathrm{PG}(2,\mathbb{K})$ is a (P,ℓ)-*perspectivity*, if σ preserves each line through the point P (the *center* of σ), and fixes each point on the line ℓ (the *axis* of σ). A (P,ℓ)-perspectivity is either an *elation* or a *homology* according as $P \in \ell$ or $P \notin \ell$. A (P,ℓ)-perspectivity is in $\mathrm{PGL}(3,q^2)$ if and only if its center and its axis are in $\mathrm{PG}(2,\mathbb{F}_{q^2})$.

Lemma 2.2. ([30, Lemma 2.3]) *For a nontrivial element $\sigma \in \mathrm{PGU}(3,q)$, one of the following cases holds.*

(A) $\mathrm{ord}(\sigma) \mid (q+1)$ and σ is a homology whose center P is a point off $\mathcal{H}_q$ and whose axis ℓ is a chord of $\mathcal{H}_q(\mathbb{F}_{q^2})$ such that (P,ℓ) is a pole-polar pair with respect to the unitary polarity associated to $\mathcal{H}_q(\mathbb{F}_{q^2})$.

(B) $\mathrm{ord}(\sigma)$ is coprime to p and σ fixes the vertices P_1,P_2,P_3 of a non-degenerate triangle T.

(B1) *The points P_1, P_2, P_3 are $\mathbb{F}_{q^6}$-rational, $P_1, P_2, P_3 \notin \mathcal{H}_q$ and the triangle T is self-polar with respect to the unitary polarity associated to $\mathcal{H}_q(\mathbb{F}_{q^2})$. Also,* $\mathrm{ord}(\sigma) \mid (q+1)$.

(B2) *The points P_1, P_2, P_3 are $\mathbb{F}_{q^6}$-rational, $P_1 \notin \mathcal{H}_q$, $P_2, P_3 \in \mathcal{H}_q$. Also,* $\mathrm{ord}(\sigma) \mid (q^2-1)$ *and* $\mathrm{ord}(\sigma) \nmid (q+1)$.

(B3) *The points P_1, P_2, P_3 have coordinates in $\mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$, $P_1, P_2, P_3 \in \mathcal{H}_q$. Also,* $\mathrm{ord}(\sigma) \mid (q^2-q+1)$.

(C) $\mathrm{ord}(\sigma) = p$ *and σ is an elation whose center P is a point of $\mathcal{H}_q$ and whose axis ℓ is a tangent of $\mathcal{H}_q(\mathbb{F}_{q^2})$; here (P, ℓ) is a pole-polar pair with respect to the unitary polarity associated to $\mathcal{H}_q(\mathbb{F}_{q^2})$.*

(D) $\mathrm{ord}(\sigma) = p$ *with $p \neq 2$, or* $\mathrm{ord}(\sigma) = 4$ *and $p = 2$. In this case σ fixes an $\mathbb{F}_{q^6}$-rational point P, with $P \in \mathcal{H}_q$, and a line ℓ which is a tangent of $\mathcal{H}_q(\mathbb{F}_{q^2})$; here (P, ℓ) is a pole-polar pair with respect to the unitary polarity associated to $\mathcal{H}_q(\mathbb{F}_{q^2})$.*

(E) $p \mid \mathrm{ord}(\sigma)$, $p^2 \nmid \mathrm{ord}(\sigma)$, *and* $\mathrm{ord}(\sigma) \neq p$. *In this case σ fixes two $\mathbb{F}_{q^6}$-rational points P, Q, with $P \in \mathcal{H}_q$, $Q \notin \mathcal{H}_q$.*

Throughout the paper, a nontrivial element of $\mathrm{PGU}(3,q)$ is said to be of type (A), (B), (B1), (B2), (B3), (C), (D), or (E), as given in Lemma 2.2.

Every subgroup G of $\mathrm{PGU}(3,q)$ produces a quotient curve $\mathcal{H}_q/G$, and the cover $\mathcal{H}_q \to \mathcal{H}_q/G$ is a Galois cover defined over $\mathbb{F}_{q^2}$ where the degree of the different divisor Δ is given by the Riemann-Hurwitz formula [32, Theorem 3.4.13],

$$\Delta = (2g(\mathcal{H}_q) - 2) - |G|(2g(\mathcal{H}_q/G) - 2). \tag{7}$$

On the other hand, $\Delta = \sum_{\sigma \in G \setminus \{id\}} i(\sigma)$, where $i(\sigma) \geq 0$ is given by the Hilbert's different formula [32, Thm. 3.8.7], namely

$$i(\sigma) = \sum_{P \in \mathcal{H}_q(\bar{\mathbb{F}}_q)} v_P(\sigma(t) - t), \tag{8}$$

where t is a local parameter at P.

By analyzing the geometric properties of the elements $\sigma \in \mathrm{PGU}(3,q)$, it turns out that there are only a few possibilities for $i(\sigma)$. This is obtained as a corollary of Lemma 2.2 and stated in the following proposition, see [30].

Theorem 2.3. ([30, Theorem 2.7]) *For a nontrivial element $\sigma \in \mathrm{PGU}(3,q)$ one of the following cases occurs.*

1. *If* $\mathrm{ord}(\sigma) = 2$ *and* $2 \mid (q+1)$, *then σ is of type* (A) *and* $i(\sigma) = q+1$.
2. *If* $\mathrm{ord}(\sigma) = 3$, $3 \mid (q+1)$ *and σ is of type* (B3), *then* $i(\sigma) = 3$.
3. *If* $\mathrm{ord}(\sigma) \neq 2$, $\mathrm{ord}(\sigma) \mid (q+1)$ *and σ is of type* (A), *then* $i(\sigma) = q+1$.
4. *If* $\mathrm{ord}(\sigma) \neq 2$, $\mathrm{ord}(\sigma) \mid (q+1)$ *and σ is of type* (B1), *then* $i(\sigma) = 0$.
5. *If* $\mathrm{ord}(\sigma) \mid (q^2-1)$ *and* $\mathrm{ord}(\sigma) \nmid (q+1)$, *then σ is of type* (B2) *and* $i(\sigma) = 2$.
6. *If* $\mathrm{ord}(\sigma) \neq 3$ *and* $\mathrm{ord}(\sigma) \mid (q^2-q+1)$, *then σ is of type* (B3) *and* $i(\sigma) = 3$.
7. *If* $p = 2$ *and* $\mathrm{ord}(\sigma) = 4$, *then σ is of type* (D) *and* $i(\sigma) = 2$.
8. *If* $\mathrm{ord}(\sigma) = p$, $p \neq 2$ *and σ is of type* (D), *then* $i(\sigma) = 2$.
9. *If* $\mathrm{ord}(\sigma) = p$ *and σ is of type* (C), *then* $i(\sigma) = q+2$.
10. *If* $\mathrm{ord}(\sigma) \neq p$, $p \mid \mathrm{ord}(\sigma)$ *and* $\mathrm{ord}(\sigma) \neq 4$, *then σ is of type* (E) *and* $i(\sigma) = 1$.

2.3 Automorphism groups of algebraic curves

This section provides a collection of preliminary results on automorphism groups of algebraic curves that will be used in the following sections for the determination of the full automorphism group of the Wiman's sextic $\mathcal{W}$.

Theorem 2.4. ([19, Theorem 11.78]) *Let $\mathcal{C}$ be an irreducible algebraic curve of genus $g \geq 1$ defined over a field of characteristic p and let G be an automorphism group of $\mathcal{C}$. Let G_P be the stabilizer of a place P of $\mathcal{C}$ and $G_P^{(i)}$ be the i-th ramification group of G at P. Then*

$$|G_P| \leq \frac{4p}{p-1} g^2. \tag{9}$$

Also, if $\mathcal{C}_i$ denotes the quotient curve $\mathcal{C}/G_P^{(i)}$, then one of the following cases occurs:

(i) $\mathcal{C}_1$ is not rational, and $|G_P^{(1)}| \leq g$;

(ii) $\mathcal{C}_1$ is rational, $G_P^{(1)}$ has a short orbit other than $\{P\}$, and

$$|G_P^{(1)}| \leq \frac{p}{p-1} g;$$

(iii) $\mathcal{C}_1$ and $\mathcal{C}_2$ are rational, $\{P\}$ is the unique short orbit of $G_P^{(1)}$, and

$$|G_P^{(1)}| \leq \frac{4p}{(p-1)^2} g^2.$$

Theorem 2.5. ([19, Theorem 11.56]) *Let $\mathcal{C}$ be an irreducible curve of genus $g \geq 2$ over a field $\mathbb{K}$. If $char(\mathbb{K}) = 0$ or $char(\mathbb{K}) = p > 0$ with $(p, |Aut(\mathcal{C})|) = 1$ then*

$$|Aut(\mathcal{C})| \leq 84(g-1). \tag{10}$$

The previous result is known in the literature as *Classical Hurwitz bound*. The following theorem describes the short orbits structure of an automorphism group $G \leq Aut(\mathcal{C})$ of an algebraic curve $\mathcal{C}$ of genus $g \geq 2$ for which the Classical Hurwitz bound does not hold.

Theorem 2.6. ([19, Theorem 11.126 and Theorem 11.56]) *Let $\mathcal{C}$ be an irreducible curve of genus $g \geq 2$ and let $G \leq Aut(\mathcal{C})$ with $|G| > 84(g-1)$. Then the quotient curve $\mathcal{C}/G$ is rational and G has at most three short orbits as follows.*

1. *Exactly three short orbits, two tame and one non-tame. Each point in the tame short orbits has stabilizer in G of order 2;*
2. *exactly two short orbits, both non-tame;*
3. *only one short orbit which is non-tame;*
4. *exactly two short orbits, one tame and one non-tame. In this case $|G| < 8g^3$, with the following exceptions:*

- $p = 2$ *and* $\mathcal{C}$ *is isomorphic to the hyperelliptic curve* $y^2 + y = x^{2^k+1}$ *with genus* 2^{k-1} *;*
- $p > 2$ *and* $\mathcal{C}$ *is isomorphic to the Roquette curve* $y^2 = x^q - x$ *with genus* $(q-1)/2$ *;*
- $p \geq 2$ *and* $\mathcal{C}$ *is isomorphic to the Hermitian curve* $y^{q+1} = x^q + x$ *with genus* $(q^2-q)/2$ *;*
- $p = 2$ *and* $\mathcal{C}$ *is isomorphic to the Suzuki curve* $y^q + y = x^{q_0}(x^q + x)$ *with genus* $q_0(q-1)$ *.*

The following lemma considers the short orbits structure of a large tame automorphism group of a curve $\mathcal{C}$ of genus $g \geq 2$.

Lemma 2.7. *Let p be a prime. Let $\mathcal{C}$ be an irreducible algebraic curve of genus $g \geq 2$ defined over a field of characteristic p such that $40(g-1) < |Aut(\mathcal{C})| \leq 84(g-1)$. Assume also that $Aut(\mathcal{C})$ is tame.*

Then $\mathrm{Aut}(\mathcal{C})$ *has exactly* 3 *tame short orbits O_i for $i = 1, 2, 3$, $\mathcal{C}/\mathrm{Aut}(\mathcal{C})$ is rational, and one of the following cases occurs.*

1. $|O_1| = |\mathrm{Aut}(\mathcal{C})|/2$, $|O_2| = |\mathrm{Aut}(\mathcal{C})|/3$, $|O_3| = |\mathrm{Aut}(\mathcal{C})|/7$ *and* $p \geq 11$. *In this cases* $\mathrm{Aut}(\mathcal{C})$ *has order* $84(g-1)$*;*
2. $|O_1| = |\mathrm{Aut}(\mathcal{C})|/2$, $|O_2| = |\mathrm{Aut}(\mathcal{C})|/3$ *and* $|O_3| = |\mathrm{Aut}(\mathcal{C})|/8$. *In this cases* $|\mathrm{Aut}(\mathcal{C})| = 48(g-1)$.

Proof. From the Riemann-Hurwitz formula

$$2g - 2 = |\mathrm{Aut}(\mathcal{C})|(2g' - 2 + d'), \tag{11}$$

where $d'_P = d_p/|\mathrm{Aut}(\mathcal{C})_P|$ and $d' = \sum_P d'_P$. Here the summation is only over a set of representatives of places in $\mathcal{C}$, exactly one from each short orbit of $Aut(\mathcal{C})$.

So, it is necessary to investigate the possibilities for $|\mathrm{Aut}(\mathcal{C})|$ according to the number r of short orbits of $Aut(\mathcal{C})$ on $\mathcal{C}$. From the Hilbert different formula, see [19, Theorem 11.70], $d_P \geq e_P - 1$, with equality holding if and only if e_P is prime to p. Therefore, if $d_P > 0$, then $d'_P \geq 1/2$. More precisely, since $Aut(\mathcal{C})$ is tame, $d'_P = (e_P - 1)/e_P$. Hence, if $d > 0$, then $d' \geq 1/2$. If $g' \geq 2$ then $|Aut(\mathcal{C})| \leq g - 1$, a contradiction. For $g' = 1$, it follows that $d' > 0$ since $g \geq 2$, and hence $|Aut(\mathcal{C})| \leq 4(g-1)$, a contradiction. Thus $g' = 0$. Then

$$2g - 2 = |Aut(\mathcal{C})|(d' - 2).$$

In particular, $d' > 2$. Therefore G has some, say $r \geq 1$, short orbits on $\mathcal{C}$. Take representatives $Q_1, \ldots, Q_r$, from each short orbit, and let $d'_i = d'_{Q_i}$ for $i = 1, \ldots, r$. After a change of indices, it may be assumed that $d'_i \leq d'_j$ for $i \leq j$.

- When $r \geq 5$, then $d' \geq 5/2$, and hence $|Aut(\mathcal{C})| \leq 4(g-1)$.
- When $r = 4$ then $d' > 2$ and $d'_i > 1/2$ for at least one place P. As $d'_i > 1/2$ implies $d'_i \geq 2/3$, so $d' - 2 \geq 1/6$, whence $|Aut(\mathcal{C})| \leq 12(g-1)$.
- When $r = 3$ then again use $d' > 2$. If $d'_1 = 2/3$ then $d'_3 \geq 3/4$ and hence $|Aut(\mathcal{C})| \leq 24(g-1)$. If $d'_1 = 1/2$ and $d'_2 \geq 3/4$ then $|Aut(\mathcal{C})| \leq 40(g-1)$. Thus, assume that $d'_1 = 1/2$ and $d'_2 = 2/3$. From (11),

  $$2(g-1) = |Aut(\mathcal{C})|(d' - 2) = |Aut(\mathcal{C})|\left(\frac{1}{2} + \frac{2}{3} + d'_3 - 2\right) > 40(g-1)\left(\frac{1}{2} + \frac{2}{3} + d'_3 - 2\right),$$

  implying that $d'_3 < 53/60$. Also $d' = 1/2 + 2/3 + d'_3 - 2 > 0$ and hence $d'_3 > 5/6$, giving $d'_3 \geq 6/7$. Thus, we get that $6/7 \leq d'_3 < 53/60$, and hence either $d'_3 = 6/7$ or $d'_3 = 7/8$. Now one of the cases 1 and 2 occurs.

- When $r = 2$ then $d' = d'_1 + d'_2 > 2$. This can only occur when either d'_1 or d'_2 or both are greater than 1. Hence, one of cases 2 and 4 of Theorem 2.6 occurs. This is not possible as we are assuming that $Aut(\mathcal{C})$ is tame.
- When $r = 1$ then $d' = d'_1 > 2$, and case 3 of Theorem 2.6 occur. Again, this is not possible as we are assuming that $Aut(\mathcal{C})$ is tame.

□

A careful analysis of the automorphism group of algebraic curves $\mathcal{C}$ of even genus $g \geq 2$ can be found in [14]. The following result provides some restrictions to the structure of an automorphism group of $\mathcal{C}$ admitting a minimal normal subgroup of order 4. We recall that a *minimal normal subgroup* N of a group G is a normal subgroup of G such that the only normal subgroup of G properly contained in N is the trivial subgroup.

Lemma 2.8. ([14, Lemma 6.6]) *Let $\mathcal{C}$ be an irreducible curve of even genus $g \geq 2$ defined over a finite field of odd characteristic. If the automorphism group $Aut(\mathcal{C})$ of $\mathcal{C}$ has a minimal normal subgroup N of order 4, then either for $Aut(\mathcal{C})$, or for a normal subgroup of G of index 3, the following condition is satisfied:*

- *$G = O(G) \rtimes S_2$ where S_2 is the direct product of a cyclic group by a group of order 2.*

Let $\mathcal{C}$ be an algebraic curve of genus $g \geq 2$ defined over an algebraically closed field $\mathbb{K}$ of positive characteristic p. If $|Aut(\mathcal{C})|$ is divisible by p then bounds for the order of a Sylow p-subgroup of $Aut(\mathcal{C})$ can be found in [31].

In the following Theorem bounds for the order of a Sylow p-subgroup of $Aut(\mathcal{C})$ are written with respect to an important birational invariant of $\mathcal{C}$, namely its *p-rank* γ. It is defined to be the rank of the (elementary abelian) group of the p-torsion points in the Jacobian variety of $\mathcal{C}$; moreover, $\gamma \leq g$ and when the equality holds then $\mathcal{C}$ is called an *ordinary* (or *general*) curve; see [19, Section 6.7].

Theorem 2.9. ([31, Theorem 1 (i)]) *Let $\mathcal{C}$ be a curve of genus $g \geq 2$ and p-rank γ defined over an algebraically closed field of positive characteristic p. Let H be a Sylow p-subgroup of $Aut(\mathcal{C})$. If $\gamma \geq 2$ then*

$$|H| \leq c_p(\gamma - 1), \tag{12}$$

where $c_p = p/(p-2)$ for $p \geq 3$ and $c_2 = 4$.

Curves $\mathcal{C}$ together with a p-group H of automorphisms such that the bound (12) is attained are called *Nakajima extremal curves*. Giulietti and Korchmáros in [16] showed that the full automorphism group of Nakajima extremal curves has a precise structure.

Theorem 2.10. ([16, Theorem 1.3]) *Let $\mathcal{C}$ be a Nakajima extremal curve, and H be a Sylow p-subgroup of $Aut(\mathcal{C})$. Then either H is a normal subgroup of $Aut(\mathcal{C})$ and $Aut(\mathcal{C})$ is the semidirect product of H by a subgroup of a dihedral group of order $2(p-1)$, or $p = 3$ and, for some subgroup M of H of index 3, M is a normal subgroup of $Aut(\mathcal{C})$ and $Aut(\mathcal{C})/M$ is isomorphic to a subgroup of* $\mathrm{GL}(2,3)$.

3 The automorphism group of $\mathcal{W}$

Wiman proved that the automorphism group of $\mathcal{W}$ over the complex field $\mathbb{C}$ is the symmetric group S_5. In this section we show that this holds true also in positive characteristics p when $p \geq 7$. Let

$$F(X,Y,Z) = X^6 + Y^6 + Z^6 + (X^2 + Y^2 + Z^2)(X^4 + Y^4 + Z^4) - 12X^2Y^2Z^2$$

be the defining polynomial of $\mathcal{W}$. First of all, in the following remark, we justify the hypothesis on p.

Remark 3.1. *Let $\mathcal{W}$ be the Wiman's sextic defined as in Equation* (1) *over a field of characteristic p. Then the following holds.*

- *If $p = 2$ or $p = 3$ then the polynomial $F(X, Y, Z) \in \mathbb{F}_p[X, Y, Z]$ is reducible.*
- *If $p = 5$ then $\mathcal{W}$ is rational. In particular from* [19, Theorem 11.14]*, $Aut(\mathcal{W}) \cong \mathrm{PGL}(2, \mathbb{K})$, where $\mathbb{K}$ is the algebraic closure of $\mathbb{F}_p$.*

From now on we assume that $p \geq 7$.

First of all, we note that the following three rational maps are automorphisms of $\mathcal{W}$ of order 2:

$$\phi : [X : Y : Z] \mapsto [X : -Y : Z], \quad \tau : [X : Y : Z] \mapsto [-X : Y : Z], \quad \rho : [X : Y : Z] \mapsto [Y : X : Z]. \tag{13}$$

Likewise by direct checking, it is easily seen that the following map provides an automorphism of order 3 of $\mathcal{W}$:

$$\gamma : [X : Y : Z] \mapsto [-Z : -X : Y]. \tag{14}$$

A more complicated automorphism of order 5 of $\mathcal{W}$ is given by the following map:

$$\alpha : [X : Y : Z] \mapsto [g_0(X, Y, Z) : g_1(X, Y, Z) : g_2(X, Y, Z)], \tag{15}$$

where

$$\begin{aligned} g_0(X, Y, Z) &= -X^2 + XY + XZ - Y^2 - YZ + Z^2, \\ g_1(X, Y, Z) &= -X^2 + XY + XZ + Y^2 - YZ - Z^2, \\ g_2(X, Y, Z) &= X^2 + XY + XZ - Y^2 - YZ - Z^2. \end{aligned}$$

Indeed the following computation shows that α is an automorphism of $\mathcal{W}$,

$$\begin{gathered} \alpha(F(X, Y, Z)) = \alpha(X^6 + Y^6 + Z^6 + (X^2 + Y^2 + Z^2)(X^4 + Y^4 + Z^4) - 12X^2Y^2Z^2) = \\ g_0(X, Y, Z)^6 + g_1(X, Y, Z)^6 + g_2(X, Y, Z)^6 + \\ +(g_0(X, Y, Z)^2 + g_1(X, Y, Z)^2 + g_2(X, Y, Z)^2)(g_0(X, Y, Z)^4 + g_1(X, Y, Z)^4 + g_2(X, Y, Z)^4) + \\ -12g_0(X, Y, Z)^2 g_1(X, Y, Z)^2 g_2(X, Y, Z)^2 = \\ 2^6(Y+Z)^2(X-Z)^2(X-Y)^2(2X^6+X^4Y^2+X^4Z^2+X^2Y^4-12X^2Y^2Z^2+X^2Z^4+2Y^6+Y^4Z^2+Y^2Z^4+2Z^6) \\ = 2^6(Y + Z)^2(X - Z)^2(X - Y)^2 F(X, Y, Z) = 0. \end{gathered}$$

Also, one can show by direct computation that

$$\alpha^5 : [X : Y : Z] \mapsto [\overline{X} : \overline{Y} : \overline{Z}]$$

with

$$\begin{aligned} \overline{X} &= (Y - Z)^2(Y + Z)^9 X(X - Z)^{10}(X + Z)^5(X - Y)^4(X + Y), \\ \overline{Y} &= (Y - Z)^2(Y + Z)^9 Y(X - Z)^{10}(X + Z)^5(X - Y)^4(X + Y), \\ \overline{Z} &= (Y - Z)^2(Y + Z)^9 Z(X - Z)^{10}(X + Z)^5(X - Y)^4(X + Y), \end{aligned}$$

implying $\alpha^5 = 1$. In this way, considering the group generated by the automorphisms defined up to now, we have that $120||Aut(\mathcal{W})|$.

The following lemma ensures that $Aut(\mathcal{W})$ is tame and hence from Theorem 2.5 that the Classical Hurwitz bound $|Aut(\mathcal{W})| \leq 84(g(\mathcal{W}) - 1)$ is satisfied.

Lemma 3.2. *Let $\mathcal{W}$ be the Wiman's sextic defined as in Equation* (1) *over a field of characteristic $p \geq 7$. Then $Aut(\mathcal{W})$ is tame. In particular $|Aut(\mathcal{W})| \leq 84(g(\mathcal{W})-1) = 420$. Since also $120 \mid |Aut(\mathcal{W})|$ then $|Aut(\mathcal{W})| \in \{120, 240, 360\}$*

Proof. Since 120 divides $Aut(\mathcal{W})$, proving that $Aut(\mathcal{W})$ is tame also the second part of the claim follows from Theorem 2.5.

- Assume that $p \geq 13$. If $Aut(\mathcal{W}) > 84(g-1)$, then from Theorem 2.6, $Aut(\mathcal{W})$ contains an auotomorphism σ of order a multiple of p and such that $\langle\sigma\rangle$ fixes some place P of $\mathcal{W}$. This contradicts Theorem 2.4 as
$$\frac{(p-1)^2}{4} \geq 36 = g^2.$$
- Assume that $p = 11$. Then by direct checking with MAGMA, $\mathcal{W}$ is an ordinary curve of genus $g = \gamma = 6$. Suppose by contradiction that $Aut(\mathcal{W})$ is nontame and let H be a Sylow 11-subgroup of $Aut(\mathcal{W})$. From Theorem 2.9,
$$11 \leq |H| \leq \frac{11}{9}(6-1) < 7,$$
a contradiction.
- Hence we can assume that $p = 7$. By direct checking with MAGMA, $\mathcal{W}$ is an ordinary curve of genus $g = \gamma = 6$. Assuming again by contradiction that a Sylow 7-subgroup H of $Aut(\mathcal{W})$ is non-trivial, from Theorem 2.9 we have that
$$7 \leq |H| \leq \frac{7}{5}(6-1) = 7.$$
Thus, $|H| = 7$ and $\mathcal{W}$ is a Nakajima extremal curve. From Theorem 2.10, $|Aut(\mathcal{W})|$ divides $2p(p-1) = 84$. Since 120 divides $|Aut(\mathcal{W})|$ we have a contradiction.

□

Consider the subgroup G of $Aut(\mathcal{W})$ generated by the three involutions ϕ, τ and ρ as defined in Equation 13. In the following lemma the structure of G is described. This forces $Aut(\mathcal{W})$ to contain a dihedral subgroup of order 8. This combined with Lemma 3.2 gives interesting constrains to the structure of $Aut(\mathcal{W})$.

Lemma 3.3. *The subgroup G of $Aut(\mathcal{W})$ with $G = \langle\tau, \phi, \rho\rangle$ is isomorphic to the dihedral group D_8 of order 8.*

Proof. Since τ and ϕ commute, the group $H = \langle\tau, \phi\rangle$ is elementary abelian of order 4. Also, ρ normalizes H as $\rho\phi\rho = \tau$. This shows that $|G| = 8$, G is not abelian and since G contains at least four distincts involution (ϕ, τ, ρ and $\phi \circ \tau$) it is necessarily isomorphic to the dihedral group D_8 of order 8. □

From Lemma 3.2, if $p \geq 7$ there are just three possibilities for $|Aut(\mathcal{W})|$. In the following a case-by-case analysis is considered to obtain the main result of this section.

- **Case 1:** $|Aut(\mathcal{W})| \in \{240, 360\}$. Our aim is to prove that this case cannot occur. From Lemma 2.7, since $200 = 40(g-1) < |\mathrm{Aut}(\mathcal{W})| < 84(g-1)$, we have that $Aut(\mathcal{W}) = 48(g-1) = 240$, hence the case $|\mathrm{Aut}(\mathcal{W})| = 360$ cannot occur. Also, if $|\mathrm{Aut}(\mathcal{W})| = 240$, Lemma 2.7 implies that $Aut(\mathcal{W})$ has a short orbit O_3 of length $|Aut(\mathcal{W}_1)|/8 = 30$.

  In particular, for $P \in O_3$, the stabilizer $Aut(\mathcal{W})_P$ has order 8. From [19, Lemma 11.44] $Aut(\mathcal{W})_P$ is a cyclic group of order 8. A Sylow 2-subgroup of $Aut(\mathcal{W})$ has order 16, contains a cyclic group

of order 8 and also a dihedral group of order 8. By direct checking with MAGMA there are just 2 groups of order 16 containing both a cyclic group of order 8 and a dihedral group of order 8, namely $G \cong SmallGroup(16, i)$ with $i = 7, 8$. Again by direct checking with MAGMA, there are no groups of order 240 whose Sylow 2-subgroup is isomorphic to $SmallGroup(16, i)$ with $i = 7, 8$, and hence this case can be excluded. This proves that $|Aut(\mathcal{W})| = 120$.

- **Case 2:** $|Aut(\mathcal{W})| = 120$. From [19, Theorem 11.79] an abelian subgroup of $Aut(\mathcal{W})$ has order at most equal to $4g + 4 = 28$. Using this information, one can check with MAGMA that the only groups of order 120 with a structure which is compatible with the above condition are $SmallGroup(120, 34)$, $SmallGroup(120, 37)$ and $SmallGroup(120, 38)$. The cases $Aut(\mathcal{W}) \cong SmallGroup(120, 37)$ and $Aut(\mathcal{W}) \cong SmallGroup(120, 37)$ are incompatible with Lemma 2.8 as they both have a minimal normal subgroup of order 4 but a Sylow 2-subgroup of $Aut(\mathcal{W})$ is isomorphic to the dihedral group D_8 which is not a direct product of a cyclic group and a group of order 2. Finally we note that $SmallGroup(120, 34)$ is isomorphic to the symmetric group S_5.

The main result of this section is now proved combining the above lemmas with Remark 3.1. It provides a positive characteristic analogue of a result of Wiman [36] dealing with the structure of $Aut(\mathcal{W})$ over $\mathbb{C}$.

Theorem 3.4. *Let $\mathcal{W}$ denote the Wiman's sextic defined as in Equation* (1) *over an algebraically closed field $\mathbb{K}$ of characteristic p. If $\mathbb{K} = \mathbb{C}$ or $p \geq 7$ then $Aut(\mathcal{W})$ is isomorphic to the symmetric group S_5. If $p = 5$ then $\mathcal{W}$ is rational and $Aut(\mathcal{W}) \cong \mathrm{PGL}(2, \mathbb{K})$. If $p = 2$ or $p = 3$ then the homogeneous polynomial defining $\mathcal{W}$ as in* (1) *is not irreducible.*

4 The $\mathbb{F}_{19^2}$-maximal Wiman Sextic $\mathcal{W}$ is not Galois covered by the Hermitian curve $\mathcal{H}_{19}$ over $\mathbb{F}_{19^2}$

In this section we show that the $\mathbb{F}_{19^2}$-maximal Wiman's sextic $\mathcal{W}$ is not Galois covered by the Hermitian curve $\mathcal{H}_{19}$ over $\mathbb{F}_{19^2}$.

The proof relies on the results of [29] and the main tools are the classification of automorphisms of the Hermitian curve based on their orders and geometrical properties, as stated in Lemma 2.2 and Theorem 2.3, as well as the Riemann-Huwritz and Hilbert's formulas (7) and (8).

Assume by contradiction that $\mathcal{W}$ is Galois covered by $\mathcal{H}_{19}$ over $\mathbb{F}_{19^2}$ and let $G \leq \mathrm{PGU}(3, 19)$ denote the corresponding Galois group. Then

$$\frac{|\mathcal{H}_{19}|}{|\mathcal{W}(\mathbb{F}_{19^2})|} \leq |G| \leq \frac{2g(\mathcal{H}_{19}) - 2}{2g(\mathcal{W}) - 2}, \tag{16}$$

see the proof of Theorem 5 in [15]. Hence

$$11 < \frac{19^3 + 1}{590} \leq |G| \leq \frac{2g(\mathcal{H}_{19}) - 2}{10} = 34.$$

Moreover, since $G < \mathrm{PGU}(3, 19)$, we have that $|G| \in \{12, \ldots, 34\}$ divides $|\mathrm{PGU}(3, 19)|$. This implies that

$$|G| \in \{12, 14, 15, 16, 18, 19, 20, 21, 24, 25, 28, 30, 32\}. \tag{17}$$

At this point a contradiction to $\mathcal{W}$ being Galois covered by $\mathcal{H}_{19}$ over $\mathbb{F}_{19^2}$, is obtained with a case-by-case analysis with respect to $|G|$ as in (17).

- **Case** $|G| = 12$. By Sylow's Theorems G contains at least two elements of order 3. Then by Theorem 2.3, $\Delta = i \cdot 2 + k \cdot 20$ with $i \geq 2$ and $k \leq 9$. This contradicts (7).

- **Case** $|G| = 14$. G is either isomorphic to C_{14} or to D_{14}. Since by Lemma 2.2 and Theorem 2.3, G cannot contain elements of order 14, we have that $G \cong D_{14}$. Then by Theorem 2.3, $\Delta = 7 \cdot 20 + 6 \cdot 3 = 158$, contradicting (7).

- **Case** $|G| = 15$. By Sylow's Theorems G is isomorphic to C_{15}. By Theorem 2.3, $\Delta = 2 \cdot 2 + 4 \cdot i + 8 \cdot 2$, with $i = 0, 20$ as a generator of the Sylow 5-subgroup of G is either of type (B1) or of type (A) in Lemma 2.2. The Riemann-Hurwitz formula (7) implies that $\Delta = 190$, a contradiction.

- **Case** $|G| = 18$. From Theorem 2.3 and Equation (7), $\Delta = 20 \cdot i + 2 \cdot (17 - i) = 160$, where i is the number of involutions of G. So $i = 7$. By Sylow's Theorems a group of order 18 cannot contain exactly 7 involutions, a contradiction.

- **Case** $|G| = 19$. Up to isomorphism G is C_{19}. Since a power of an elation is an elation, by Theorem 2.3 we obtain that $\Delta = 18i$ with $i = 21$ or $i = 2$. This contradict Equation (7).

- **Case** $|G| = 21$. By Sylow's Theorems and Schur-Zassenhaus Theorem [26, Corollary 7.5], G is isomorphic either to C_{21} or to the semidirect product $C_7 \rtimes C_3$. The former case is not possible because it contradicts Theorem 2.3; the latter, again using Theorem 2.3, contradicts Equation (7).

- **Case** $|G| = 25$. G is isomorphic either to C_{25} or to $C_5 \times C_5$. The former case contradicts Theorem 2.3. In the latter case, since every non-trivial element in G has order 5, G contains only elements either of type (A) or of type (B1) from Lemma 2.2. Since powers of a homology are homologies themselves, Δ must be divisible by 4, contradicting Equation (7).

- **Case** $|G| = 28$. Since G cannot contain elements of order 14 from Theorem 2.3 and G has exactly one Sylow 7-subgroup, we have that $\Delta = i \cdot 20 + 6 \cdot 3$ for some non-negative integer i. This contradicts Equation (7).

- **Case** $|G| = 30$. Since there are at least two elements of type (B3) in G and $\Delta = 40$ from Equation (7), we conclude that G has a unique Sylow 2-subgroup. This implies that $G \simeq C_{30}$ and, by Theorem 2.3, $\Delta = 1 \cdot 20 + 2 \cdot 3 + 4 \cdot i + 2 \cdot 2 + 4 \cdot k + 8 \cdot 2 + 8 \cdot 2 \geq 62$ where i is either equal to 20 or to 0 as the elements of order 5 are either homologies or of type (B1), while k is either equal to 20 or to 0 as the elements of order 10 in $\mathrm{PGU}(3, 19)$ are either homologies or of type (B1) from Lemma 2.2. Combining the above arguments on Δ we deduce that this case cannot occur.

At this point, to conclude the proof of the main result of this section, we need to examine the following cases: $|G| \in \{16, 20, 24, 32\}$. The arithmetical arguments used for the previous cases are not sufficient, and hence normalizers of subgroups of $\mathrm{PGU}(3, 19)$ need to be considered.

Assume that $\mathcal{W} \cong \mathcal{H}_{19}/G$, and let N be the normalizer N of G in $\mathrm{PGU}(3, 19)$ and Q be the factor group N/G. From Galois theory Q is a subgroup of $Aut(\mathcal{W}) \cong \mathrm{S}_5$. Since subgroups of the symmetric group S_5 can be completely listed, a contradiction can be obtained proving that the structure of Q is not compatible with the subgroup structure of S_5.

- **Case** $|G| = 16$. We can use MAGMA to obtain the complete list, up to conjugation, of subgroups of $\mathrm{PGU}(3, 19)$ of order 16. Defining in MAGMA $S := SubgroupLattice(\mathrm{PGU}(3, 19) : Properties := true)$; we get that the subgroups G of $\mathrm{PGU}(3, q)$ of order 16 are: $G = SubgroupLattice(\mathrm{PGU}(3, 19))[i]$

with $i \in \{70, 71, 72\}$. Considering the normalizer N of G in $\mathrm{PGU}(3, 19)$ we get that $|Q| \in \{150, 30, 10\}$. Since S_5 has neither subgroups of order 150 nor of order 30, we get that the unique admissible case is $|Q| = 10$. In this case Q is cyclic but in S_5 each subgroup of order 10 is dhiedral. We deduce that this case cannot occur.

- **Case** $|G| = 20$. As before, using MAGMA, we obtain the complete list of subgroups of order 20 of $\mathrm{PGU}(3, 19)$, namely $G = S[i]$ with $i \in \{40, \ldots, 51\}$. In these cases, $|Q| \in \{6840, 40, 20\}$. Clearly S_5 has no subgroups of orders 6840 or 40. Hence $|Q| = 20$. In this case Q abelian. Since S_5 has no abelian subgroups of order 20 we have a contradiction.

- **Case** $|G| = 24$. Using MAGMA, we obtain the complete list of subgroups of order 24 in $\mathrm{PGU}(3, 19)$: $G = S[i]$ with $i \in \{73, \ldots, 77\}$. In these cases, $|Q| \in \{30, 20, 10\}$. We note that S_5 contains no subgroups of orders 30 while if $|Q| = 20$ or $|Q| = 10$ then Q is cyclic. Since S_5 has no cyclic subgroups of order 20 or 10 we have a contradiction.

- **Case** $|G| = 32$. Arguing as before, we get that G is isomorphic to $S[118]$. A contradiction is obtained combining Equation (7) with the fact that G contains seven involutions.

The main result of this section is now proved.

Theorem 4.1. *The $\mathbb{F}_{19}$-maximal Wiman's sextic $\mathcal{W}$ is not Galois covered by the Hermitian curve $\mathcal{H}_{19}$ over $\mathbb{F}_{19^2}$.*

Acknowledgments

The authors would like to thank the Italian Ministry MIUR, Strutture Geometriche, Combinatoria e loro Applicazioni, Prin 2012 prot. 2012XZE22K and GNSAGA of the Italian INDAM.

This resarch was carried out within the project "Progetto *Geometrie di Galois, Curve Algebriche su campi finiti e loro Applicazioni*", supported by Fondo Ricerca di Base, 2015, of Università degli Studi di Perugia.

References

[1] P. Beelen and M. Montanucci: A new family of maximal curves, preprint, arXiv:1711.02894.

[2] A. Cossidente, G. Korchmáros and F. Torres: *On curves covered by the Hermitian curve*, J. Algebra **216**, Issue 1, 56–76 (1999).

[3] A. Cossidente, G. Korchmáros and F. Torres: *Curves of large genus covered by the Hermitian curve*, Comm. Algebra **28**, 4707–4728 (2000).

[4] P. Deligne and G. Lusztig: *Representations of reductive groups over finite fields*, Ann. of Math. **103**, 103–161 (1976).

[5] I. Duursma and K.H. Mak: *On maximal curves which are not Galois subcovers of the Hermitian curve*, Bull. Braz. Math. Soc. (N.S.) **43** (3), 453–465 (2012).

[6] R. Fuhrmann, R. and F. Torres: *On Weierstrass points and optimal curves*, Rend. Circ. Mat. Palermo Suppl. **51** (Recent Progress in Geometry, Ballico E, Korchmáros G, (Eds.)), 25–46 (1998).

[7] A. Garcia: *Curves over finite fields attaining the Hasse-Weil upper bound*, In: European Congress of Mathematics, vol. II (Barcellona 2000), Progr. Math. **202**, Birkhäuser, Basel, 199–205 (2001).

[8] A. Garcia: *On curves with many rational points over finite fields*,In: Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, Springer, Berlin, 152–163 (2002).

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

[10] A. Garcia and H. Stichtenoth.: *Algebraic function fields over finite fields with many rational places*, IEEE Trans. Inform. Theory **41**, 1548–1563 (1995).

[11] A. Garcia and H. Stichtenoth: *A maximal curve which is not a Galois subcover of the Hermitian curve*, Bull. Braz. Math. Soc. (N.S.) **37**, 139–152 (2006).

[12] A. Garcia, H. Stichtenoth and C.P. Xing: *On subfields of the Hermitian function field*, Compositio Math. **120**, 137-170 (2000).

[13] M. Giulietti, J.W.P. Hirschfeld, G. Korchmáros and F. Torres: *A family of curves covered by the Hermitian curve*, Sémin. Congr. **21**, 63–78 (2010).

[14] M. Giulietti and G. Korchmáros: *Algebraic curves with many automorphisms*, preprint, arXiv:1702.08812v1.

[15] M. Giulietti, G. Korchmáros: *A new family of maximal curves over a finite field*, Math. Ann. **343**, (2009) 229-245.

[16] M. Giulietti and G. Korchmáros: *Large p-groups of automorphisms of algebraic curves in characteristic p*, J. Algebra **481**, 215-249 (2017).

[17] M. Giulietti, M. Montanucci and G. Zini: *On maximal curves that are not quotients of the Hermitian curve*, Finite Fields Appl. **41**, 72-88 (2016).

[18] R.W. Hartley: *Determination of the ternary collineation groups whose coefficients lie in the* $GF(2^n)$, Ann. of Math. Second Series **27**, Issue 2, 140–158 (1925).

[19] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves over a Finite Field, Princeton Series in Applied Mathematics*, Princeton, (2008).

[20] A.R. Hoffer: *On unitary collineation groups*, J. Algebra **22**, 211–218 (1972).

[21] D.R. Hughes and F.C. Piper: *Projective Planes*. Graduate Text in Mathematics **6**, Springer, Berlin, xii+793 pp. (1973).

[22] E. Kani and M. Rosen: *Idempotent relations and factors of Jacobians*, Math. Ann. **284**, 307-327 (1989).

[23] M.Q. Kawakita: *Wimans and Edges sextics attaining Serres bound*, European Journal of Mathematics, (2017).

[24] S.L. Kleiman: *Algebraic cycles and the Weil conjectures*, in: Dix exposés sur la cohomologie des schémas, in: Adv. Stud. Pure Math. **3**, 359-386 (1968).

[25] G. Lachaud: *Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C.R. Acad. Sci. Paris **305**, Série I, 729–732 (1987).

[26] A. Machì: *Groups, An introduction to ideas and methods of the theory of groups*, Unitext **58**, Springer, Milan, xiv+371 pp. (2012).

[27] K.H. Mak: *On Congruence Function Fields with many rational places*, PhD Thesis, www.ideals.illinois.edu/bitstream/handle/2142/34193/Mak_KitHo.pdf?sequence=1.

[28] H.H. Mitchell: *Determination of the ordinary and modular ternary linear groups*, Trans. Amer. Math. Soc. **12**, Issue 2, 207-242 (1911).

[29] M. Montanucci and G. Zini, *On the spectrum of genera of Galois subcovers of the Hermitian curve*, preprint, arXiv: 1703.10592.

[30] M. Montanucci and G. Zini: *Some Ree and Suzuki curves are not Galois covered by the Hermitian curve*, Finite Fields Appl. **48**, 175–195 (2017).

[31] S. Nakajima: *p-ranks and automorphism groups of algebraic curves*, Trans. Amer. Math. Soc. **303**, 595-607 (1987).

[32] H. Stichtenoth: *Algebraic function fields and codes*, Springer, (2009).

[33] R.C. Valentini and M.L. Madan: *A Hauptsatz of L.E. Dickson and Artin–Schreier extensions*, J. Reine Angew. Math. **318**, 156–177 (1980).

[34] G. van der Geer: *Curves over finite fields and codes*, In: *European Congress of Mathematics*, vol. II (Barcellona 2000), Progr. Math. **202**, Birkhäuser, Basel, 225–238 (2001).

[35] G. van der Geer: *Coding theory and algebraic curves over finite fields: a survey and questions*, In: Applications of Algebraic Geometry to Coding Theory, Physics and Computation, NATO Sci. Ser. II Math. Phys. Chem. **36**, Kluwer, Dordrecht, 139–159 (2001).

[36] A. Wiman: *Ueber eine einfuche Gruppe von 360 ebenen Collineationen*. Math. Ann., **47**, (1896).

Massimo Giulietti

Universitá degli Studi di Perugia,
Dipartimento di Matematica e Informatica,
Via Vanvitelli 1,
06123 Perugia,
Italy,
massimo.giulietti@unipg.it

Motoko Kawakita

Shiga University of Medical Science,
Seta Tsukinowa-cho
Otsu city, Shiga 520-2192

Japan,
kawakita@belle.shiga-med.ac.jp

Stefano Lia
stefano.lia.7@gmail.com

Maria Montanucci
Universitá degli Studi della Basilicata,
Dipartimento di Matematica, Informatica ed Economia,
Campus di Macchia Romana,
Viale dell' Ateneo Lucano 10,
85100 Potenza,
Italy,
maria.montanucci@unibas.it