COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 72, No. 1 2024

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171–8501 JAPAN

Computational Search for Superelliptic Curves Attaining the Gonality-Point Bound, with Extra Genus-5 Examples

by

Momonari KUDO* and Shushi HARASHITA†

(Received August 11, 2023)
(Revised November 14, 2023)

Abstract. For natural numbers g, N, r and for a power q of a prime, it is a basic problem to determine the maximum number of $\mathbb{F}_{q^r}$-rational points on a genus-g curve over $\mathbb{F}_q$ of gonality N. The upper-bound $N(q^r+1)$ is known as the gonality-point bound, which may be less than the Hasse-Weil upper-bound for small q^r. In this paper, we discuss the existence and the enumeration of curves of the following types attaining the gonality-point bound: We firstly study the superelliptic case, and secondly deal with the case of genus-5 curves over small finite fields, which complements our previous result [15] on the non-hyperelliptic and non-trigonal case.

1. Introduction

Throughout this paper, we use curve to mean a non-singular projective variety of dimension one. Let p be a rational prime, q a power of p, and r a natural number. Let $\mathbb{F}_q$ denote the finite field of q elements. For a curve C of genus g over $\mathbb{F}_q$, we denote by $|C(\mathbb{F}_{q^r})|$ the number of its $\mathbb{F}_{q^r}$-rational points. Finding a curve C over $\mathbb{F}_q$ with $|C(\mathbb{F}_{q^r})|$ as large as possible (relative to g) is an interesting problem in itself, and also such a curve is useful in applications such as coding theory (e.g., [10]). The most well-known (upper-)bound on $|C(\mathbb{F}_{q^r})|$ is the Hasse-Weil bound:

$$|C(\mathbb{F}_{q^r})| \leq q^r + 1 + 2g\sqrt{q^r}\,. \tag{1.1}$$

For further improvements of (1.1) when g is larger with respect to q, see e.g., [11], [18] and [16].

Here is another kind of bound in the case where there exists a morphism defined over $\mathbb{F}_{q^r}$ from C to the projective line $\mathbb{P}^1$ of degree N: Since every $\mathbb{F}_{q^r}$-rational point of C maps to an $\mathbb{F}_{q^r}$-rational point of $\mathbb{P}^1$, we have

$$|C(\mathbb{F}_{q^r})| \leq N(q^r+1)\,. \tag{1.2}$$

*Faculty of Information Engineering, Fukuoka Institute of Technology.
†Graduate School of Environment and Information Sciences, Yokohama National University.

Key words— Algebraic curves, Rational points, Superelliptic curves, Curves of genus five, Trigonal curves.
2010 Mathematical Subject Classification: 14G05, 14G15, 14H50, 14Q05, 68W30

This upper-bound is called *the gonality-point bound* (cf. [4]). Of course, this bound is not optimal in many cases: Actually when we fix g and N, this bound exceeds the Hasse-Weil bound if

$$q^{r/2} > \frac{g + \sqrt{g^2 - (N-1)^2}}{N-1} \tag{1.3}$$

for $g \geq N-1$. Van der Geer asked in [6]: What is the maximum number of rational points on a curve of genus g and gonality N defined over $\mathbb{F}_q$? See Faber and Grantham [3] and [4] for recent results on this question for small q and g. In [19], Vermeulen showed that a curve attaining the gonality-point bound exists for sufficient large g, which answers a conjecture proposed in [4].

In this paper, we study the existence/enumeration of curves attaining the gonality-point bound for two types of curves: Superelliptic curves (including the hyperelliptic case) and genus-5 curves. The case of genus-5 non-hyperellitic and non-trigonal curves has been studied in [15]. Following Serre's paper [18], we denote by $N_q(g)$ the maximal number of $\mathbb{F}_q$-rational points on a curve C of genus g over $\mathbb{F}_q$, namely,

$$N_q(g) = \max\{\, |C(\mathbb{F}_q)| : C \text{ is a curve of genus } g \text{ over } \mathbb{F}_q \,\},$$

and then (1.1) implies $N_q(g) \leq q+1+2g\sqrt{q}$. According to [8], the "smallest" case among the unknown cases at this point is $(q,\, g) = (9,\, 5)$. The maximal number of the $\mathbb{F}_9$-rational points of the known $\mathbb{F}_9$-rational points on curves of genus 5 over $\mathbb{F}_9$ is 32. However, the theoretical upper-bound of $N_9(5)$ is 35 [16], i.e, so far we know $32 \leq N_9(5) \leq 35$. So far as is known, there are four concrete examples attaining $|C(\mathbb{F}_9)| = 32$: The first example was found by van der Geer - van der Vlugt [7], and other two examples were known, one was found by Fischer (cf. [8]) and the other was found by Ramos-Ramos in [17]. In [15], Kudo and Harashita found a new example with enumeration of generic curves C over $\mathbb{F}_3$ of genus 5 such that $|C(\mathbb{F}_9)| = 32$, where "generic curve" means a non-hyperelliptic and non-trigonal curve of genus 5 with a sextic model in $\mathbb{P}^2$ with mild singularities, see [15] for the precise definition. They also proved that there is no generic curve over $\mathbb{F}_3$ with $|C(\mathbb{F}_9)| > 32$. This paper investigates remaining cases, i.e., the hyperelliptic and trigonal cases, but in these cases the gonality-point bound is 20 (resp. 30), which is less than 32. Hence we set the aim to showing the existence of these curves attaining the gonality-point bound, and to enumerating such curves.

This paper has the following two aims:

- **(A)** Giving algorithms to find/enumerate superelliptic curves attaining the gonality-point bound;
- **(B)** Enumerating trigonal genus-5 curves over a small field attaining the gonality-point bound.

We explain the detail of each part.

(A) We give algorithms to find/enumerate superelliptic curves attaining the gonality-point bound for given g, q, r, and N, see Section 3. Applying the algorithms to the hyperelliptic cases with $(g, q, r) = (5, 3, 2)$, we obtain:

THEOREM 1.1 (Theorem 4.1.2 and Corollary 4.1.3). *There exists a genus-five hyperelliptic curve C over $\mathbb{F}_3$ attaining the gonality-point equality $|C(\mathbb{F}_9)| = 20$ (see (4.7) given*

in Example 4.2.2 for an explicit example), and hence the maximal number of $\mathbb{F}_9$-rational points of genus-five hyperelliptic curves over $\mathbb{F}_3$ is 20. Moreover, there are exactly 573 $\mathbb{F}_9$-isomorphism classes of such curves C, and there are exactly 419 $\mathbb{F}_9$-isogeny classes of Jacobian varieties among them.

See Section 4, for further many examples on the enumeration of superelliptic curves attaining the gonality-point bound. We observe from our computational results summarized in Table 2 and Fig. 1 that the number of superelliptic curves of a fixed genus $y^N = f(x)$ with $\deg(f) = d$ over $\mathbb{F}_q$ attaining the gonality-point bound is maximal when q^r is near from d. It would be interesting to know more precise reason of this phenomenon.

(B) We execute another algorithm for trigonal (possibly non-superelliptic) curves, for $(g, q, r) = (5, 3, 2)$ with $N = 3$, we enumerate trignal curves attaining the gonality-point bound. We also determine the Weil polynomials of the enumerated curves:

THEOREM 1.2 (Theorem 5.2.2 and Corollary 5.2.3). *There exists a genus-five trigonal curve C over $\mathbb{F}_3$ attaining the gonality-point equality $|C(\mathbb{F}_9)| = 30$ (see the proof given in Subsection 5.2 for explicit examples), and hence the maximal number of $\mathbb{F}_9$-rational points of genus-five trigonal curves over $\mathbb{F}_3$ is 30. Moreover, there are exactly eight $\mathbb{F}_9$-isomorphism classes of such curves C, and there are also exactly eight $\mathbb{F}_9$-isogeny classes of Jacobian varieties among them.*

The organization of this paper is as follows. Section 2 collects some results on counting rational points on superelliptic curves and on genus-5 curves with the classification of curves of genus 5. In Section 3, we give algorithms to find/enumerate superelliptic curves attaining the gonality-point bound. The enumeration results obtained by executing algorithms are found in Section 4. In Section 5, we give a reduction of quintic models of trigonal curves (in characteristic 3) and obtain the enumeration result of such curves attaining the gonality-point bound. Section 6 is devoted to conclusion and future works.

Acknowledgments

The authors thank the reviewers for their helpful comments and suggestions. This work was supported by JSPS Grant-in-Aid for Young Scientists 20K14301 and 23K12949, and JSPS Grant-in-Aid for Scientific Research (C) 21K03159.

2. Superelliptic curves and curves of genus 5

In this section, we recall some facts on superelliptic curves and on curves of genus 5 with the classification of curves of genus 5, and study some constraints so that they attain the gonality-point bound.

2.1. Superelliptic curves

Let q be a power of a prime p. Let N be an integer ≥ 2 with $(N, p) = 1$. A cyclic covering $C \to \mathbb{P}^1$ of degree N over $\mathbb{F}_q$ with nonsingular projective curve C over $\mathbb{F}_q$ is realized as the desingularization of the projective closure of

$$y^N = f(x) := a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0\,, \tag{2.1}$$

for some $f(x) \in \mathbb{F}_q[x]$. The cyclic covering $C \to \mathbb{P}^1$ (or simply C) is called *a superelliptic curve* over $\mathbb{F}_q$ if $f(x)$ is a separable polynomial. It is known that the genus of C is

$$g(C) = 1 + \frac{1}{2}\left((d-1)N - d - \left(N, d\right)\right).$$

The necessary and sufficient condition for $|C(\mathbb{F}_{q^r})|$ attaining the gonality-point bound $N(q^r+1)$ is that the morphism $C \to \mathbb{P}^1$ obtained by forgetting y is totally decomposed over every $\mathbb{F}_{q^r}$-rational point on $\mathbb{P}^1$, especially as the infinite point is a rational point, $N|d$ and $a_d \in (\mathbb{F}_{q^r}^\times)^N$ are required. The condition $N|d$ implies

$$g(C) = \frac{(d-2)(N-1)}{2}. \tag{2.2}$$

The condition that $a_d \in (\mathbb{F}_{q^r}^\times)^N$, say $a_d = u^N$ with $u \in \mathbb{F}_{q^r}^\times$, allows us to assume $a_d = 1$ by replacing y by uy.

In Section 4, we shall discuss about the number of C's of the form (2.1) with $|C(\mathbb{F}_{q^r})|$ attaining the gonality-point bound with respect to the relative position of d and q^r. Here we give a simple bound of q^r in d.

LEMMA 2.1.1. *If there exists a superelliptic curve C of the form (2.1) with $d \geq 4$ so that $|C(\mathbb{F}_{q^r})|$ attains the gonality-point bound, then we have*

$$q^r + 1 \leq \frac{(d-2)^2 + (d-2)\sqrt{d^2-4d}}{2}. \tag{2.3}$$

Proof. If such a C exists, then the gonality-point bound is less than or equal to the Hasse-Weil bound:

$$N(q^r+1) \leq q^r + 1 + 2g(C)\sqrt{q^r}.$$

The lemma follows from a straightforward computation with (2.2). □

For example, the integer part of the right-hand side of (2.3) is 2, 7, 14, 23, 34, 47, 62, 79, 98 for $d = 4, 5, 6, 7, 8, 9, 10, 11, 12$ respectively. In particular, there is no (q, r) satisfying (2.3) for $d = 4$. See the table below for the totality of the pairs (N, d) for genus ≤ 5 satisfying (2.2), $N|d$ and that the right-hand side of (2.3) is greater than 2.

g	(N, d)
2	(2,6)
3	(2,8)
4	(2,10), (3,6)
5	(2,12)

Table 1. Possible (N, d) for the existence of C of genus ≤ 5 attaining gonality-point bound

2.2. Curves of genus 5

Let C be a curve of genus 5 over a field K. Over the algebraic closure $\overline{K}$ of K, the gonality of C is either of 2, 3 and 4, see [9, Chap. IV, Example 5.5.3 and Ex. 5.5]. The first case and the second are called *hyperelliptic* and *trigonal* respectively.

Assume that K is a finite field. If C is hyperelliptic (resp. trigonal), then C has a morphism $C \to \mathbb{P}^1$ defined over K of degree 2 (resp. 3), by the uniqueness of g^1_2 (resp. g^1_3), see [9, Chap. IV, Prop. 5.3] and [14, 2.1].

A hyperelliptic curve of genus g over K of characteristic $\neq 2$ is realized as the desingularization of the projective closure of

$$y^2 = f(x)$$

for an $f(x) \in K[x]$ of degree $2g+2$. Note that even if $\deg f = 2g+1$, we have a hyperelliptic curve of genus g, but such a curve has an extra condition: a branched point of the hyperelliptic fibration $C \to \mathbb{P}^1$ is a K-rational point. In Subsection 4.1, we shall enumerate hyperelliptic genus-5 curves C over $\mathbb{F}_3$ so that $|C(\mathbb{F}_9)|$ (resp. $|C(\mathbb{F}_3)|$) attains the gonality-point bound, making use of an algorithm for superelliptic curves.

As mentioned above, a trigonal curve C over K admits a morphism $\pi : C \to \mathbb{P}^1$ over K of degree 3. Let ω_C be the canonical sheaf and set $\mathcal{L} = \pi^* O_{\mathbb{P}^1}(1)$. Then the linear system $\omega_C \otimes \mathcal{L}^{-1}$ defines a morphism $\rho : C \to \mathbb{P}^2$. The image of ρ turns out to be a quintic in $\mathbb{P}^2$ with single singular point, which is a K-rational point and is a node or a cusp. Thus, any trigonal curve of genus 5 is realized as the desingularization of such a quintic in $\mathbb{P}^2$, see [14, Subsection 2.1] for more details. In Section 5, we shall enumerate trigonal genus-5 curves C over $\mathbb{F}_3$ so that $|C(\mathbb{F}_9)|$ (resp. $|C(\mathbb{F}_3)|$) attains the gonality-point bound. Note that such trigonal genus-5 curves are not superelliptic of the form (2.1) with $N = 3$, see Table 1.

Finally it is known that any non-hyperelliptic and non-trigonal curve C of genus 5 is realized as a complete intersection of three quadrics in $\mathbb{P}^4$ (cf. [9, Chap. IV, Ex. 5.5]). We need so many indeterminates to parameterize three quadrics, but in [15] the authors introduced a sextic model of $\mathbb{P}^2$ constructed from C and two distinct points on C, which enables us to parameterize these curves very efficiently. Although C has gonality 4 over $\overline{K}$ (cf. [9, Chap. IV, Example 5.5.3]), C may not admit a morphism $C \to \mathbb{P}^1$ over K of degree 4 (i.e., the smallest degree of $C \to \mathbb{P}^1$ over K can be greater than 4). For $g = 5$ and $N \geq 4$, by (1.3) the gonality-point bound is greater than the Hasse-Weil upper bound if $q^r > 9$. Consulting manYPoint site [8] for $q^r \leq 9$, we conclude that there is no non-hyperelliptic and non-trigonal curve of genus 5 over any finite field attaining the gonality-point bound.

3. Algorithms for superelliptic curves and their complexities

As in the previous section, let q be a power of a prime p, and r a positive integer. In this section, we consider to find or enumerate superelliptic genus-g curves C over $\mathbb{F}_q$ so that $\left|C(\mathbb{F}_{q^r})\right|$ attains the gonality-point bound. Let N be an integer with $N \geq 2$.

Assume that $(N, p) = 1$ and $N \mid d$ and $\boldsymbol{\mu}_N := \{\mu \in \overline{\mathbb{F}_p} : \mu^N = 1\} \subset \mathbb{F}_{q^r}^{\times}$, i.e., $N \mid (q^r - 1)$. These assumptions are satisfied if $N = 2$ and $d = 2g+2$. Let C be the desingularization at the point at infinity ∞ of

$$y^N = f(x) := a_d x^d + a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_1 x + a_0\,, \tag{3.1}$$

where $f(x)$ is a square-free univariate polynomial over $\mathbb{F}_q$ with $a_d = 1$. The assumptions $N \mid d$ and $a_d = 1$ imply that C has N rational points over the point at infinity. By the

assumption $\mu_N \subset \mathbb{F}_{q^r}^\times$, we have $\left|C(\mathbb{F}_{q^r})\right| = N(q^r+1)$ if and only if $f(\alpha) \in (\mathbb{F}_{q^r}^\times)^N$ for all $\alpha \in \mathbb{F}_{q^r}$.

3.1. Algorithm based on exhaustive search

The most simplest computational method to find or enumerate C with $\left|C(\mathbb{F}_{q^r})\right| = N(q^r+1)$ is an exhaustive search: For each $(a_0, \ldots, a_{d-1}) \in (\mathbb{F}_q)^{\oplus d}$, compute $f(\alpha)$ for all $\alpha \in \mathbb{F}_{q^r}$, and check whether they belong to $(\mathbb{F}_{q^r}^\times)^N$ or not. Here, f' denotes the derivative of f.

LEMMA 3.1.1. *The complexity of the exhaustive search is $\tilde{O}(q^d(d+r^2q^r))$ (resp. $\tilde{O}(q^{d+r}r)$) operations in $\mathbb{F}_{q^r}$ if $d \geq q^r$ (resp. $d < q^r$).*

Proof. The set $(\mathbb{F}_{q^r}^\times)^N$ is constructed in $\frac{q^r-1}{N}\log(N)$ operations in $\mathbb{F}_{q^r}$, since $\left|(\mathbb{F}_{q^r}^\times)^N\right| = \frac{q^r-1}{N}$ by the assumption $\mu_N \subset \mathbb{F}_{q^r}^\times$. The number of loops on $(a_0, \ldots, a_{d-1})$ is q^d. For each loop, the values $f(\alpha)$ for all $\alpha \in \mathbb{F}_{q^r}$ are computed as follows:

- If $d \geq q^r$, we first compute the remainder $g(x) := f(x) \bmod (x^{q^r}-x)$ of $f(x)$ by $x^{q^r}-x$, in $O(d)$ operations in $\mathbb{F}_q$. Then it suffices to compute $g(\alpha)$ for all $\alpha \in \mathbb{F}_{q^r}$ since $g(\alpha) = f(\alpha)$. Computing $g(\alpha)$'s is done in $\mathsf{M}(q^r)\log(q^r)$ operations in $\mathbb{F}_{q^r}$, by using divide-and-conquer, where $\mathsf{M}(n)$ denotes the complexity of multiplying two univariate polynomials of degree at most n over $\mathbb{F}_q$.
- If $d < q^r$, we divide the elements of $\mathbb{F}_{q^r}$ into $\lceil q^r/d \rceil$ groups, where each group consists of at most d elements. For each group, it suffices to compute $f(\alpha)$ for all α belonging to the group. Computing $g(\alpha)$'s is done in $\lceil q^r/d \rceil\ \mathsf{M}(d)\log(d)$ operations in $\mathbb{F}_{q^r}$, by using divide-and-conquer (cf. [5, Corollary 10.8]).

The complexity of checking whether $f(\alpha) \in (\mathbb{F}_{q^r}^\times)^N$ for all $\alpha \in \mathbb{F}_{q^r}$ or not is $O\left(q^r \log\left|(\mathbb{F}_{q^r}^\times)^N\right|\right)$, and that of computing $\gcd(f, f')$ is $\mathsf{M}(d)\log d$ (see e.g., [5, Corollary 11.9]). By $\left|(\mathbb{F}_{q^r}^\times)^N\right| = \frac{q^r-1}{N}$, the total complexity of the exhaustive search is

$$\begin{cases} \frac{q^r-1}{N}\log(N) + q^d\left(d + \mathsf{M}(q^r)\log(q^r) + q^r \log\frac{q^r-1}{N} + \mathsf{M}(d)\log d\right) & (d \geq q^r), \\ \frac{q^r-1}{N}\log(N) + q^d\left(\lceil q^r/d \rceil\ \mathsf{M}(d)\log(d) + q^r \log\frac{q^r-1}{N} + \mathsf{M}(d)\log d\right) & (d < q^r) \end{cases} \tag{3.2}$$

operations in $\mathbb{F}_{q^r}$. Assuming $\mathsf{M}(n) = n\log(n)\log(\log(n))$, we can bound (3.2) by $\tilde{O}(q^d(d+r^2q^r))$ (resp. $\tilde{O}(q^{d+r}r)$) if $d \geq q^r$ (resp. $d < q^r$). □

3.2. Algorithms based on linear algebra

We construct alternative algorithms which rely on solving linear systems over finite fields. The idea is as follows: Regarding $a_0, \ldots, a_{d-1}$ and $c_\alpha := f(\alpha)$ as unknowns, we solve a system of linear equations

$$\sum_{i=0}^{d-1} a_i \alpha^i = c_\alpha - \alpha^d \quad (\alpha \in \mathbb{F}_{q^r}) \tag{3.3}$$

on $a_0, \ldots, a_{d-1}$ for any possible values $c_\alpha \in (\mathbb{F}_{q^r}^\times)^N$. For each solution $(a_0, \ldots, a_{d-1})$ to the system, we also check if $\gcd(f, f') = 1$ or not, and if so, store the superelliptic curve $C : y^N = f(x)$.

In the following, we shall precisely describe an algorithm constructed from this idea, and analyze its complexity, dividing the case into **(A)** $q^r \geq d$ and **(B)** $q^r < d$. Also in each case, we use the orbit decomposition of $\mathbb{F}_{q^r}$ with respect to the q-th power Frobenius map, and so recall it here briefly: For each positive integer e dividing r, let S_e denote the set of elements α in $\mathbb{F}_{q^e}$, such that α does not belong to any smaller subfield of $\mathbb{F}_{q^e}$, say $S_e := \{\alpha \in \mathbb{F}_{q^e} : \alpha \notin \mathbb{F}_{q^{e'}} \text{ for } \forall e' \mid e \text{ with } e' < e\}$. Each S_e is decomposed into $S_e = \bigsqcup_{i=1}^{|S_e|/e} S_{e,i}$, where $S_{e,i}$ is an orbit of the q-th power on S_e, that is, $S_{e,i} = \{\alpha_{e,i}^{q^j} : 0 \leq j \leq e-1\}$ for some $\alpha_{e,i} \in S_e$. We then obtain the desired orbit decomposition as

$$\mathbb{F}_{q^r} = \bigsqcup_{e|r} S_e = \bigsqcup_{e|r} \bigsqcup_{i=1}^{|S_e|/e} S_{e,i} \,. \tag{3.4}$$

Throughout the rest of this subsection, we also fix $\alpha_{e,i}$ for each (e, i).

3.2.1. Case (A): $q^r \geq d$.

Choosing arbitrary d distinct elements $\alpha_0, \ldots, \alpha_{d-1}$ of $\mathbb{F}_{q^r}$, we deduce a linear system

$$\sum_{i=0}^{d-1} a_i \alpha_j^i = c_{\alpha_j} - \alpha_j^d \quad (0 \leq j \leq d-1) \tag{3.5}$$

from (3.3). This system has a unique solution $(a_0, \ldots, a_{d-1})$, which is computed with a Vandermonde matrix with respect to $\alpha_0, \ldots, \alpha_{d-1}$. For the obtained $(a_0, \ldots, a_{d-1})$, we need to check whether $f(\alpha) \in (\mathbb{F}_{q^r}^\times)^N$ for all $\alpha \in \mathbb{F}_{q^r} \setminus \{\alpha_0, \ldots, \alpha_{d-1}\}$ or not. From this, we obtain the following algorithm:

ALGORITHM 3.2.1. *Given (N, d, q, r) with $q^r \geq d$, proceed with the following*:

(0) *Construct the set $(\mathbb{F}_{q^r}^\times)^N$.*

(1) *Choose arbitrary d distinct elements $\alpha_0, \ldots, \alpha_{d-1}$ of $\mathbb{F}_{q^r}$, and compute α_j^i for all $0 \leq j \leq d-1$ and $2 \leq i \leq d$. Construct a Vandermonde matrix with respect to $\alpha_0, \ldots, \alpha_{d-1}$, and its inverse.*

(2) *For each $(c_{\alpha_j})_{0 \leq j \leq d-1} \in \prod_{j=0}^{d-1} (\mathbb{F}_{q^r}^\times)^N$, conduct the following:*

  (2-1) *Compute a unique solution $(a_0, \ldots, a_{d-1})$ to the linear system (3.5), by using the inverse of the Vandermonde matrix constructed in Step (1).*

  (2-2) *Compute $c_\alpha := f(\alpha)$ for all $\alpha \in \mathbb{F}_{q^r} \setminus \{\alpha_0, \ldots, \alpha_{d-1}\}$. Test if each c_α belongs to $(\mathbb{F}_{q^r}^\times)^N$ or not.*

  (2-3) *If $c_\alpha \in (\mathbb{F}_{q^r}^\times)^N$ for all $\alpha \in \mathbb{F}_{q^r} \setminus \{\alpha_0, \ldots, \alpha_{d-1}\}$, compute $\gcd(f, f')$. If $\gcd(f, f') = 1$, store the superelliptic curve $C : y^N = f(x)$.*

(3) *Output C's collected in Step (2).*

LEMMA 3.2.2. *Assuming that the complexity of Step (0) is negligible compared to those of the other steps, Algorithm 3.2.1 runs in $\tilde{O}(q^{rd}(d^2 + q^r r))$ operations in $\mathbb{F}_{q^r}$.*

Proof. For Step (1), computing α_j^i for all $0 \leq j \leq d-1$ and $2 \leq i \leq d$ is done in $O(d^2)$, and the inverse of a Vandermonde matrix with respect to $\alpha_0, \ldots, \alpha_{d-1}$ is computed in $O(d^\omega)$, where ω is the exponent of matrix multiplication with $2 < \omega \leq 3$. Hence, the complexity of Step (1) is $d^2 + d^\omega = O(d^\omega)$.

As for Step (2), the number of loops for this step is $\left|(\mathbb{F}_{q^r}^\times)^N\right|^d = \left(\frac{q^r-1}{N}\right)^d = O(q^{rd})$. For each loop, the complexity of Step (2-1) is estimated as that of multiplying the inverse of the Vandermonde matrix constructed in Step (1) by a d-dimensional vector whose entries are $c_{\alpha_i} - \alpha_i^d$ with $0 \leq j \leq d-1$, say $O(d^2)$. Similarly to the proof of Lemma 3.1.1, we can estimate the complexities of Steps (2-2) and (2-3) as $\left\lceil \frac{q^r-d}{d} \right\rceil \mathsf{M}(d)\log(d) + (q^r - d)\log\left|(\mathbb{F}_{q^r}^\times)^N\right| = \tilde{O}(q^r r)$ and $\mathsf{M}(d)\log d = \tilde{O}(d)$ respectively, where we used $\mathsf{M}(n) = n\log(n)\log(\log(n))$. Hence, the complexity of Step (2) is estimated as

(3.6)
$$q^{rd}\left(d^2 + \left\lceil \frac{q^r-d}{d} \right\rceil \mathsf{M}(d)\log(d) + (q^r-d)\log\frac{q^r-1}{N} + \mathsf{M}(d)\log d\right) = \tilde{O}(q^{rd}(d^2+q^r r))\,.$$

Therefore, the total complexity is $d^\omega + q^{rd}(d^2+q^r r) = \tilde{O}(q^{rd}(d^2+q^r r))$, as desired. □

Improvement of Algorithm 3.2.1. Using the orbit decomposition (3.4), we can improve Algorithm 3.2.1 as follows. First, for checking whether $f(\alpha) \in (\mathbb{F}_{q^r}^\times)^N$ for all $\alpha \in \mathbb{F}_{q^r} \setminus \{\alpha_0, \ldots, \alpha_{d-1}\}$ or not, it suffices to test if $f(\alpha_{e,i}) \in (\mathbb{F}_{q^r}^\times)^N \cap \mathbb{F}_{q^e}$ for all $\alpha_{e,i}$ or not, since $f(\alpha^{q^i}) = f(\alpha)^{q^i}$ for any $\alpha \in \mathbb{F}_{q^r}$ and $1 \leq i \leq r-1$. Second, the number of choices of c_α's is $\left|(\mathbb{F}_{q^r}^\times)^N\right|^d$ naively, but it can be reduced by choosing $\alpha_0, \ldots, \alpha_{d-1}$ appropriately. Specifically, we choose (e_k, i_k) with $1 \leq k \leq t$ so that $\sum_{k=1}^t |S_{e_k,i_k}| \geq d$, and take arbitrary d distinct elements of $\bigsqcup_{k=1}^t S_{e_k,i_k}$ as $\alpha_0, \ldots, \alpha_{d-1}$. In this case, once the value of c_α for $\alpha = \alpha_{e_k,i_k}$ is given, that of $c_{\alpha^{q^j}}$ is also determined as $c_\alpha^{q^j}$ for each $1 \leq j \leq e_k - 1$. Taking these into account, we here present an improved algorithm:

ALGORITHM 3.2.3 (Improvement of Algorithm 3.2.1). *Given (N, d, q, r) with $q^r \geq d$, proceed with the following*:

(0) *Compute the orbit decomposition (3.4), and then choose and fix an element $\alpha_{e,i}$ of each orbit $S_{e,i}$. Construct also the set $(\mathbb{F}_{q^r}^\times)^N$, and compute the set $(\mathbb{F}_{q^r}^\times)^N \cap \mathbb{F}_{q^e}$ for each positive integer e dividing r.*

(1) *Choose (e_k, i_k) with $1 \leq k \leq t$ so that $\sum_{k=1}^t |S_{e_k,i_k}| \geq d$, and arbitrary d distinct elements $\alpha_0, \ldots, \alpha_{d-1}$ from $\bigsqcup_{k=1}^t S_{e_k,i_k}$. Compute also a Vandermonde matrix with respect to $\alpha_0, \ldots, \alpha_{d-1}$, and its inverse.*

(2) *For each $(c_k)_{1\leq k\leq t} \in \prod_{k=1}^t (\mathbb{F}_{q^r}^\times)^N \cap \mathbb{F}_{q^{e_k}}$, conduct the following*:

(2-1) *Putting the value of c_α for $\alpha = \alpha_{e_k,i_k}$ as c_k, compute c_{α_i} for all $0 \leq i \leq d-1$. Compute also a unique solution $(a_0, \ldots, a_{d-1})$ to the linear system (3.5), by using the inverse of the Vandermonde matrix constructed in Step (1).*

(2-2) *Compute* $c_{\alpha_{e,i}} := f(\alpha_{e,i})$ *for all* (e,i) *with* $\alpha_{e,i} \notin \{\alpha_{e_1,i_1}, \ldots, \alpha_{e_t,i_t}\}$. *Test if each* $c_{\alpha_{e,i}}$ *belongs to* $(\mathbb{F}_{q^r}^\times)^N \cap \mathbb{F}_{q^e}$ *or not.*

(2-3) *If* $c_{\alpha_{e,i}} \in (\mathbb{F}_{q^r}^\times)^N \cap \mathbb{F}_{q^e}$ *for all* (e,i), *compute* $\gcd(f, f')$. *If* $\gcd(f, f') = 1$, *store the superelliptic curve* $C : y^N = f(x)$.

(3) *Output* C*'s collected in Step* (2).

LEMMA 3.2.4. *Assuming that the complexity of Step (0) is negligible compared to those of the other steps, Algorithm 3.2.3 runs in* $\tilde{O}(q^r(dr + d^2 + q^r))$ *operations in* $\mathbb{F}_{q^r}$.

Proof. It follows from the proof of Lemma 3.2.2 that the complexity of Step (1) is $\tilde{O}(d^\omega)$. As for the complexity of Step (2), the number of loops for this step is $\prod_{k=1}^{t} \left|(\mathbb{F}_{q^r}^\times)^N \cap \mathbb{F}_{q^{e_k}}\right|$. In the worst case, we take the whole $\mathbb{F}_{q^r}$ as $\bigsqcup_{k=1}^{t} S_{e_k,i_k}$, so that

$$\prod_{k=1}^{t} \left|(\mathbb{F}_{q^r}^\times)^N \cap \mathbb{F}_{q^{e_k}}\right| \le \prod_{e|r} \prod_{i=1}^{|S_e|/e} \left|(\mathbb{F}_{q^r}^\times)^N \cap \mathbb{F}_{q^e}\right| \le \left(\frac{q^r-1}{N}\right)^s \tag{3.7}$$

by $\left|(\mathbb{F}_{q^r}^\times)^N\right| = \frac{q^r-1}{N}$, where s is the number of orbits of the q-th power on $\mathbb{F}_{q^r}$. Since s is estimated as

$$s = \sum_{e|r} \frac{1}{e} \sum_{i|e} \mu\left(\frac{e}{i}\right) q^i \sim \frac{q^r}{r}$$

with the Möbius function μ, it follows from (3.7) that the number of loops for Step (2) is upper-bounded by $\left(\frac{q^r-1}{N}\right)^{q^r/r}$. For each loop, one computes c_{α_i} for all $0 \le i \le d-1$ in $d \log(q^r) = \tilde{O}(dr)$ in Step (2-1). By $s \sim q^r/r$, the complexities of the rest of Step (2-1) and the last steps can be estimated in a way similar to the proof of Lemma 3.2.2, so that the complexity of Step (2) is

$$\left(\frac{q^r-1}{N}\right)^{\frac{q^r}{r}} \left(dr + d^2 + \left\lceil \frac{q^r}{rd} \right\rceil \mathsf{M}(d) \log(d) + \frac{q^r}{r} \log \frac{q^r-1}{N} + \mathsf{M}(d)\right) = \tilde{O}(q^{q^r}(dr + d^2 + q^r)).$$

Therefore, the total complexity is $d^\omega + q^{q^r}(dr + d^2 + q^r) = \tilde{O}(q^{q^r}(dr + d^2 + q^r))$, as desired. □

3.2.2. Case (B): $q^r < d$

In this case, we cannot take d distinct elements from $\mathbb{F}_{q^r}$, and so a solution to (3.3) is not unique if it exists. Nevertheless, once the values of $f(\alpha)$ for all $\alpha \in \mathbb{F}_{q^r}$ are specified, we can compute any solutions $(a_0, \ldots, a_{d-1})$. Indeed, the system (3.3) is re-written as

$$\begin{cases} a_0 = f(0), \\ \displaystyle\sum_{i=0}^{q^r-2} \left(\sum_{0 \le j \le d-1 \text{ with } j \equiv i \bmod (q^r-1)} a_j \right) \alpha^i = f(\alpha) - \alpha^d \quad (\alpha \in \mathbb{F}_{q^r}^\times), \end{cases} \tag{3.8}$$

where we used $\alpha^{q^r-1} = 1$ for any $\alpha \in \mathbb{F}_{q^r}^{\times}$. Regarding the coefficient of each α^i in (3.8) as an unknown A_i, and putting $c_\alpha := f(\alpha) \in (\mathbb{F}_{q^r}^{\times})^N$ for each $\alpha \in \mathbb{F}_{q^r}$, we construct a system of linear equations

$$\sum_{i=0}^{q^r-2} A_i \alpha^i = c_\alpha - \alpha^d \quad (\alpha \in \mathbb{F}_{q^r}^{\times}) \tag{3.9}$$

whose coefficient matrix is a $(q^r - 1) \times (q^r - 1)$ invertible Vandermonde matrix. This system has a unique solution $(A_i)_{0 \le i \le q^r-2}$, where each A_i of the solution belongs to $\mathbb{F}_q$. Moreover, regarding $a_1, \ldots, a_{d-1}$ as unknowns, we also obtain a system of $q^r - 1$ linear equations

$$\sum_{0 \le j \le d-1 \text{ with } j \equiv i \bmod (q^r-1)} a_j = A_i \qquad (i = 0, \ldots, q^r - 2) \tag{3.10}$$

with $a_0 := c_0$. The extended coefficient matrix of (3.10) is of the form

$$\begin{array}{c} i \\ 1 \\ 2 \\ \vdots \\ q^r-2 \\ 0 \end{array}
\begin{array}{ccccc|ccccc|cc|c}
a_1 & a_2 & \cdots & a_{q^r-2} & a_{q^r-1} & a_{q^r} & a_{q^r+1} & \cdots & a_{2q^r-3} & a_{2q^r-2} & \cdots & \cdots & \\
1 & & & & & 1 & & & & & & & A_1 \\
 & 1 & & & & & 1 & & & & & & A_2 \\
 & & \ddots & & & & & \ddots & & & \cdots & \cdots & \vdots \\
 & & & 1 & & & & & 1 & & & & A_{q^r-2} \\
 & & & & 1 & & & & & 1 & & & A_0 - c_0
\end{array},$$

where the row indexed by i corresponds to the equation indexed by i in (3.10) for each i with $0 \le i \le q^r - 2$. Thus, both the coefficient matrix and the extended one of (3.10) have rank $q^r - 1$, and a solution is $(a_1, \ldots, a_{q^r-2}, a_{q^r-1}, a_{q^r}, \ldots, a_{d-1}) = (A_0, \ldots, A_{q^r-2}, A_0 - c_0, 0, \ldots, 0)$. This implies that the dimension of the null-space of the coefficient matrix is $d - q^r$, and it is straightforward that any solution is of the form

$$(a_1, \ldots, a_{d-1}) = (A_1, \ldots, A_{q^r-2}, A_0 - c_0, 0, \ldots, 0) + \sum_{j=q^r}^{d-1} a_j \left(\mathbf{e}_j - \mathbf{e}_{j \bmod q^r-1}\right),$$

where $\mathbf{e}_j$ denotes the $(q^r - 1)$-dimensional vector with 1 in the j-th (resp. $(q^r - 1)$-th) coordinate and 0's elsewhere for $1 \le j \le q^r - 2$ (resp. $j = 0$).

Here, we write down the above method to compute $(a_0, \ldots, a_{d-1})$'s as an algorithm:

ALGORITHM 3.2.5. *Given (N, d, q, r) with $q^r < d$, proceed with the following*:

(0) *Construct the set* $(\mathbb{F}_{q^r}^{\times})^N$.

(1) *Construct a Vandermonde matrix with respect to the elements of* $\mathbb{F}_{q^r}^{\times}$, *and its inverse.*

(2) *For each* $(c_\alpha)_{\alpha \in \mathbb{F}_{q^r}} \in \prod_{\alpha \in \mathbb{F}_{q^r}} (\mathbb{F}_{q^r}^{\times})^N$, *conduct the following*:

(2-1) *Compute a unique solution* $(A_0, \ldots, A_{q^r-2})$ *to the linear system* (3.9), *by using the inverse of the Vandermonde matrix constructed in Step* (1).

(2-2) *For each* $(a_{q^r}, a_{q^r+1} \ldots, a_{d-1}) \in (\mathbb{F}_q)^{\oplus(d-q^r)}$, *compute* $(a_1, \ldots, a_{q^r-1})$ *by* (3.2.2)*, and then compute* $\gcd(f, f')$. *If* $\gcd(f, f') = 1$, *store the superelliptic curve* $C : y^N = f(x)$.

(3) *Output* C*'s collected in Step (2).*

Compute the space V of g in the case where $c_\alpha = 0$ for all α. Let f_0 be a solution for (c_α). Then for every solution f for (c_α) is written as a sum $f_0 + g$, where $g \in V$.

	Exhaustive search	Linear Algebra method	Use orbit decomp.
$q^r \geq d$	$\tilde{O}(q^{d+r}r)$	$\tilde{O}(q^{rd}(d^2+q^r r))$	$\tilde{O}(q^{q^r}(dr+d^2+q^r))$
$q^r < d$	$\tilde{O}(q^d(r^2q^r+d))$	$\tilde{O}(q^{rq^r}(q^{2r}+q^{d-q^r}d))$	$\tilde{O}(q^{q^r}(q^{2r}+q^{d-q^r}d))$

The complexity of the exhaustive search is $\tilde{O}(q^d(d+r^2q^r))$ (resp. $\tilde{O}(q^{d+r}r)$) operations in $\mathbb{F}_{q^r}$ if $d \geq q^r$ (resp. $d < q^r$).

LEMMA 3.2.6. *Assuming that the complexity of Step (0) is negligible compared to those of the other steps, Algorithm* 3.2.5 *runs in* $\tilde{O}(q^{rq^r}(q^{2r}+q^{d-q^r}d))$ *operations in* $\mathbb{F}_{q^r}$.

Proof. As in the proof of Lemma 3.2.2, the complexity of Step (1) is estimated as $O(q^{\omega r})$. The number of loops for Step (2) is $\left|(\mathbb{F}_{q^r}^\times)^N\right|^{q^r} = \left(\frac{q^r-1}{N}\right)^{q^r} = O(q^{rq^r})$. For each loop, the complexity of Step (2-1) is estimated as $O(q^{2r})$. In Step (2-2), a solution (3.2.2) and $\gcd(f, f')$ are computed respectively in $O(d)$ and in $O(\mathsf{M}(d))$, in q^{d-q^r} times. Hence, the complexity of Step (2) is

$$q^{rq^r}\left(q^{2r}+q^{d-q^r}\mathsf{M}(d)\right) = \tilde{O}(q^{rq^r}(q^{2r}+q^{d-q^r}d))\,. \tag{3.11}$$

Therefore, the total complexity is $q^{\omega r} + q^{rd}(q^{2r}+q^{d-q^r}d) = \tilde{O}(q^{rd}(q^{2r}+q^{d-q^r}d))$, as desired. □

Similarly to Algorithm 3.2.3, we can improve Algorithm 3.2.5 with the orbit decomposition (3.4). An improved version is given as follows:

ALGORITHM 3.2.7 (Improvement of Algorithm 3.2.5). *Given* (N, d, q, r) *with* $q^r < d$, *proceed with the following*:

(0) *Compute the orbit decomposition* (3.4)*, and then choose and fix an element* $\alpha_{e,i}$ *of each orbit* $S_{e,i}$. *Construct also the set* $(\mathbb{F}_{q^r}^\times)^N$, *and compute the set* $(\mathbb{F}_{q^r}^\times)^N \cap \mathbb{F}_{q^e}$ *for each positive integer* e *dividing* r.

(1) *Construct a Vandermonde matrix with respect to the elements of* $\mathbb{F}_{q^r}^\times$, *and its inverse.*

(2) *For each* $(c_{e,i})_{e,i} \in \prod_{e|r}\prod_{i=1}^{|S_e|/e}(\mathbb{F}_{q^r}^\times)^N \cap \mathbb{F}_{q^e}$, *conduct the following*:

(2-1) *For each positive integer* e *dividing* r *and for each integer* i *with* $1 \leq i \leq |S_e|/e$, *compute the value of* c_α *for* $\alpha = \alpha_{e,i}^{q^j}$ *as* $c_{e,i}^{q^j}$ *for each integer* j *with* $1 \leq j \leq e-1$.

(2-2) *Compute a unique solution* $(A_0, \ldots, A_{q^r-2})$ *to the linear system* (3.9)*, by using the inverse of the Vandermonde matrix constructed in Step* (1).

(2-3) *For each* $(a_{q^r}, a_{q^r+1} \ldots, a_{d-1}) \in (\mathbb{F}_q)^{\oplus(d-q^r)}$, *compute* $(a_1, \ldots, a_{q^r-1})$ *by* (3.2.2)*, and then compute* $\gcd(f, f')$. *If* $\gcd(f, f') = 1$, *store the superelliptic curve* $C : y^N = f(x)$.

(3) *Output C's collected in Step* (2).

LEMMA 3.2.8. *Assuming that the complexity of Step (0) is negligible compared to those of the other steps, Algorithm 3.2.7 runs in $\tilde{O}(q^{q^r}(q^{2r}+q^{d-q^r}d))$ operations in $\mathbb{F}_{q^r}$.*

Proof. The complexity of Step (1) is estimated as $O(q^{\omega r})$, see the proof of Lemma 3.2.6. From the proof of Lemma 3.2.4, the number of loops for Step (2) is upper-bounded by $\left(\frac{q^r-1}{N}\right)^s$, which is asymptotically equal to $O(q^{q^r})$ by $s \sim q^r/r$. For each loop, one computes $c_{e,i}^{q^j}$ for all (e,i) and $1 \leq j \leq e-1$ in $sr\log(q) = \tilde{O}(q^r)$ in Step (2-1). Since the complexities of Steps (2-2) and (2-3) are respectively $\tilde{O}(q^{2r})$ and $\tilde{O}(q^{d-q^r}\mathsf{M}(d))$ from the proof of Lemma 3.2.6, the complexity of Step (2) is

$$q^{q^r}\left(q^r+q^{2r}+q^{d-q^r}\mathsf{M}(d)\right) = \tilde{O}(q^{q^r}(q^{2r}+q^{d-q^r}d))\,. \tag{3.12}$$

Therefore, the total complexity is $q^{\omega r}+q^{q^r}(q^{2r}+q^{d-q^r}d) = \tilde{O}(q^{q^r}(q^{2r}+q^{d-q^r}d))$, as desired. □

REMARK 3.2.9. From the proof of Lemma 3.2.8, the number of C's enumerated by Algorithm 3.2.7 is upper-bounded by

$$\left(\frac{q^r-1}{N}\right)^s \times q^{d-q^r} \sim \frac{q^d}{N^{q^r/r}}\,, \tag{3.13}$$

by $\left|(\mathbb{F}_{q^r}^\times)^N\right| = \frac{q^r-1}{N}$, where s is the number of orbits of the q-th power on $\mathbb{F}_{q^r}$. Here we do not exclude C's with $\gcd(f,f') \neq 1$ nor identify isomorphic C's.

4. Computational results

We implemented Algorithms 3.2.3 and 3.2.7 on the computer algebra system Magma V2.26-10 [1], [2] on a computer with macOS Monterey 12.0.1, at 2.6 GHz CPU 6 Core (Intel Core i7) and 16GB memory. In this section, we summarize computational results obtained by our implementation. The source codes and the log files are summarized at [20].

4.1. Enumeration of superelliptic curves attaining the gonality-point bound

For each set of values (N,d) in Table 1, we executed Algorithm 3.2.3 for the case where $q^r \geq d$ and Algorithm 3.2.7 for the case where $q^r < d$, where we choose (q,r) so that $\boldsymbol{\mu}_N \subset \mathbb{F}_{q^r}^\times$, i.e., $N \mid (q^r-1)$.

- For $g=2$, we have completed the enumeration of superelliptic curves attaining the gonality-point bound. Namely, we enumerated hyperelliptic curves of genus 2 over $\mathbb{F}_q$ with $|C(\mathbb{F}_{q^r})| = 2(q^r+1)$ for all (q,r) satisfying (2.3). As a result, we find that there exists such a curve for each (q,r) with $q^r \leq 13$, see the left figure in Fig. 1 below for the number of such curves.
- Also for $g=4$ with $(N,d)=(3,6)$, we have enumerated superelliptic curves attaining the gonality-point bound for all possible (q,r)'s: $(2,2)$, $(4,1)$, $(7,1)$, and $(13,1)$. Consequently, such curves do exist for $(q,r)=(2,2)$, $(4,1)$, $(7,1)$,

Table 2. The number of genus-g superelliptic curves C of the form (3.1) over $\mathbb{F}_q$ with $a_d = 1$ such that $\left|C(\mathbb{F}_{q^r})\right| = N(q^r+1)$, obtained by executing Algorithms 3.2.3 or 3.2.7 for a set of parameters (N, d, q, r), where we choose (N, d) from Table 1 and (q, r) so that $N \mid (q^r - 1)$. "Upper-bound on q^r by Lemma 2.1.1" shows an upper-bound on q^r deduced from the inequality (2.3) of Lemma 2.1.1 for which there exists a superelliptic curve over $\mathbb{F}_q$ with $\left|C(\mathbb{F}_{q^r})\right| = N(q^r+1)$.

g	(N, d)	Upper-bound on q^r by Lemma 2.1.1	(q, r)	Num. of C's	Time (s)
2	(2, 6)	13	(3, 1)	19	0.016
			(5, 1)	32	<0.001
			(7, 1)	595	0.031
			(9, 1)	540	0.250
			(11, 1)	297	0.750
			(13, 1)	104	2.609
			(3, 2)	22	< 0.001
3	(2, 8)	33	(3, 1)	219	0.016
			(5, 1)	3795	0.250
			(7, 1)	14490	3.047
			(9, 1)	65536	37.984
			(11, 1)	74965	69.781
			(13, 1)	66963	102.050
			(17, 1)	27302	957.850
			(19, 1)	13851	3543.490
			(3, 2)	207	0.016
			(5, 2)	45	5.109
4	(2, 10)	61	(3, 1)	2058	0.109
			(5, 1)	97776	191.141
			(7, 1)	740313	2905.290
			(3, 2)	1488	0.125
			(5, 2)	1992	41.609
	(3, 6)	13	(2, 2)	4	< 0.001
			(4, 1)	10	< 0.001
			(7, 1)	42	< 0.001
			(13, 1)	0	0.328
5	(2, 12)	97	(3, 1)	18658	3.797
			(5, 1)	2452130	60389.340
			(3, 2)	13544	2.188

but do not exist for $(q, r) = (13, 1)$. In particular, there are precisely 6 curves over $\mathbb{F}_4$ which are not defined over the prime field $\mathbb{F}_2$, see Example 4.2.1 below for explicit equations.

- In the case where $g \in \{3, 4, 5\}$, we have succeeded in enumerating hyperelliptic curves of genus g over $\mathbb{F}_q$ with $|C(\mathbb{F}_{q^r})| = 2(q^r + 1)$ only for (q, r)'s shown in Table 2, not all (q, r)'s satisfying (2.3). For example, we enumerated such curves of genus 3 for all (q, r)'s with $q^r \leq 25$ and $q^r \neq 23$ completely (see the right figure in Fig. 1 below for the number of such curves), but have not succeeded in finishing the enumeration for the cases where $q^r = 23, 27, 29, 31$ yet.

Among the curves enumerated in Table 2, we classified $\mathbb{F}_{q^r}$-isomorphism classes for the cases $(g, q^r) = (5, 3), (5, 3^2)$ by an algorithm presented in [13, Section 2.3 (C)]; the

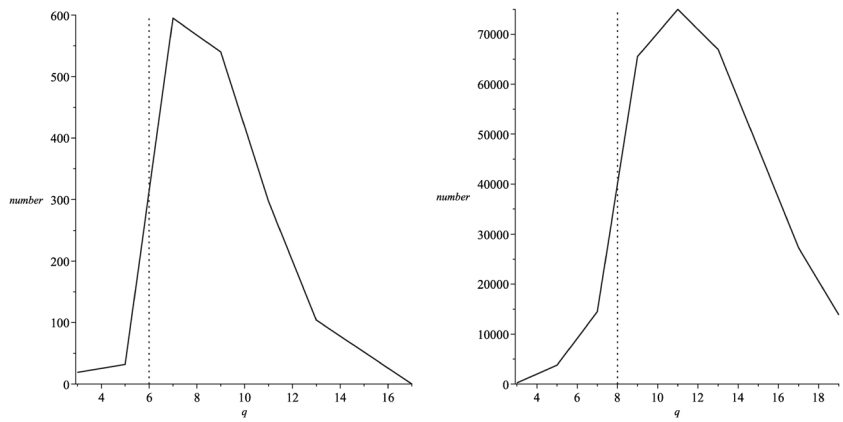

Fig. 1. The number of hyperelliptic curves C of $g = 2, 3$ attaining the gonality bound for $r = 1$. The horizontal axis shows the order q of the field of definition $\mathbb{F}_q$ for C, and the dot line is $x = d$.

same method can be applied to the other cases, but we here treat with these two cases only, based on our motivation described in the third paragraph of Section 1. Our results on the isomorphism classification are as follows:

THEOREM 4.1.1. *There exists a genus-five hyperelliptic curve C over $\mathbb{F}_3$ attaining the gonality-point equality $|C(\mathbb{F}_3)| = 8$, and hence the maximal number of $\mathbb{F}_3$-rational points of genus-five hyperelliptic curves over $\mathbb{F}_3$ is 8. Moreover, there are exactly 820 $\mathbb{F}_3$-isomorphism classes of such curves C.*

THEOREM 4.1.2 (Theorem 1.1). *There exists a genus-five hyperelliptic curve C over $\mathbb{F}_3$ attaining the gonality-point equality $|C(\mathbb{F}_9)| = 20$, and hence the maximal number of $\mathbb{F}_9$-rational points of genus-five hyperelliptic curves over $\mathbb{F}_3$ is 20. Moreover, there are exactly 573 $\mathbb{F}_9$-isomorphism classes of such curves C.*

By a method described in Remark 4.1.4 below, we also computed the Weil polynomials of the $\mathbb{F}_9$-isomorphism classes to classify their Jacobian varieties:

COROLLARY 4.1.3. *Among the 573 $\mathbb{F}_9$-isomorphism classes in Theorem 4.1.2, there are exactly 419 $\mathbb{F}_9$-isogeny classes of Jacobian varieties.*

In Example 4.2.2 below, an example of genus-five hyperelliptic curves C over $\mathbb{F}_3$ with $|C(\mathbb{F}_3)| = 8$ (resp. $|C(\mathbb{F}_9)| = 20$) is given; $C : y^2 = x^{12} - x^2 + 1$ in (4.4) (resp. $C : y^2 = x^{12} - x^4 + 1$ in (4.7)).

REMARK 4.1.4. To prove Corollary 4.1.3, we computed the Weil polynomial of each of the 573 curves. A computational method which we adopt is as follows: Let C be a non-singular curve of genus g over $\mathbb{F}_q$. The Weil polynomial of C, say $W(t) = \prod_{i=0}^{2g}(t - \alpha_i) = \sum_{i=0}^{2g} a_i t^i$, is determined by the numbers $|C(\mathbb{F}_{q^e})|$ for $e = 1, 2, \ldots, g$. Indeed, the values $a_0, a_1, \ldots, a_g$ with $a_k = (-1)^k \sum_{i_1 < i_2 < \ldots < i_k} \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_k}$ are determined by Newton's identities and $\sum_{i=0}^{2g} \alpha_i^e = 1 + q^e - |C(\mathbb{F}_{q^e})|$ for $e = 1, 2, \ldots, g$. The remaining values

$a_{g+1}, \cdots, a_{2g}$ are determined by the formula $a_{2g-i} = q^{g-i}a_i$, which follows from the functional equation of the congruent zeta function. Our computation of Weil polynomials just used this method.

4.2. Some concrete examples

Here, we show concrete examples:

EXAMPLE 4.2.1. Among the curves enumerated in Table 2, the 10 superelliptic curves of genus 4 over $\mathbb{F}_4$ with gonality $N = 3$ attaining $|C(\mathbb{F}_4)| = N(q^r + 1) = 15$ are the following:

$$
\begin{aligned}
&y^3 = x^6 + x^3 + 1\,,\\
&y^3 = x^6 + x^4 + x^3 + x + 1\,,\\
&y^3 = x^6 + tx^4 + x^3 + tx + 1\,,\\
&y^3 = x^6 + t^2x^4 + x^3 + t^2x + 1\,,\\
&y^3 = x^6 + x^5 + x^3 + x^2 + 1\,,\\
&y^3 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\,,\\
&y^3 = x^6 + tx^5 + x^3 + tx^2 + 1\,,\\
&y^3 = x^6 + tx^5 + t^2x^4 + x^3 + tx^2 + t^2x + 1\,,\\
&y^3 = x^6 + t^2x^5 + x^3 + t^2x^2 + 1\,,\\
&y^3 = x^6 + t^2x^5 + tx^4 + x^3 + t^2x^2 + tx + 1\,,
\end{aligned}
$$

where t is an element of $\mathbb{F}_{2^2}$ with $t^2 + t + 1 = 0$. The first and fifth examples in the above list are the special cases of the following curves: It is straightforward to see that for a pair (N, q^r) with $N \mid (q^r - 1)$ and a positive integer m, the curves

$$
\begin{aligned}
y^N &= x^{mp(q^r-1)} + x^{(mp-1)(q^r-1)} + \cdots + x^{2(q^r-1)} + x^{q^r-1} + 1,\\
y^N &= x^{mp(q^r-1)} + x^{mp(q^r-1)-1} + \cdots + x + 1 = \frac{x^{mp(q^r-1)+1} - 1}{x - 1}
\end{aligned}
$$

are superelliptic, whose $\mathbb{F}_{q^r}$-rational points attain the gonality-point bound.

EXAMPLE 4.2.2. Among the curves enumerated in Table 2, we find the following hyperelliptic curves of genus $g = 4, 5$ over $\mathbb{F}_p$ attaining $|C(\mathbb{F}_{q^r})| = 2(q^r + 1)$:

$$y^2 = x^{10} - x^2 + 1 \quad \text{with } (g, q^r) = (4, 3)\,, \tag{4.1}$$

$$y^2 = x^{10} - x^2 + 1 \quad \text{with } (g, q^r) = (4, 5)\,, \tag{4.2}$$

$$y^2 = x^{10} - x^2 + 1 \quad \text{with } (g, q^r) = (4, 9)\,, \tag{4.3}$$

$$y^2 = x^{12} - x^2 + 1 \quad \text{with } (g, q^r) = (5, 3)\,. \tag{4.4}$$

Although we have not finished the enumeration for $p \geq 5$ when $g = 5$ yet, we have succeeded in finding some examples of curves over $\mathbb{F}_p$ attaining $|C(\mathbb{F}_{q^r})| = 2(q^r + 1)$:

$$y^2 = x^{12} - x^4 + 1 \quad \text{with } (g, q^r) = (5, 5)\,, \tag{4.5}$$

$$y^2 = x^{12} - x^6 + 1 \quad \text{with } (g, q^r) = (5, 7)\,, \tag{4.6}$$

$$y^2 = x^{12} - x^4 + 1 \quad \text{with } (g, q^r) = (5, 9)\,, \tag{4.7}$$

(4.8) $$y^2 = x^{12} - x^2 + 1 \quad \text{with } (g, q^r) = (5, 11)\,.$$

We also find that these examples are the special cases of the following hyperelliptic curves $y^2 = f(x)$:

- (4.1), (4.4), (4.5), and (4.6): $y^2 = f(x) = x^{m(q^r-1)} - x^{q^r-1} + 1$, where $f(x)$ is separable if m is divided by p as in (4.4) or if $(1 - m^{-1})^{m-1} \not\equiv m \pmod{p}$ as in (4.1), (4.5), and (4.6). Indeed, the former case is trivial, and the latter case is shown as follows: The derivative f' is
$$f' = m(q^r - 1)x^{m(q^r-1)-1} - (q^r - 1)x^{q^r-2} = -mx^{m(q^r-1)-1} + x^{q^r-2}\,.$$
If $\alpha \neq 0$ were a common root of f and f', we have $\alpha^{q^r-1} = m\alpha^{m(q^r-1)}$ by $f'(\alpha) = 0$, whence $(1 - m^{-1})\alpha^{q^r-1} = 1$ by $f(\alpha) = 0$. Taking the $(m-1)$-th powers of both sides, we also have $(1 - m^{-1})^{m-1}\alpha^{m(q^r-1)-q^r+1} = 1$, and thus $(1 - m^{-1})^{m-1}\alpha^{m(q^r-1)-1} = \alpha^{q^r-2}$. It follows from $(1 - m^{-1})^{m-1} \not\equiv m \pmod{p}$ that $f'(\alpha) \neq 0$, a contradiction.
- (4.2) and (4.7): $y^2 = f(x) = (x^{\frac{q^r-1}{2}})^n + (-1)^n x^{\frac{q^r-1}{2}} + 1$, where $f(x)$ is separable if n is divided by p as in (4.2) and (4.7).
- (4.3) and (4.8): $y^2 = f(x) = x^{q^r+1} - x^2 + 1$, where $f(x)$ is separable if $p > 3$ or if $p = 3$ and $q^r \equiv 1 \pmod 4$. Indeed, if α were a common root of $f(x)$ and $f'(x) = x^{q^r} - 2x$, we have $f(\alpha) = \alpha\alpha^{q^r} - \alpha^2 + 1 = 2\alpha^2 - \alpha^2 + 1 = \alpha^2 + 1 = 0$ and $\alpha \neq 0$. On the other hand, we have $f'(\alpha) = \alpha((\alpha^2)^{\frac{q^r-1}{2}} - 2) = \alpha((-1)^{\frac{q^r-1}{2}} - 2)$, which is non-zero if $p > 3$ or if $p = 3$ and $q \equiv 1 \pmod 4$.

In each case, it is straightforward that $f(\alpha) = 0$ for all $\alpha \in \mathbb{F}_{q^r}$, whence $y^2 = f(x)$ is a hyperelliptic curve attaining the gonality-point bound (if $f(x)$ is separable).

5. Trigonal curves of genus five in characteristic three

In this section, we enumerate trigonal curves of genus five in characteristic $p = 3$ attaining the gonality-point bound, our motivation described in the third paragraph of Section 1.

Let K be a finite field of characteristic $p = 3$, and let q be the cardinality of K. We choose a primitive element ζ of $K^\times$ and a non-square element ε of $K^\times \setminus (K^\times)^2$, and fix them throughout this section. As quintic models of trigonal curves of genus $g = 5$ over K, we have the following three types (cf. [14, Subsection 2.1]):

(Split node case) $C' = V(F)$ for some $F = xyz^3 + f$;
(Non-split node case) $C' = V(F)$ for some $F = (x^2 - \varepsilon y^2)z^3 + f$;
(Cusp case) $C' = V(F)$ for some $F = x^2z^3 + f$,

where f is the sum of monomial terms over K which can not be divided by z^3. Note that in the cusp case, the y^3z^2-coefficient of f has to be non-zero.

5.1. Reduction for trigonal curves of genus five in characteristic three

We here give reduced forms of the defining polynomial F in each of the three cases **(Split node case)**, **(Non-split node case)**, and **(Cusp case)**. In [14, Section 3], we considered similar reductions, but those do not work for $p = 3$.

PROPOSITION 5.1.1 (Split node case). *Any genus-five trigonal curve over K of split node type has a quintic model in $\mathbb{P}^2$ of the form*

(5.1)
$$xyz^3 + (a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3)z^2 + (a_5x^4 + a_6x^3y + a_7x^2y^2 + a_8xy^3 + a_9y^4)z + a_{10}x^5 + a_{11}x^4y + a_{12}x^3y^2 + a_{13}x^2y^3 + a_{14}xy^4 + a_{15}y^5$$

for $a_i \in K$, where either of the following (1) – (5) *hold.*

(1) $a_1 = 1$, $a_2 \in \{0, 1\}$ *and* $a_5 = a_6 = 0$;
(2) $a_1 = 0$, $a_2 = 1$, $a_3 \in \{0, 1\}$ *and* $a_6 = a_7 = 0$;
(3) $a_1 = a_2 = 0$, $a_3 = 1$, $a_4 \in \{0, 1\}$ *and* $a_7 = a_8 = 0$;
(4) $a_1 = a_2 = a_3 = 0$, $a_4 = 1$ *and* $a_8 = a_9 = 0$;
(5) $a_1 = a_2 = a_3 = a_4 = 0$, $a_6 \in \{0, 1, \zeta\}$ *and* $a_7 \in \{0, 1\}$.

Proof. Note that (5.1) is the general form of the quintic in the split node case. Considering $z \to z + \alpha x + \beta y$, we can transform the quintic (5.1) to a quintic of the form:

$$F = xyz^3 + (a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3)z^2 + f_1z + f_0\,, \tag{5.2}$$

where

$$f_1 = (2\alpha a_1 + a_5)x^4 + (2\beta a_1 + 2\alpha a_2 + a_6)x^3y + (2\beta a_2 + 2\alpha a_3 + a_7)x^2y^2 + (2\beta a_3 + 2\alpha a_4 + a_8)xy^3 + (2\beta a_4 + a_9)y^4 \tag{5.3}$$

and f_0 is a quintic form in x and y.

(1) ($a_1 \neq 0$) Putting $\alpha := -a_5/(2a_1)$ and $\beta := -(2\alpha a_2 + a_6)/(2a_1)$, we may assume $a_5 = a_6 = 0$ in (5.1). Considering $(x, y) \to (\gamma x, \delta y)$ and the multiplication by $(\gamma\delta)^{-1}$, the coefficients a_1 and a_2 are transformed into $\gamma^2\delta^{-1}a_1$ and γa_2 respectively. Putting $\gamma := a_2^{-1}$ (resp. $\gamma := 1$) if $a_2 \neq 0$ (resp. $a_2 = 0$) and $\delta := \gamma^2 a_1$, we may assume that the coefficients of x^3z^2 and x^2yz^2 are 1 and 0, 1 respectively.

(2) ($a_1 = 0$ and $a_2 \neq 0$) Putting $\alpha := -a_6/(2a_2)$ and $\beta := -(2\alpha a_3 + a_7)/(2a_2)$, we may assume $a_6 = a_7 = 0$ in (5.1). Considering $(x, y) \to (\gamma x, \delta y)$ and the multiplication by $(\gamma\delta)^{-1}$, the coefficients a_2 and a_3 are transformed into γa_2 and δa_3 respectively. Putting $\gamma := a_2^{-1}$ and $\delta := a_3^{-1}$ (resp. $\delta := 1$) if $a_3 \neq 0$ (resp. $a_3 = 0$), we may assume that the coefficients of x^2yz^2 and xy^2z^2 are 1 and 0, 1 respectively.

(3) ($a_1 = a_2 = 0$ and $a_3 \neq 0$) Putting $\alpha := -a_7/(2a_3)$ and $\beta := -(2\alpha a_4 + a_8)/(2a_3)$, we may assume $a_7 = a_8 = 0$ in (5.1). Considering $(x, y) \to (\gamma x, \delta y)$ and the multiplication by $(\gamma\delta)^{-1}$, the coefficients a_3 and a_4 are transformed into δa_3 and $\gamma^{-1}\delta^2 a_4$ respectively. Putting $\delta := a_3^{-1}$ and $\gamma := \delta^2 a_4$ (resp. $\gamma := 1$) if $a_4 \neq 0$ (resp. $a_4 = 0$), we may assume that the coefficients of xy^2z^2 and y^3z^2 are 1 and 0, 1 respectively.

(4) ($a_1 = a_2 = a_3 = 0$ and $a_4 \neq 0$) Putting $\alpha := -a_8/(2a_4)$ and $\beta := -a_9/(2a_4)$, we may assume $a_8 = a_9 = 0$ in (5.1). Considering $(x, y) \to (\gamma x, \delta y)$ and the multiplication by $(\gamma\delta)^{-1}$, the coefficient a_4 is transformed into $\gamma^{-1}\delta^2 a_4$. Putting $\gamma := a_4$ and $\delta := 1$, we may assume that the coefficient of y^3z^2 is 1.

(5) ($a_1 = a_2 = a_3 = a_4 = 0$) Considering $(x, y) \to (\gamma x, \delta y)$ and the multiplication by $(\gamma\delta)^{-1}$, the coefficients a_6 and a_7 are transformed into $\gamma^2 a_6$ and $\gamma\delta a_7$ respectively.

If $a_6 = 0$, put $\gamma := 1$ and $\delta := a_7^{-1}$ if $a_7 \neq 0$. If $a_6 \neq 0$, write $a_6 = \zeta^{2i+j}$ for $i \in \{0, \dots, (q-3)/2\}$ and $j \in \{0, 1\}$, and put $\gamma := \zeta^{-i}$ and $\delta := (\gamma a_7)^{-1}$ if $a_7 \neq 0$.

□

PROPOSITION 5.1.2 (Non-split node case). *Any genus-five trigonal curve over K of non-split node type has a quintic model in $\mathbb{P}^2$ of the form*

(1) *for $a_i \in K$,*

$$\begin{aligned} F = (x^2-\varepsilon y^2)z^3 + \left\{a_1x(x^2-\varepsilon y^2) + a_2x^3 + y^3\right\} z^2 + (a_3x^4 + a_4x^3y + a_5x^2y^2)z \\ + a_6x^5 + a_7x^4y + a_8x^3y^2 + a_9x^2y^3 + a_{10}xy^4 + a_{11}y^5 . \end{aligned} \tag{5.4}$$

(2) *for $a_i \in K$,*

$$\begin{aligned} F = (x^2 - \varepsilon y^2)z^3 + \left\{x(x^2 - \varepsilon y^2) + a_1x^3\right\} z^2 + (a_2x^4 + a_3x^3y + a_4y^4)z \\ + a_5x^5 + a_6x^4y + a_7x^3y^2 + a_8x^2y^3 + a_9xy^4 + a_{10}y^5 . \end{aligned} \tag{5.5}$$

(3) *for $a_i \in K$,*

$$\begin{aligned} F = (x^2 - \varepsilon y^2)z^3 + x^3z^2 + (a_1x^2y^2 + a_2xy^3 + a_3y^4)z \\ + a_4x^5 + a_5x^4y + a_6x^3y^2 + a_7x^2y^3 + a_8xy^4 + a_9y^5 . \end{aligned} \tag{5.6}$$

(4) *for $a_i \in K$,*

$$\begin{aligned} F = (x^2 - \varepsilon y^2)z^3 + (a_1x^4 + a_2x^3y + a_3x^2y^2 + a_4xy^3 + a_5y^4)z \\ + a_6x^5 + a_7x^4y + a_8x^3y^2 + a_9x^2y^3 + a_{10}xy^4 + a_{11}y^5 , \end{aligned} \tag{5.7}$$

where $(a_6, \dots, a_{11})$ is either of $(0, \dots, 0, 1, a_{i+1}, \dots, a_{11})$ for $i = 6, \dots, 11$.

Proof. Let V be the K-vector space consisting of cubic forms in x, y over K. As seen in [12, Lemma 4.1.1], the representation V of the group

$$\tilde{\mathrm{C}} := \left\{ \begin{pmatrix} r & \varepsilon s \\ s & r \end{pmatrix} : r, s \in K, r^2 - \varepsilon s^2 \neq 0 \right\}$$

defined by $\gamma x = rx + \varepsilon sy$ and $\gamma y = sx + ry$ for $\gamma = \begin{pmatrix} r & \varepsilon s \\ s & r \end{pmatrix} \in \tilde{\mathrm{C}}$ is decomposed as $V_1 \oplus V_2$, where $V_1 = \langle x(x^2-\varepsilon y^2),\, y(x^2-\varepsilon y^2)\rangle$ and $V_2 = \langle x(x^2+3\varepsilon y^2),\, y(3x^2+\varepsilon y^2)\rangle = \langle x^3,\, y^3\rangle$. We write

$$\begin{aligned} F = (x^2 - \varepsilon y^2)z^3 + \left\{c_1x(x^2 - \varepsilon y^2) + c_2y(x^2 - \varepsilon y^2) + b_1x^3 + b_2y^3\right\} z^2 \\ + (a_1x^4 + a_2x^3y + a_3x^2y^2 + a_4xy^3 + a_5y^4)z \\ + a_6x^5 + a_7x^4y + a_8x^3y^2 + a_9x^2y^3 + a_{10}xy^4 + a_{11}y^5 . \end{aligned} \tag{5.8}$$

An element $\gamma = \begin{pmatrix} r & \varepsilon s \\ s & r \end{pmatrix}$ of $\tilde{\mathrm{C}}$ sends $c_1x(x^2 - \varepsilon y^2) + c_2y(x^2 - \varepsilon y^2)$ to

$$(r^2 - \varepsilon s^2)((c_1r + c_2s)x(x^2 - \varepsilon y^2) + (c_1\varepsilon s + c_2r)y(x^2 - \varepsilon y^2)) .$$

As there exists an $(r, s) \in K^2 \setminus \{(0, 0)\}$ so that $c_1\varepsilon s + c_2 r = 0$, we may assume that $c_2 = 0$:

$$\begin{aligned} F = {} & (x^2 - \varepsilon y^2)z^3 + \left\{c_1 x(x^2 - \varepsilon y^2) + b_1 x^3 + b_2 y^3\right\} z^2 \\ & + (a_1 x^4 + a_2 x^3 y + a_3 x^2 y^2 + a_4 x y^3 + a_5 y^4)z \\ & + a_6 x^5 + a_7 x^4 y + a_8 x^3 y^2 + a_9 x^2 y^3 + a_{10} x y^4 + a_{11} y^5 . \end{aligned} \tag{5.9}$$

(1) Assume $b_2 \neq 0$. We take the coordinate-change $(x, y, z) \mapsto (x, y, b_2 z)$ and multiply F by b_2^{-3}; then we may assume $b_2 = 1$. Considering the transformation sending z to $z - (a_4/2 + c_1\varepsilon a_5/4)x - (a_5/2)y$, we may eliminate the terms of xy^3 and y^4 from F, i.e., we may assume $(a_4, a_5) = (0, 0)$:

$$\begin{aligned} F = {} & (x^2 - \varepsilon y^2)z^3 + \left\{c_1 x(x^2 - \varepsilon y^2) + b_1 x^3 + y^3\right\} z^2 + (a_1 x^4 + a_2 x^3 y + a_3 x^2 y^2)z \\ & + a_6 x^5 + a_7 x^4 y + a_8 x^3 y^2 + a_9 x^2 y^3 + a_{10} x y^4 + a_{11} y^5 . \end{aligned} \tag{5.10}$$

(2) Assume $b_2 = 0$ and $c_1 \neq 0$. We take the coordinate-change $(x, y, z) \mapsto (x, y, c_1 z)$ and multiply F by c_1^{-3}; then we may assume $c_1 = 1$. Considering the transformation sending z to $z - (a_3/(-2\varepsilon))x - (a_4/(-2\varepsilon))y$, we may eliminate the terms of x^2y^2 and xy^3 from F, i.e., we may assume $(a_3, a_4) = (0, 0)$:

$$\begin{aligned} F = {} & (x^2 - \varepsilon y^2)z^3 + \left\{x(x^2 - \varepsilon y^2) + b_1 x^3\right\} z^2 + (a_1 x^4 + a_2 x^3 y + a_5 y^4)z \\ & + a_6 x^5 + a_7 x^4 y + a_8 x^3 y^2 + a_9 x^2 y^3 + a_{10} x y^4 + a_{11} y^5 . \end{aligned} \tag{5.11}$$

(3) Assume $b_2 = 0$ and $c_1 = 0$ and $b_1 \neq 0$. Similarly F is reduced to

$$\begin{aligned} F = {} & (x^2 - \varepsilon y^2)z^3 + x^3 z^2 + (a_3 x^2 y^2 + a_4 x y^3 + a_5 y^4)z \\ & + a_6 x^5 + a_7 x^4 y + a_8 x^3 y^2 + a_9 x^2 y^3 + a_{10} x y^4 + a_{11} y^5 . \end{aligned} \tag{5.12}$$

□

PROPOSITION 5.1.3 (Cusp case). *Any genus-five trigonal curve over K of cusp type has a quintic model in $\mathbb{P}^2$ of the form*

$$\begin{aligned} F = {} & x^2 z^3 + (b_1 x^3 + b_2 x^2 y + a_1 x y^2 + a_2 y^3)z^2 + (a_3 x^4 + a_4 x^3 y + a_5 x^2 y^2)z \\ & + a_6 x^5 + a_7 x^4 y + a_8 x^3 y^2 + a_9 x^2 y^3 + a_{10} x y^4 + a_{11} y^5 \end{aligned} \tag{5.13}$$

for $a_i \in K$ with $a_2 \neq 0$, where $b_1, b_2 \in \{0, 1\}$.

Proof. Recall from the paragraph at the beginning of this section that any trigonal curve of genus 5 over K of cusp type has a quintic model in $\mathbb{P}^2$ of the form

$$\begin{aligned} F_0 = {} & x^2 z^3 + (a_1 x^3 + a_2 x^2 y + a_3 x y^2 + a_4 y^3)z^2 + (a_5 x^4 + a_6 x^3 y + a_7 x^2 y^2 + a_8 x y^3 \\ & + a_9 y^4)z + a_{10} x^5 + a_{11} x^4 y + a_{12} x^3 y^2 + a_{13} x^2 y^3 + a_{14} x y^4 + a_{15} y^5 , \end{aligned} \tag{5.14}$$

where $a_i \in K$ with $a_4 \neq 0$. Considering $z \to z + \alpha x + \beta y$, we can transform the quintic (5.14) to a quintic of the form:

$$F = x^2 z^3 + (a_1 x^3 + a_2 x^2 y + a_3 x y^2 + a_4 y^3)z^2 + f_1 z + f_0 , \tag{5.15}$$

where f_1 is the same as in (5.3), and where f_0 is a quintic form in x and y. Putting $\beta := -a_9/(2a_4)$ and $\alpha := -(2\beta a_3 + a_8)/(2a_4)$, we may assume $a_8 = a_9 = 0$ in (5.14). Considering $(x, y) \to (\gamma x, \delta y)$ and the multiplication by γ^{-2}, the coefficients a_1 and a_2 are transformed into γa_1 and δa_2 respectively. Thus, we may assume that the coefficients of x^3z^2 and x^2yz^2 are 0 or 1. □

5.2. Curves attainning the gonality-point bound

Based on the reduction for genus-five trigonal curves C provided in the previous subsection, we enumerate those curves over $\mathbb{F}_3$ attaining the gonality-point bound, i.e., $|C(\mathbb{F}_{q^r})| = N(q^r + 1)$ with $(N, q) = (3, 3)$, for the following two cases: $r = 1$ and $r = 2$. As in the superelliptic case treated in Section 4, we use Magma for our enumeration. We also note that our enumeration will be done by an exhaustive search, different from the superellitic case.

First, we consider the case where $r = 1$. In this case, the gonality-point bound is $3(3^1 + 1) = 12$, and we have the following theorem:

THEOREM 5.2.1. *There exists a genus-five trigonal curve C over $\mathbb{F}_3$ attaining the gonality-point equality $|C(\mathbb{F}_3)| = 12$, and hence the maximal number of $\mathbb{F}_3$-rational points of genus-five trigonal curves over $\mathbb{F}_3$ is 12. Moreover, there are exactly nine $\mathbb{F}_3$-isomorphism classes of such curves C.*

Proof. We enumerate quintic models $V(F)$ maximizing $|C(\mathbb{F}_3)|$. For this, we conducted an exhaustive search on all possible unknown coefficients over Magma, for each form ((5.1), (5.4) – (5.7), or (5.13)) of F. The source code for collecting F and its log file are available at [20], and they are named `trigonal_g5q3_step1.txt` and `log_trigonal_g5q3_step1.txt`. It took about 13 hours to execute the code.

We found from the output (`log_trigonal_g5q3_step1.txt`) that the maximal value of $|C(\mathbb{F}_3)|$ is 12. In the following, we list quintic forms F such that $|C(\mathbb{F}_3)| = 12$:

- **(Split node case)** The quintic forms F of the form (5.1) such that the normalization of $V(F) \subset \mathbb{P}^2$ has 12 $\mathbb{F}_3$-rational points are the following:

$$
\begin{aligned}
F_1 &= xyz^3+(x^3+x^2y+2xy^2+2y^3)z^2+(2x^2y^2+2xy^3+y^4)z+2x^5+x^3y^2\,;\\
F_2 &= xyz^3+(x^3+x^2y+2xy^2+2y^3)z^2+(x^2y^2+2xy^3+2y^4)z+2x^5\\
&\quad +2x^4y+x^3y^2+x^2y^3\,;\\
F_3 &= xyz^3+(x^3+x^2y+2xy^2+2y^3)z^2+(2x^2y^2+2xy^3+y^4)z+2x^5\\
&\quad +x^4y+x^3y^2+2x^2y^3\,;\\
F_4 &= xyz^3+(x^3+x^2y+2xy^2+2y^3)z^2+(x^2y^2+2xy^3+2y^4)z+2x^5\\
&\quad +x^4y+x^3y^2+2x^2y^3\,;\\
F_5 &= xyz^3+(x^3+x^2y+2xy^2+2y^3)z^2+(x^2y^2+2xy^3+2y^4)z+2x^5+xy^4;\\
F_6 &= xyz^3+(x^3+x^2y+2xy^2+2y^3)z^2+(2x^2y^2+2xy^3+y^4)z+2x^5\\
&\quad +2x^4y+x^2y^3+xy^4\,;\\
F_7 &= xyz^3+(x^3+x^2y+2xy^2+2y^3)z^2+(x^2y^2+2xy^3+2y^4)z+2x^5\\
&\quad +2x^4y+x^2y^3+xy^4\,;
\end{aligned}
$$

$$F_8 = xyz^3 + (x^3 + x^2y + 2xy^2 + 2y^3)z^2 + (2x^2y^2 + 2xy^3 + y^4)z + 2x^5 + x^4y + 2x^2y^3 + xy^4;$$
$$F_9 = xyz^3 + (x^3 + x^2y + 2xy^2 + 2y^3)z^2 + (2x^2y^2 + 2xy^3 + y^4)z + 2x^5 + 2x^3y^2 + 2xy^4;$$
$$F_{10} = xyz^3 + (x^3 + x^2y + 2xy^2 + 2y^3)z^2 + (x^2y^2 + 2xy^3 + 2y^4)z + 2x^5 + 2x^4y + 2x^3y^2 + x^2y^3 + 2xy^4;$$
$$F_{11} = xyz^3 + (x^3 + x^2y + 2xy^2 + 2y^3)z^2 + 2xy^3z + 2x^5 + x^3y^2 + 2x^2y^3 + y^5;$$
$$F_{12} = xyz^3 + (x^3 + x^2y + 2xy^2 + 2y^3)z^2 + 2xy^3z + 2x^5 + 2x^4y + xy^4 + y^5;$$
$$F_{13} = xyz^3 + (x^3 + x^2y + 2xy^2 + 2y^3)z^2 + 2xy^3z + 2x^5 + x^4y + x^2y^3 + xy^4 + y^5;$$
$$F_{14} = xyz^3 + (x^3 + x^2y + 2xy^2 + 2y^3)z^2 + 2xy^3z + 2x^5 + 2x^2y^3 + xy^4 + y^5;$$
$$F_{15} = xyz^3 + (x^3 + x^2y + 2xy^2 + 2y^3)z^2 + 2xy^3z + 2x^5 + x^4y + 2x^3y^2 + x^2y^3 + 2xy^4 + y^5.$$

- **(Non-split node case)** There are no F that achieves $|C(\mathbb{F}_3)| = 12$.
- **(Cusp case)** The quintic forms F of the form (5.13) such that the normalization of $V(F) \subset \mathbb{P}^2$ has 12 $\mathbb{F}_3$-rational points are the following:

$$F_{16} = x^2z^3 + (x^2y + 2y^3)z^2 + 2x^4z + 2x^2y^3 + y^5;$$
$$F_{17} = x^2z^3 + (x^2y + 2y^3)z^2 + 2x^4z + 2x^4y + 2x^3y^2 + xy^4 + y^5;$$
$$F_{18} = x^2z^3 + (x^2y + 2y^3)z^2 + 2x^4z + 2x^4y + x^3y^2 + 2xy^4 + y^5.$$

For the above 22 curves, we classify their $\mathbb{F}_3$-isomorphism classes of the above 18 curves, by an algorithm provided in [14, Section 5]. The source code for the isomorphism classification and its log file are available at [20], and they are named `log_trigonal_g5q3_step2.txt` and `log_trigonal_g5q3_step2.txt` respectively. The time it took to execute the code is about 0.3 seconds. As a result, there are nine $\mathbb{F}_3$-isomorphism classes:

(1) F_1 and F_8; (2) F_2 and F_{13}; (3) F_3; (4) F_4 and F_{15};
(5) F_5 and F_{11}; (6) F_6 and F_9; (7) F_7 and F_{14}; (8) F_{10} and F_{12};
(9) F_{16}, F_{17}, and F_{18}.

□

Next, we consider the case where $r = 2$. In this case, the gonality-point bound is $3(3^2 + 1) = 30$, and we have the following theorem:

THEOREM 5.2.2 (Theorem 1.2). *There exists a genus-five trigonal curve C over $\mathbb{F}_3$ attaining the gonality-point equality $|C(\mathbb{F}_9)| = 30$, and hence the maximal number of $\mathbb{F}_9$-rational points of genus-five trigonal curves over $\mathbb{F}_3$ is 30. Moreover, there are exactly eight $\mathbb{F}_3$-isomorphism classes of such curves C.*

Proof. Similarly to the case where $r = 1$ (cf. the proof of Theorem 5.2.1), we conducted an exhaustive search on all possible unknown coefficients over Magma, for each form ((5.1), (5.4) – (5.7), or (5.13)) of F. The source code and its log file are available at

[20], and they are named `trigonal_g5q9_step1.txt` and `log_trigonal_g5q9_step1.txt` respectively. It took about 2.5 hours to execute the code.

We found from the output (`log_trigonal_g5q9_step1.txt`) that the maximal number of $\mathbb{F}_9$-rational points of the normalization C of such a quintic $V(F)$ is 30. In the following, we list quintic forms F such that $|C(\mathbb{F}_9)| = 30$:

- **(Split node case)** The quintic forms F of the form (5.1) such that the normalization of $V(F) \subset \mathbb{P}^2$ has 30 $\mathbb{F}_9$-rational points are the following:

$$\begin{aligned}
F_1 &= xyz^3 + (x^3 + xy^2 + y^3)z^2 + xy^3z + x^5 + x^3y^2 + x^2y^3 + y^5\,;\\
F_2 &= xyz^3 + (x^3 + 2xy^2 + y^3)z^2 + (2x^2y^2 + 2xy^3)z + x^5 + 2x^4y + x^2y^3 + 2xy^4\\
&\quad + y^5\,;\\
F_3 &= xyz^3 + (x^3 + xy^2 + 2y^3)z^2 + (x^2y^2 + xy^3 + 2y^4)z + x^5 + x^3y^2 + 2x^2y^3\\
&\quad + 2xy^4 + y^5\,;\\
F_4 &= xyz^3 + (x^3 + xy^2 + y^3)z^2 + xy^3z + x^5 + x^3y^2 + 2x^2y^3 + 2y^5;\\
F_5 &= xyz^3 + (x^3 + xy^2 + y^3)z^2 + (2x^2y^2 + xy^3 + y^4)z + x^5 + x^3y^2 + x^2y^3\\
&\quad + 2xy^4 + 2y^5\,;\\
F_6 &= xyz^3 + (x^3 + 2xy^2z^2 + 2y^3)z^2 + (x^2y^2 + 2xy^3)z + x^5 + x^4y + 2x^2y^3\\
&\quad + 2xy^4 + 2y^5\,;\\
F_7 &= xyz^3 + (x^3 + x^2y + y^3)z^2 + (2x^2y^2 + 2xy^3)z + x^5 + 2x^4y + 2x^2y^3 + y^5;\\
F_8 &= xyz^3 + (x^3 + x^2y + 2y^3)z^2 + (2x^2y^2 + 2y^4)z + x^5 + x^4y + xy^4 + y^5\,;\\
F_9 &= xyz^3 + (x^3 + x^2y + y^3)z^2 + (2x^2y^2 + 2y^4)z + 2x^5 + x^3y^2 + 2x^2y^3\\
&\quad + xy^4 + 2y^5\,;\\
F_{10} &= xyz^3 + (x^3 + x^2y + 2xy^2 + 2y^3)z^2 + 2x^2y^2z + x^5 + x^4y + 2xy^4 + 2y^5\,.
\end{aligned}$$

- **(Non-split node case)** The quintic forms F of the form (5.4) – (5.7) such that the normalization of $V(F) \subset \mathbb{P}^2$ has 30 $\mathbb{F}_9$-rational points are the following:

$$\begin{aligned}
F_{11} &= (x^2 - \varepsilon y^2)z^3 + (x(x^2 - \varepsilon y^2) + x^3 + y^3)z^2 + x^2y^2z + 2x^5 + 2x^4y\\
&\quad + x^3y^2 + y^5\,;\\
F_{12} &= (x^2 - \varepsilon y^2)z^3 + (2x(x^2 - \varepsilon y^2) + 2x^3 + y^3)z^2x^2y^2z + x^5 + 2x^4y\\
&\quad + 2x^3y^2 + y^5\,;\\
F_{13} &= (x^2 - \varepsilon y^2)z^3 + (2x(x^2 - \varepsilon y^2) + x^3 + y^3)z^2 + (x^4 + x^3y)z + x^5\\
&\quad + 2x^2y^3 + y^5\,;\\
F_{14} &= (x^2 - \varepsilon y^2)z^3 + (x(x^2 - \varepsilon y^2) + 2x^3 + y^3)z^2 + (x^4 + 2x^3y)z + 2x^5\\
&\quad + 2x^2y^3 + y^5\,;\\
F_{15} &= (x^2 - \varepsilon y^2)z^3 + (x(x^2 - \varepsilon y^2) + y^3)z^2 + (2x^3y + 2x^2y^2)z + x^5 + x^4y\\
&\quad + x^3y^2 + 2x^2y^3 + y^5\,;\\
F_{16} &= (x^2 - \varepsilon y^2)z^3 + (2x(x^2 - \varepsilon y^2) + y^3)z^2 + (x^3y + 2x^2y^2)z + 2x^5 + x^4y\\
&\quad + 2x^3y^2 + 2x^2y^3 + y^5\,;
\end{aligned}$$

$$F_{17} = (x^2 - \varepsilon y^2)z^3 + (x(x^2 - \varepsilon y^2) + 2x^3)z^2 + (x^4 + y^4)z + x^5\,,$$
where $\varepsilon = 2 \in \mathbb{F}_3^\times \smallsetminus (\mathbb{F}_3^\times)^2$.

- **(Cusp case)** The quintic forms F of the form (5.13) such that the normalization of $V(F) \subset \mathbb{P}^2$ has 30 $\mathbb{F}_9$-rational points are the following:

$$\begin{aligned}
F_{18} &= x^2z^3 + (x^2y + y^3)z^2 + (x^4 + 2x^2y^2)z + x^4y + y^5\,;\\
F_{19} &= x^2z^3 + (x^2y + 2y^3)z^2 + (2x^4 + 2x^2y^2) + 2x^4y + 2y^5\,;\\
F_{20} &= x^2z^3 + (x^2y + 2y^3)z^2 + (x^4 + x^3y + 2x^2y^2)z + x^5 + 2x^3y^2 + 2x^2y^3\\
&\quad + xy^4 + 2y^5\,;\\
F_{21} &= x^2z^3 + (x^2y + 2y^3)z^2 + (x^4 + 2x^3y + 2x^2y^2)z + 2x^5 + x^3y^2 + 2x^2y^3\\
&\quad + 2xy^4 + 2y^5\,;\\
F_{22} &= x^2z^3 + (x^3 + x^2y + y^3)z^2 + (2x^3y + 2x^2y^2)z + x^5 + 2x^3y^2 + x^2y^3\\
&\quad + xy^4 + y^5\,.
\end{aligned}$$

For the above 22 curves, we classify their $\mathbb{F}_9$-isomorphism classes, by an algorithm provided in [14, Section 5]. As a result, there are eight $\mathbb{F}_9$-isomorphism classes among them:

(1) F_1, F_4, and F_9; (2) F_2, F_6, and F_8; (3) F_3, F_5, and F_7;
(4) F_{10} and F_{17}; (5) F_{11} and F_{12}; (6) F_{13} and F_{14};
(7) F_{15} and F_{16}; (8) F_{18}, F_{19}, F_{20}, F_{21}, and F_{22}.

The text files `log_trigonal_g5q9_step2.txt` and `log_trigonal_g5q9_step2.txt` are the source code and its log file respectively, and it took within a second to execute the code. □

We also computed the Weil polynomials of the 8 curves by a method described in Remark 4.1.4. At [20], the source code for computing the Weil polynomials and its log file are named `trigonal_g5q9_WeilPoly.txt` and `log_trigonal_g5q9_WeilPoly.txt` respectively at [20], and the time it took to execute the code is about 40 seconds. As a result, we have the following corollary:

COROLLARY 5.2.3. *The Weil polynomials of the eight* $\mathbb{F}_9$*-isomorphism classes* (1)–(8) *given in the proof of Theorem* 5.2.2 *are as follows*:

(1): $(t+3)^4(t^6 + 8t^5 + 44t^4 + 149t^3 + 396t^2 + 648t + 729)$;
(2): $(t^2+5t+9)(t^8+15t^7+112t^6+549t^5+1927t^4+4941t^3+9072t^2+10935t+6561)$;
(3): $t^{10}+20t^9+196t^8+1247t^7+5714t^6+19667t^5+51426t^4+101007t^3+142884t^2+131220t + 59049$;
(4) *and* (8): $(t^2 + 2t + 9)(t^4 + 9t^3 + 37t^2 + 81t + 81)^2$;
(5): $t^{10}+20t^9+200t^8+1299t^7+6030t^6+20843t^5+54270t^4+105219t^3+145800t^2+131220t + 59049$;
(6): $(t+3)^2(t^2 + 5t + 9)(t^6 + 9t^5 + 49t^4 + 177t^3 + 441t^2 + 729t + 729)$;

(7): $t^{10}+20t^9+194t^8+1210t^7+5433t^6+18539t^5+48897t^4+98010t^3+141426t^2+131220t+59049$.

Note that, in general, any two curves over a finite field which are isomorphic to each other have the same Weil polynomials.

6. Conclusions and future works

We proposed algorithms to find/enumerate superelliptic curves C over $\mathbb{F}_q$ such that $|C(\mathbb{F}_{q^r})|$ attains the gonality-point bound. Here is the computational result (see also Table 2 and Example 4.2.2) for the hyperelliptic case with $q = p$ obtained by executing our algorithms:

$g \setminus p^r$	3	5	7	9	11	13	
2	◎	◎	◎	◎	◎	◎	× if $p^r > 13$
3	◎	◎	◎	◎	◎	◎	× if $p^r > 33$
4	◎	◎	◎	◎	?	?	× if $p^r > 61$
5	◎	○	○	◎	○	?	× if $p^r > 97$

Table 3. Hyperlliptic curve $C/\mathbb{F}_p$ with $|C(\mathbb{F}_{p^r})|$ attaining the gonality-point bound.
×: non-existence; ○:existence; ◎: the enumeration is done.

As for trigonal curves, for $g \leq 4$ the existence/non-existence of trigonal curves over $\mathbb{F}_q$ attaining the gonality-point bound is known. When $g = 3$, the condition that the gonality-point bound is less than or equal to the Ihara bound is equivalent to that the gonality is at most 2, whence there is no trigonal curve attaining the gonality-point bound. When $g = 4$, we can read the existence of trigonal curves attaining the gonality-point bound for small q^r from manYPoint site [8], for example it exists for $q^r = 3, 4, 5, 7, 9$. In this paper, we give an algorithm for $g = 5$ and executed it on Magma for $(q, r) = (3, 1), (3, 2)$ to obtain the totality of trigonal genus-5 curves attaining the gonality-point bound for those (q, r). Moreover we determine the isomorphism classes of them with their Weil polynomials.

$g \setminus q^r$	2	3	4	5	7	8	9	11	13
3	×	×	×	×	×	×	×	×	×
4	×	○	○	○	○	×	○	×	×
5	× [3]	○	○ [4]				○		

Table 4. Existence of trigonal curve attaining the gonality-point bound

As future works, we would like to study the following:

(i) The distribution of the number (considered as a function in q, see also Fig. 1 for $g = 2, 3$) of superelliptic curves of $C : y^N = f(x)$ (of the form (3.1) with $a_d = 1$) over $\mathbb{F}_q$ with $\deg f = d$ such that $|C(\mathbb{F}_{q^r})|$ attains the gonality-point bound, for a fixed (N, d, r).

(ii) The existence/enumeration of genus-5 trigonal curves over $\mathbb{F}_q$ attaining the gonality-point bound for larger q.

References

[1] Bosma, W., Cannon, J., Playoust, C. (1997). The Magma algebra system. I. The user language, *Journal of Symbolic Computation* **24**: 235–265. DOI: 10.1006/jsco.1996.0125

[2] Cannon, J., et al. (2016). Magma A Computer Algebra System, School of Mathematics and Statistics, University of Sydney, 2016. http://magma.maths.usyd.edu.au/magma/

[3] Faber, X. and Grantham, J. (2022). Binary Curves of small fixed genus and gonality with many rational points, *J. Algebra* **597**: 24–46.

[4] Faber, X. and Grantham, J. (2021). Ternary and quaternary curves of small fixed genus and gonality with many rational points, *Experimental Mathematics* **32**(2), 337–349. DOI: 10.1080/10586458.2021.1926015

[5] Joachim von zur Gathen and Jürgen Gerhard, Modern computer algebra, 3rd ed., Cambridge University Press, Cambridge, 2013. MR3087522

[6] van der Geer, G. (2001). Curves over finite fields and codes. Casacuberta, Carles (ed.) et al., 3rd European congress of mathematics (ECM), Barcelona, Spain, July 10-14, 2000. Volume II. Basel: Birkhäuser. Prog. Math. **202**, 225–238.

[7] van der Geer, G., van der Vlugt, M. (2000). Tables of curves with many points, *Math. Comp.* **69**, no. 230: 797–810. DOI: 10.1090/S0025-5718-99-01143-6

[8] van der Geer, et al. (2009). Tables of Curves with Many Points, http://www.manypoints.org, Retrieved at 7th August, 2023.

[9] Hartshorne, R. (1997). Algebraic Geometry, *GTM* 52, Springer-Verlag.

[10] Hurt, N. E. (2003). Many Rational Points: Coding Theory and Algebraic Geometry, Kluwer Academic Publishers, Dordrecht.

[11] Ihara, Y. (1981). Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Tokyo* **28**: 721–724.

[12] Kudo, M., Harashita, S (2017). Superspecial curves of genus 4 in small characteristic. Finite Fields Appl. **45**, 131–169 (2017).

[13] Kudo, M., Harashita, S. (2022). Algorithmic study of superspecial hyperelliptic curves over finite fields, *Commentarii Mathematici Universitatis Sancti Pauli*, Vol. **70**, 49–64.

[14] Kudo, M., Harashita, S. (2020). Superspecial trigonal curves of genus 5. *Experimental Mathematics, Published online*: 16 Apr. 2020. DOI: 10.1080/10586458.2020.1723745 (preprint ver: arXiv:1804.11277 [math.AG]).

[15] Kudo, M. and Harashita, S. (2023). Representation of non-special curves of genus 5 as plane sextic curves and its application to finding curves with many rational points. *Journal of Symbolic Computation*, **122**, 15 pages, (DOI) https://doi.org/10.1016/j.jsc.2023.102272

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

[17] Andrade Ramos, C., Garzón Ramos, A. (2010). Polynomials with a restricted range and curves with many points. *Rev. Acad. Colomb. Cienc.* **34**(131): 229–239.

[18] Serre, J.-P. (1985). Rational points on curves over finite fields, Lectures given at Harvard University. Notes by Fernando Q. Gouvéa.

[19] Vermeulen, F. (2021): Curves of fixed gonality with many rational points. arXiv:2102.00900v3.

[20] Computation programs and log files for the paper "Genus-five hyperelliptic or trigonal curves with many rational points in characteristic three", available on the web page: https://sites.google.com/view/m-kudo-official-website/english/code/genus5-many-points

E-mail address of the first author: m-kudo@fit.ac.jp
E-mail address of the second author: harasita@ynu.ac.jp