Point counting on curves using a gonality preserving lift

Wouter Castryck and Jan Tuitman

March 9, 2016

Abstract

We study the problem of lifting curves from finite fields to number fields in a genus and gonality preserving way. In particular, we show how this can be done efficiently for curves of gonality at most four over finite fields of odd characteristic. We then use such a lift as input to an algorithm due to the second author for computing zeta functions of curves over finite fields using p-adic cohomology.

Contents

1 Introduction **2**

2 Background **5**
2.1 First facts on the gonality 5
2.2 Baker's bound 6
2.3 Preliminary discussion 8

3 Curves of low genus **9**
3.1 Curves of genus three 9
3.2 Curves of genus four 13
3.3 Curves of genus five 22

4 Rational normal scrolls **35**
4.1 Scroll associated to a map to $\mathbb{P}^1$ 35
4.2 Lie algebra method 35

5 Curves of low gonality **35**
5.1 Trigonal curves 35
5.2 Tetragonal curves 35

6 Conclusions **35**

1 Introduction

This article is about efficiently lifting algebraic curves over finite fields to characteristic zero, in a genus and gonality preserving way. Throughout, our curves are always understood to be geometrically irreducible, but not necessarily non-singular and/or complete. By the genus of a curve we mean its geometric genus, unless otherwise stated. As for the gonality of a curve over a field k, we make a distinction between two notions: by its *k-gonality* we mean the minimal degree of a non-constant k-rational map to the projective line, while by its *geometric gonality* we mean the $\bar{k}$-gonality, where $\bar{k}$ denotes an algebraic closure of k. We also make a notational distinction between projective, affine or toric (= affine minus coordinate hyperplanes) n-space in characteristic zero, in which case we write $\mathbf{P}^n, \mathbf{A}^n, \mathbf{T}^n$, and their finite characteristic counterparts, where we opt for $\mathbb{P}^n, \mathbb{A}^n, \mathbb{T}^n$. Apart from that we avoid reference to the base field, which should always be clear from the context. Similarly we write $\mathbf{Q}$ for the field of rational numbers, and $\mathbb{F}_q$ for the finite field with q elements, where $q = p^a$ is a power of a prime number p. For each such q we fix a degree a extension $K \supset \mathbf{Q}$ in which p is inert, and let $\mathcal{O}_K$ be its ring of integers. We then identify $\mathbb{F}_q$ with the residue field $\mathcal{O}_K/(p)$. Our lifting problem is as follows:

Problem 1. *Given a curve $\overline{C}$ over $\mathbb{F}_q$, find an efficient algorithmic way of producing a polynomial $f \in \mathcal{O}_K[x, y]$ such that*

(i) its reduction mod p defines a curve that is birationally equivalent to $\overline{C}$,

(ii) the curve $C \subset \mathbf{A}^2$ it defines has the same genus as $\overline{C}$,

(iii) its degree in y equals the $\mathbb{F}_q$-gonality of $\overline{C}$.

Note that these conditions imply that the K-gonality of C equals the $\mathbb{F}_q$-gonality of $\overline{C}$, because the gonality cannot increase under reduction mod p; see e.g. [18, Thm. 2.5]. We do not know whether an f satisfying (i-iii) exists in general. Grothendieck's existence theorem [32] implies that in theory one can achieve (i) and (ii) over the ring of integers $\mathbf{Z}_q$ of the p-adic completion $\mathbf{Q}_q$ of K, but first it is not clear that we can always take f to be defined over $\mathcal{O}_K$ and second we do not know whether it is always possible to incorporate (iii), let alone in an effective way. However, we will take a more practical approach to the problem and construct a lift f satisfying (i-iii) in some interesting special cases.

perhaps a bit more detail on which special cases?

We are intentionally vague about what it means to be *given* a curve $\overline{C}$ over $\mathbb{F}_q$. It could mean that we are considering the affine plane curve defined by a given absolutely irreducible polynomial $\overline{f} \in \mathbb{F}_q[x, y]$. Or it could mean that we are considering the affine/projective curve defined by a given more general system of equations over $\mathbb{F}_q$. But in all cases we will ignore the cost of computing the genus g of $\overline{C}$. Moreover, in case $g = 0$ we assume that it is easy to realize $\overline{C}$ as a plane conic (using the anticanonical embedding) and if $g = 1$ we ignore the cost of finding a plane Weierstrass model. By the Hasse-Weil bound every genus one curve over $\mathbb{F}_q$ is elliptic, so this is indeed possible. If $g \geq 2$ then we assume that one can easily decide whether $\overline{C}$ is hyperelliptic or not (note that over finite fields, curves are hyperelliptic iff they are geometrically hyperelliptic, so there is no ambiguity here; see Section 2.3). If it is then we suppose that it is easy to

find a generalized Weierstrass model. If not then it is assumed that one can effectively compute a canonical map

$$\kappa : \overline{C} \to \mathbb{P}^{g-1}$$

along with a minimal set of generators for the ideal of its image. The latter will usually be our starting point. Each of the foregoing tasks is tantamount to computing certain Riemann-Roch spaces. There is extensive literature on this functionality, which has been implemented in several computer algebra packages, such as Magma [5]. We refer to [28] for background on how Riemann-Roch computations are done.

The idea is then to use the output polynomial f as input to a recent algorithm due to the second author [49, 50] for computing the Hasse-Weil zeta function of $\overline{C}$. This algorithm uses p-adic cohomology, which it represents through the map $\varphi : C \to \mathbf{P}^1 : (x, y) \mapsto x$. The algorithm only works if C and φ have appropriate reduction modulo p, in a rather subtle sense for the precise description of which we refer to [50, Ass. 1]. This condition is needed to be able to apply a comparison theorem between the (relative) p-adic cohomology of $\overline{C}$ and the (relative) de Rham cohomology of $C \otimes \mathbf{Q}_q$, which is where the actual computations are done. For such a theorem to hold, by dimension arguments it is necessary that C and $\overline{C}$ have the same genus, whence our condition (ii). This may be insufficient, in which case f will be rejected, but for $p > 2$ our experiments show that this is rarely a concern as soon as q is sufficiently large. Moreover, in many cases below, our construction leaves enough freedom to retry in the event of a failure.

The algorithm from [49, 50] has a running time that is sextic in $\deg \varphi$, which equals the degree in y of f, so it is important to keep this value within reason. Because the $\mathbb{F}_q$-gonality of $\overline{C}$ is an innate lower bound, it is natural to try to meet this value, whence our condition (iii). At the benefit of other parameters affecting the complexity, one could imagine it being useful to allow input polynomials whose degree in y exceeds the $\mathbb{F}_q$-gonality of $\overline{C}$, but in all cases that we studied the best performance results were indeed obtained using a gonality-preserving lift. At the same time, looking for such a lift is a theoretically neat problem. (Increasing the degree in y is potentially useful for dealing with curves for which [50, Ass. 1] is violated, though.)

Remark 2. For the purpose of point counting, it is natural to wonder why we lift to $\mathcal{O}_K$, and not to the ring $\mathbf{Z}_q$, which is a priori easier. In fact, most computations in the algorithm from [49, 50] are carried out to some finite p-adic precision N, so it would even be sufficient to lift to $\mathcal{O}_K/(p^N) = \mathbf{Z}_q/(p^N)$. The reason for lifting to $\mathcal{O}_K$ is that at the start of the algorithm some integral bases have to be computed in the function field of the curve. Over a number field K this is standard and implemented in Magma, but to finite p-adic precision no implementation seems to be available. Therefore, the integral bases are currently computed to exact precision, and we need f to be defined over $\mathcal{O}_K$.

In Section 2 we review some basic/known facts on the gonality. This will reduce our study to the case of non-hyperelliptic curves of genus $g \geq 3$. Recall that being non-hyperelliptic is synonymous to having $\mathbb{F}_q$-gonality different from 2. The main contribution of this article is a solution to Problem 1 for curves of $\mathbb{F}_q$-gonality three and four over finite fields $\mathbb{F}_q$ of odd characteristic. Such curves will be called trigonal and tetragonal, respectively.

Because of their practical relevance, we first provide a separate and rather extensive treatment of curves having low genus; this is done in Section 3. For this we rely on the language of Newton polygons and Baker's genus bound, which is recalled in Section 2.2 below. In Sections 3.1, 3.2 and 3.3 we attack Problem 1 for curves of genus 3, 4 and 5, respectively. Each of these sections is organized in a stand-alone way, as follows:

- In a first part we classify curves by their $\mathbb{F}_q$-gonality γ, and solve Problem 1 in its basic version. If the reader is interested in such a basic solution only, he/she can skip the other parts.
- Next, in an optimization part we take into account the fact that the actual input to the algorithm from [49, 50] must be monic when considered as a polynomial in y. This is easily achieved: if we write

$$f = f_0(x)y^\gamma + f_1(x)y^{\gamma-1} + \cdots + f_{\gamma-1}(x)y + f_\gamma(x),$$

  then the birational transformation $y \leftarrow y/f_0(x)$ gives

$$y^\gamma + f_1(x)y^{\gamma-1} + \cdots + f_{\gamma-1}(x)f_0(x)^{\gamma-2}y + f_\gamma(x)f_0(x)^{\gamma-1}, \tag{1}$$

  which still satisfies (i), (ii) and (iii). But one sees that the degree in x inflates, and this affects the running time. We discuss how our basic solution to Problem 1 can be enhanced such that (1) becomes a more compact expression.
- In a third part we report on an implementation of our method, and on how it performs in composition with the algorithm from [49, 50] for computing Hasse-Weil zeta functions.

As we will see, the case of trigonal curves of genus 5 provides a natural transition to the study of general trigonal and tetragonal curves.

This is done from Section 4 on. At a high level our method can be described as follows. We first realize the input curve as a smooth complete intersection of $n-1$ hypersurfaces in a rational normal scroll of dimension $n = \gamma - 1$. On a dense torus $\mathbb{T}^n$ inside this scroll, these hypersurfaces are defined by Laurent polynomials $\overline{f}_1, \ldots, \overline{f}_{n-1} \in \mathbb{F}_q[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$. We then naively lift these Laurent polynomials to $f_1, \ldots, f_{n-1} \in \mathcal{O}_K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$, where 'naively' means that the only restriction is that zero terms should not lift to non-zero terms. We show that these lifted polynomials again define a smooth complete intersection in $\mathbf{T}^n$, having the right genus and K-gonality. Finally we appropriately project to $\mathbf{A}^2$ in order to obtain a defining polynomial of the requested form. One of our main tasks turns out to be the effective recognition of a dense torus $\mathbb{T}^n$ inside the scroll, so that we can find the Laurent polynomials $\overline{f}_1, \ldots, \overline{f}_{n-1}$. For this we develop a finite field version of the Lie algebra method due to de Graaf, Harrison, Pílniková and J. Schicho [15]; this is done in Section 4.2. Then in Section 5 we elaborate the above ideas in detail and describe how to solve Problem 1 for trigonal and tetragonal curves. Here again, we report on an implementation and we discuss the implications for point counting, along with concrete runtimes and success ratios. But we spend less effort on optimizing the output. In Section 6 we conclude with some possibilities for future research.

The main implication of our work is that computing Hasse-Weil zeta functions using p-adic cohomology has now become practical on virtually all curves of genus at most five and/or $\mathbb{F}_q$-gonality at most four over finite fields $\mathbb{F}_q$ of (small) odd characteristic. We stress that such curves cannot be tackled using any of the previous Kedlaya-style point counting algorithms, that were designed to deal with elliptic curves [41], hyperelliptic curves [16, 25, 27, 31, 33], superelliptic curves [23, 36], C_{ab} curves [10, 17, 52] and nondegenerate curves [9, 51], in increasing order of generality. In terms of moduli the locus of the latter has dimension $\min\{3g-3, 2g+1\}$ as soon as $g \geq 2$, except for $g = 7$ where the dimension reads $2g + 2$. On the other hand the space of curves of geometric gonality at most four has dimension $2g + 3$ by [?].

referentie zoeken

2 Background

2.1 First facts on the gonality

Let k be a field and let C be a curve over k. The geometric gonality of C is a classical invariant. It is 1 if and only if the genus of C equals $g = 0$, while for curves of genus $g \geq 1$, by Brill-Noether theory the geometric gonality γ lies in the range

$$2, \ldots, \lceil g/2 \rceil + 1.$$

All of these values of γ can occur: inside the moduli space of curves of genus $g \geq 2$ the corresponding locus has dimension $\min\{2g - 5 + 2\gamma, 3g - 3\}$. In particular, for a generic curve the Brill-Noether upper bound $\lceil g/2 \rceil + 1$ is met. From a practical point of view, determining the geometric gonality of a given curve is usually a non-trivial computational task, although in theory it can be computed using so-called scrollar syzygies [42].

In the arithmetic (= non-geometric) case the gonality has seen much less study, even for classical fields such as the reals [13]. Of course the geometric gonality is always less than or equal to the k-gonality, but the inequality may be strict. In particular the Brill-Noether upper bound $\lceil g/2 \rceil + 1$ is no longer valid. For curves of genus $g = 1$ over certain fields k, the k-gonality γ can even be arbitrarily large [12]. As for the other genera, using the canonical or anticanonical linear system one finds

- if $g = 0$ then $\gamma \leq 2$,
- if $g \geq 2$ then $\gamma \leq 2g - 2$.

These bounds can be met. We refer to [39, Prop. 1.1] and the references therein for precise statements, along with some additional first facts.

If $k = K$ is a number field then the notion of K-gonality has enjoyed more attention, both from a computational [18, 19] and a theoretical [1, 39] point of view, especially in the case where C is a modular curve. This is due to potential applications towards effective versions of the uniform boundedness conjecture; see [46] for an overview. In the non-modular case not much literature seems available, but our rash guess would be that almost all (in any honest sense) curves of genus $g \geq 2$ over K meet the upper bound

$\gamma = 2g - 2$. This is somewhat supported by the Franchetta conjecture; see again [39, Prop. 1.1] and the references therein for a more extended discussion.

Over finite fields $k = \mathbb{F}_q$ the notion has attracted the attention of coding theorists, in the context of Goppa codes [38, 48]. They proved the following result:

Lemma 3. *If the $\overline{C}$ is a curve over a finite field $\mathbb{F}_q$ then its $\mathbb{F}_q$-gonality is at most $g+1$. Moreover, if equality holds then $g \leq 10$ and $q \leq 31$.*

Proof. See [48, §4.2]. □

In [48, §4.2] it is stated as an open problem to find tighter bounds for the $\mathbb{F}_q$-gonality. In fact we expect the sharpest possible upper bound to be $\lceil g/2 \rceil + 1 + \varepsilon$ for some small ε; maybe $\varepsilon \leq 1$ is sufficient as soon as q is large enough. Indeed for schemes over finite fields, such as the Brill-Noether loci of $\overline{C}$, it is easy to acquire rational points, a fact which contrasts with the number field case. A byproduct of this paper is a detailed understanding of which $\mathbb{F}_q$-gonalities can occur for curves of genus at most five, in the cases where q is odd (the cases where q is even should be analyzable in a similar way). The following table summarizes this.

g	Brill-Noether upper bound	possible $\mathbb{F}_q$-gonalities (union over all odd q)	possible $\mathbb{F}_q$-gonalities (for a given odd $q > B$)	B
0	1	1	1	1
1	2	2	2	1
2	2	2	2	1
3	3	2, 3, 4	2, 3	29
4	3	2, 3, 4, 5	2, 3, 4	7
5	4	2, 3, 4, 5, 6	2, 3, 4, 5	3

For proofs we refer to Section 2.3 (for $g \leq 2$), Lemma 5 (for $g = 3$), Lemma 8 (for $g = 4$), and Lemma 14 and Remark 16 (for $g = 5$).

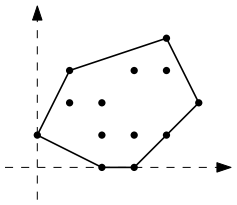
2.2 Baker's bound

Throughout a large part of this paper we will use the convenient language of Newton polygons. Let

$$f = \sum_{(i,j) \in \mathbf{Z}^2_{\geq 0}} c_{i,j} x^i y^j \in k[x, y]$$

be an irreducible polynomial over a field k. Then its Newton polygon is

$$\Delta(f) = \operatorname{conv} \left\{ (i, j) \in \mathbf{Z}^2_{\geq 0} \;\middle|\; c_{i,j} \neq 0 \right\}$$



(convex hull in $\mathbf{R}^2$). Note that $\Delta(f)$ lies in the first quadrant and meets the coordinate axes in at least one point each, by the irreducibility of f. Let C be the affine curve that is cut out by f. Then one has the following bounds on the genus and the gonality of C, purely in terms of the combinatorics of $\Delta(f)$:

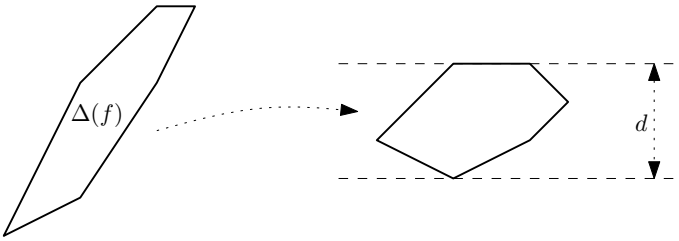
- The genus of C is at most *the number of points in the interior* of $\Delta(f)$ having integer coordinates: this is Baker's theorem. See [4, Thm. 2.4] for an elementary proof and [14, §10.5] for a more conceptual version (using adjunction theory on toric surfaces).

  If one fixes the Newton polygon, then Baker's bound on the genus is generically attained, i.e. meeting the bound is a non-empty Zariski-open condition; this result is essentially due to Khovanskii [34]. An explicit sufficient generic condition is that f is nondegenerate with respect to its Newton polygon [9, Prop. 2.3, Cor. 2.8].

- The k-gonality is at most the *lattice width* $\mathrm{lw}(\Delta(f))$ of $\Delta(f)$. By definition, this is the minimal height d of a horizontal strip

$$\left\{ (a,b) \in \mathbf{R}^2 \;\middle|\; 0 \le b \le d \right\}$$

  inside which $\Delta(f)$ can be mapped using a unimodular transformation, i.e. an affine transformation of $\mathbf{R}^2$ with linear part in $\mathrm{GL}_2(\mathbf{Z})$ and translation part in $\mathbf{Z}^2$.



  This is discussed in [6, §2], but in brief the argument goes as follows. By applying the same transformation to the exponents (which is a k-rational birational change of variables), our polynomial f can be transformed along with its Newton polygon. When orienting f in this way one obtains $\deg_y f = \mathrm{lw}(\Delta(f))$, and the gonality bound follows by considering the k-rational map $(x,y) \mapsto x$.

  Of course then also the geometric gonality of C is bounded by $\mathrm{lw}(\Delta(f))$. If a unimodular transformation can be used to transform $\Delta(f)$ into

$$2\Upsilon := \mathrm{conv}\{(-2,-2),(2,0),(0,2)\} \quad \text{or} \quad d\Sigma := \mathrm{conv}\{(0,0),(d,0),(0,d)\} \text{ for } d \ge 2$$

  then the geometric gonality enjoys the sharper bound $\mathrm{lw}(\Delta(f)) - 1$ (amounting to 3 resp. $d-1$); see [6, Thm. 3]. If one fixes the Newton polygon and if $\mathrm{char}\, k = 0$, then the sharpest applicable foregoing bound on the geometric gonality is generically met, and again nondegeneracy is a sufficient condition [8, Cor. 6.2]. In fact, the slightly weaker condition of meeting Baker's genus bound is already sufficient [8, §4].

  Summing up, if $\mathrm{char}\, k = 0$ and we are not in the exceptional cases $2\Upsilon, d\Sigma$ $(d \ge 2)$ then meeting Baker's bound is sufficient for the k-gonality to equal $\mathrm{lw}(\Delta(f))$. In the exceptional cases the k-gonality is either $\mathrm{lw}(\Delta(f))$ or $\mathrm{lw}(\Delta(f)) - 1$. If $\mathrm{char}\, k > 0$ then these statements are probably true as well; e.g. for hyperelliptic and trigonal curves a working proof can be found in [6, §5]. But the general results of [8] have been proven in characteristic 0 only.

Baker's bound (and the fact that it is generically attained) yields a large class of defining polynomials $\overline{f} \in \mathbb{F}_q[x,y]$ for which finding an $f \in \mathcal{O}_K[x,y]$ satisfying (i) and (ii) is easy. Indeed, by lower semi-continuity the genus cannot increase under reduction modulo p. Therefore if $\overline{f}$ attains Baker's upper bound on the genus, then it suffices to pick any $f \in \mathcal{O}_K[x,y]$ that reduces to $\overline{f}$ mod p, in such a way that $\Delta(f) = \Delta(\overline{f})$: then the corresponding curve C/K necessarily attains Baker's upper bound, too.

Moreover, we expect that this construction usually takes care of (iii) at once. Indeed, if Baker's bound is met and we are not in the exceptional cases 2Υ and $d\Sigma$ ($d \geq 2$), then from the above discussion we know that the K-gonality of C is $\mathrm{lw}(\Delta(f)) = \mathrm{lw}(\Delta(\overline{f}))$. As mentioned, we believe that this generically (or even always) matches with the $\mathbb{F}_q$-gonality γ of $\overline{C}$, even though we recall that this is unproven in general. If things work out properly, then a unimodular transformation ensures that $\deg_y f = \mathrm{lw}(\Delta(f)) = \gamma$, as desired. Such a transformation is computationally easy to find [21].

It is therefore justifiable to say that conditions (i), (ii) and probably (iii) are easy to deal with for almost all polynomials $\overline{f} \in \mathbb{F}_q[x,y]$. But be cautious: this does not mean that almost all *curves* $\overline{C}/\mathbb{F}_q$ are defined by such a polynomial. In terms of moduli, the locus of curves for which this is true has dimension $2g+1$, except if $g = 7$ where it is 16; see [11, Thm. 12.1]. Recall that the moduli space of curves of genus g has dimension $3g-3$, so as soon as $g \geq 5$ the defining polynomial $\overline{f}$ of a plane model of a generic curve $\overline{C}/\mathbb{F}_q$ of genus g can never attain Baker's bound. For such curves, the foregoing discussion becomes counterproductive: if we take a naive coefficient-wise lift $f \in \mathcal{O}_K[x,y]$ of $\overline{f}$, then it is very likely to satisfy Baker's bound, causing an increase of genus. This shows that f has to be constructed with more care, which is somehow the main point of this article.

2.3 Preliminary discussion

We will attack Problem 1 in the cases where the genus g of $\overline{C}$ is at most five (in Section 3) and/or the $\mathbb{F}_q$-gonality γ of $\overline{C}$ is at most four (in Section 5), where we recall our overall assumption that q is odd. Note that for the purpose of computing the Hasse-Weil zeta function the characteristic p of $\mathbb{F}_q$ should be small: this restriction is common to all p-adic point counting algorithms. We will occasionally extrapolate a statement from the literature that is available in characteristic 0 only: this mainly applies to the theory of genus five curves due to Arbarello, Cornalba, Griffiths and Harris [2, VI.§4.F], and to some statements on tetragonal curves due to Schreyer [44]. But we will always be explicit about this.

op het einde nog eens allemaal checken

Note that if $\overline{C}$ is a curve of genus $g = 0$ then $\overline{C} \cong \mathbb{P}^1$, because every plane conic carries at least one $\mathbb{F}_q$-point, and projection from that point gives an isomorphism to the line. In particular $\gamma = 1$ if and only if $g = 0$, in which case Problem 1 can be addressed by simply outputting $f = y$.

Next, if $g = 1$ then we assume that $\overline{C}$ is defined by a polynomial $\overline{f} \in \mathbb{F}_q[x,y]$ in Weierstrass form. In this case $\gamma = 2$, and any $f \in \mathcal{O}_K[x,y]$ for which $\Delta(f) = \Delta(\overline{f})$ will address Problem 1 (for instance because Baker's bound is attained, or because a non-zero discriminant must lift to a non-zero discriminant).

Finally, if $g \geq 2$ then $\overline{C}$ is geometrically hyperelliptic if and only if κ realizes $\overline{C}$ as

a degree 2 cover of a curve of genus zero [26, IV.5.2-3]. By the foregoing discussion the latter is isomorphic to $\mathbb{P}^1$, and therefore every geometrically hyperelliptic curve $\overline{C}/\mathbb{F}_q$ admits an $\mathbb{F}_q$-rational degree 2 map to $\mathbb{P}^1$. In particular, one can unambiguously talk about hyperelliptic curves over $\mathbb{F}_q$. In this case it is standard how to produce a defining polynomial $\overline{f} \in \mathbb{F}_q[x,y]$ that is in Weierstrass form. Then again any $f \in \mathcal{O}_K[x,y]$ for which $\Delta(f) = \Delta(\overline{f})$ will address Problem 1.

Remark 4. Let g^1_d be a complete base-point free $\mathbb{F}_q$-rational linear pencil on a non-singular projective curve $\overline{C}/\mathbb{F}_q$. Then from standard arguments in Galois cohomology (that are specific to finite fields) it follows that this g^1_d automatically contains an $\mathbb{F}_q$-rational effective divisor, which can be used to construct an $\mathbb{F}_q$-rational map to $\mathbb{P}^1$ of degree d. See for instance the proof of [24, Lem. 6.5.3]. This gives another way of seeing that a geometrically hyperelliptic curve over $\mathbb{F}_q$ is automatically $\mathbb{F}_q$-hyperelliptic, because the hyperelliptic pencil g^1_2 is unique, hence indeed defined over $\mathbb{F}_q$. The advantage of this argument is that it is more flexible: for instance it also shows that a geometrically trigonal curve $\overline{C}/\mathbb{F}_q$ of genus $g \geq 5$ always admits an $\mathbb{F}_q$-rational degree 3 map to $\mathbb{P}^1$, again because the g^1_3 on such a curve is unique. So we can unambiguously talk about trigonal curves from genus five on.

Summing up, throughout the paper, it suffices to consider curves of $\mathbb{F}_q$-gonality $\gamma > 2$, so that the canonical map κ is an embedding. In particular we have $g \geq 3$. From the point counting viewpoint, all omitted cases are covered by the algorithms of Satoh [41] and Kedlaya [25, 33].

3 Curves of low genus

3.1 Curves of genus three

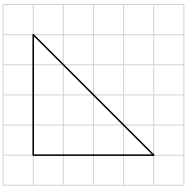
3.1.1 Lifting curves of genus three

Solving Problem 1 in genus three in its basic version is not hard, so we consider this as a warm-up discussion. We first analyze which $\mathbb{F}_q$-gonalities can occur:

Lemma 5. *Let $\overline{C}/\mathbb{F}_q$ be a non-hyperelliptic curve of genus 3 and $\mathbb{F}_q$-gonality γ, and assume that q is odd. If $\#\overline{C}(\mathbb{F}_q) = 0$ then $\gamma = 4$, while if $\#\overline{C}(\mathbb{F}_q) > 0$ (which is guaranteed if $q > 29$) then $\gamma = 3$.*

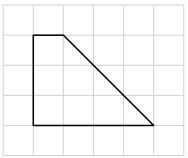
Proof. Using the canonical embedding we can assume that $\overline{C}$ is a smooth plane quartic. It is classical that such curves have geometric gonality 3, and that each gonal map arises as projection from a point on the curve. For a proof see [45, Prop. 3.13], where things are formulated in characteristic zero, but the same argument works in positive characteristic; alternatively one can consult [29]. In particular if there is no $\mathbb{F}_q$-point then there is no rational gonal map and $\gamma > 3$. But then a degree 4 map can be found by projection from an $\mathbb{F}_q$-point outside the curve. By [30, Thm. 3(2)] there exist pointless non-hyperelliptic curves of genus three over $\mathbb{F}_q$ if and only if $q \leq 23$ or $q = 29$. □

We can now address Problem 1 as follows. As in the proof we assume that $\overline{C}$ is given as a smooth plane quartic. First suppose that $\#\overline{C}(\mathbb{F}_q) = 0$. Because this is possible for $q \leq 29$ only, the occurrence of this event can be verified exhaustively. In this case the Newton polygon of the defining polynomial $\overline{f} \in \mathbb{F}_q[x, y]$ of the affine part of $\overline{C}$ equals:



$(\Delta_3^{0,0})$

In particular Baker's bound is attained, and a naive Newton polygon preserving lift $f \in \mathcal{O}_K[x, y]$ automatically addresses (i), (ii) and (iii). If $\#\overline{C}(\mathbb{F}_q) > 0$ then one picks a random $\mathbb{F}_q$-point P (which can be found quickly) and one applies a projective transformation that maps P to $(0 : 1 : 0)$. After doing so the Newton polygon of $\overline{f} \in \mathbb{F}_q[x, y]$ becomes contained in (and typically equals)



$(\Delta_3^{1,0})$

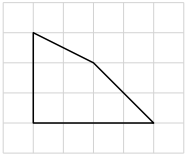
Again Baker's bound is attained, and a naive Newton polygon preserving lift $f \in \mathcal{O}_K[x, y]$ satisfies (i), (ii) and (iii).

It is important to transform the curve *before* lifting to characteristic 0. Indeed, if one would immediately lift our input quartic to a curve $C \subset \mathbf{P}^2$ then it is highly likely that $C(K) = \emptyset$, and therefore that the K-gonality equals 4 (by the same proof as above). This type of reasoning plays an important role throughout the paper, often in a more subtle way than here.

Remark 6. The indices i, j in $\Delta_3^{i,j}$ refer to the multiplicities of intersection of $\overline{C}$ with the line at infinity at the coordinate points $(0 : 1 : 0)$ and $(1 : 0 : 0)$, assuming that it is defined by a polynomial having Newton polygon $\Delta_3^{i,j}$.

3.1.2 Optimizations

For point counting purposes we can of course assume that $q > 29$, so that $\gamma = 3$. By applying (1) to a polynomial with Newton polygon $\Delta_3^{1,0}$ one ends up with a polynomial that is monic in y and that has degree $4 + (\gamma - 1) = 6$ in x. This can be improved: in addition to mapping P to $(0 : 1 : 0)$, we can have its tangent line $T_P(\overline{C})$ sent to the line at infinity. If we then lift $\overline{f}$ to $\mathcal{O}_K[x, y]$ we find an f whose Newton polygon is contained in (and typically equals)



$(\Delta_3^{2,0})$

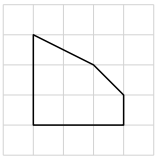
Algorithm 1 Lifting curves of genus 3: basic solution

Input non-hyperelliptic genus 3 curve $\overline{C}$ over $\mathbb{F}_q$

Output lift $f \in \mathcal{O}_K[x, y]$ satisfying (i), (ii), (iii) that is supported
- on $\Delta_3^{0,0}$ if $\overline{C}(\mathbb{F}_q) = \emptyset$, or else
- on $\Delta_3^{2,0}$

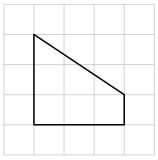
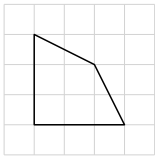
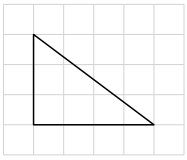
1: $\overline{C} \leftarrow \text{CanonicalImage}(\overline{C})$ in $\mathbb{P}^2 = \text{Proj}\,\mathbb{F}_q[X, Y, Z]$;
2: **if** $q > 29$ or $\overline{C}(\mathbb{F}_q) \neq \emptyset$ (verified exhaustively) **then**
3: $P := \text{Random}(\overline{C}(\mathbb{F}_q))$
4: apply automorphism of $\mathbb{P}^2$ transforming $T_P(\overline{C})$ into $Z = 0$
5: and P into $(0 : 1 : 0)$
6: **return** NaiveLift(Dehomogenization$_Z$(DefiningPolynomial($\overline{C}$)))

In particular f is monic (up to a scalar) and $\deg_x f \leq 4$. We can in fact achieve $\deg_x f = 3$ in all cases of practical interest. Indeed, with an asymptotic chance of 50% our tangent line $T_P(\overline{C})$ intersects $\overline{C}$ in two other rational points. The above construction leaves enough freedom to position one of those points Q at $(1 : 0 : 0)$. The resulting lift f then becomes contained in (and typically equals)

 $(\Delta_3^{2,1})$

In case of failure we retry with another P. If $q > 59$ (say) then there are enough $\mathbb{F}_q$-points $P \in \overline{C}$ for this approach to work with near certainty, although there might exist sporadic counterexamples well beyond that point.

Remark 7. For large values of q one might want to pursue a further compactification of the Newton polygon. Namely, if one manages to choose $P \in \overline{C}(\mathbb{F}_q)$ such that it is an ordinary flex or such that $T_P(\overline{C})$ is a bitangent, then $T_P(\overline{C})$ meets $\overline{C}$ in a unique other point Q, which is necessarily defined over $\mathbb{F}_q$. By proceeding as before one respectively ends up inside the first or second polygon below. If one manages to let $P \in \overline{C}(\mathbb{F}_q)$ be a non-ordinary flex, i.e. a hyperflex, then positioning it at $(0 : 1 : 0)$ results in a polygon of the third form.

 $(\Delta_3^{3,1})$  $(\Delta_3^{2,2})$  $(\Delta_3^{4,0})$

Finding an ordinary flex (resp. a hyperflex) amounts to finding a non-singular $\mathbb{F}_q$-point (resp. a singular $\mathbb{F}_q$-point) on the subscheme of flexes, which is cut out by the Hessian if $3 \nmid q$. Typically this subscheme is zero-dimensional of degree 24, and we heuristically expect the probability of it having a non-singular $\mathbb{F}_q$-point (resp. a singular $\mathbb{F}_q$-point) to

be comparable to that of a univariate degree 24 polynomial over $\mathbb{F}_q$ having a rational root (resp. a rational double root). This is known to converge to $1/2!-1/3!+1/4!-\cdots+1/24! \approx 1-1/e \approx 63.2\%$ (resp. 0%) as $q \to \infty$ by [37, Ex. 11.2.28]. On the other hand, one can find a bitangent that intersects $\overline{C}$ in two $\mathbb{F}_q$-points P and Q as soon as one of the 28 nodes of the dual curve is rational and has rational branches. We heuristically expect the probability of this event to be comparable to that of a univariate degree 28 polynomial over $\mathbb{F}_q$ having a rational root that is a square. This converges to about $1-1/\sqrt{e} \approx 39.4\%$ by an argument similar to that in [37, Ex. 11.2.28]. Assuming independence of events, we expect $\Delta_3^{3,1}$ or $\Delta_3^{2,2}$ to be attainable for roughly $1-1/e^{3/2} \approx 77.7\%$ of all smooth plane quartics, as is confirmed by experiment. In contrast the hyperflex case $\Delta_3^{4,0}$ is very exceptional, but we included it in the discussion because it corresponds to the well-known class of $C_{3,4}$ curves: even though $\deg_x f = 4$ here, the corresponding point count is slightly faster.

3.1.3 Implementation and timings

We have implemented the algorithms from this paper in the computer algebra system MAGMA. The resulting package is called `goodmodels` and can be found at the webpage http://perswww.kuleuven.be/jan_tuitman. The code for prime fields $\mathbb{F}_p$ is loaded as follows:

```
load "goodmodels_p.m";
```

Note that the package `pcc_p` from [49, 50], that we use for computing the zeta function, comes with `goodmodels` and is automatically loaded.

As an example, we generate a random quartic `f` in 3 variables over the finite field $\mathbb{F}_{97}$ and compute the best lift `Q` to characteristic 0 of some model of the corresponding curve using the methods explained above (including all the optimisations).

```
p:=97;
f:=random_genus3(p);
Q:=optimal_model_genus3(f);
```

Now we compute the numerator of the zeta function of the curve defined by `f` by calling the function `num_zeta` from `pcc_p`:

```
chi:=num_zeta(Q,p);
```

Note that the denominator of the zeta function of a curve is always `(1-T)(1-pT)`, so the zeta function can easily deduced from its numerator `chi`. To repeat this example over the non prime field $\mathbb{F}_{3^{10}}$, the commands are as follows:

```
load "goodmodels_q.m";
q:=3^10;
f:=random_genus3(q);
Q:=optimal_model_genus3(f);
chi:=num_zeta(Q,q);
```

Alternatively, in both examples we can compute the zeta function of the curve defined by `f` using a single command:

```
zeta:=zeta_genus3(f);
```

The three tables below contain timings and memory usage for various values of p and $q = p^n$. All computations were carried out with MAGMA V2.21-8 using a single core on an i7-4910MQ CPU running at 2.90GHz. The code used to generate the tables can be found in the subdirectory `./profiling` of `goodmodels`.

The first column in each table contains the time used by `optimal_model_genus3`, i.e. to compute the lift `Q` to characteristic 0 averaged over 1000 random examples. Then the second column gives the time used by the point counting code `pcc` averaged over at least 10 different examples. Next, the third column contains the total memory used in the computation. Finally, the last column gives the number of examples out of the 1000 where we did not find a lift satisfying [50, Ass. 1], which each time turned out to be 0, i.e. we always found a good lift.

p	time lift(s)	time pcc(s)	space (Mb)	fails /1000
11	0.3	0.3	32	0
67	0.3	0.9	32	0
521	0.3	7.4	32	0
4099	0.3	69	124	0
32771	0.3	763	956	0

q	time lift(s)	time pcc(s)	space (Mb)	fails /1000
3^5	0.4	4.7	32	0
7^5	0.4	11	32	0
17^5	0.4	23	64	0
37^5	0.4	53	76	0
79^5	0.4	124	124	0

q	time lift(s)	time pcc(s)	space (Mb)	fails /1000
3^{10}	0.5	34	64	0
7^{10}	0.6	67	76	0
17^{10}	0.7	188	124	0
37^{10}	0.7	347	241	0
79^{10}	0.8	1048	500	0

Alternatively, without using the methods from this section, we can just make the plane quartic `f` monic using (1), then lift naively to characteristic 0 and try to use this lift `Q` as input for `pcc`. This way, we obtain the following three tables.

p	time pcc(s)	space (Mb)	fails /1000
11	0.6	32	225
67	2.2	32	52
521	17	76	5
4099	150	223	1
32771	1820	1894	0

q	time pcc(s)	space (Mb)	fails /1000
3^5	12	32	13
7^5	32	32	0
17^5	76	73	0
37^5	180	118	0
79^5	410	209	0

q	time pcc(s)	space (Mb)	fails /1000
3^{10}	96	64	0
7^{10}	211	118	0
17^{10}	704	241	0
37^{10}	1534	403	0
79^{10}	3920	864	0

Comparing the different tables, we see that our approach in this section saves a factor of about 3 in runtime and a factor of about 2 in memory usage! Moreover, for small fields the naive lift of a plane quartic sometimes does not satisfy [50, Ass. 1], while this never seems to be the case for the lift constructed using the methods in this section.

3.2 Curves of genus four

3.2.1 Lifting curves of genus four

By [26, Ex. IV.5.2.2] the ideal of a canonical model

$$\overline{C} \subset \mathbb{P}^3 = \operatorname{Proj} \mathbb{F}_q[X, Y, Z, W]$$

of a non-hyperelliptic genus $g = 4$ curve is generated by a cubic $\overline{S}_3$ and a unique quadric $\overline{S}_2$. The latter can be written as

$$\begin{pmatrix} X & Y & Z & W \end{pmatrix} \cdot \overline{M} \cdot \begin{pmatrix} X & Y & Z & W \end{pmatrix}^t, \qquad \overline{M} \in \mathbb{F}_q^{4\times 4},\ \overline{M}^t = \overline{M}.$$

Let $\chi_2 : \mathbb{F}_q \to \{0, \pm 1\}$ denote the quadratic character on $\mathbb{F}_q$. Then $\chi_2(\det \overline{M})$ is an invariant of $\overline{C}$, which is called the discriminant.

If we let $S_2, S_3 \in \mathcal{O}_K[X, Y, Z, W]$ be homogeneous polynomials that reduce to $\overline{S}_2$ and $\overline{S}_3$ modulo p, then by [26, Ex. IV.5.2.2] these define a genus 4 curve $C \subset \mathbf{P}^3$ over K, thereby addressing (i) and (ii). However, as mentioned in Section 2.1 we expect the K-gonality of C to be typically $2g - 2 = 6$. This exceeds the $\mathbb{F}_q$-gonality of $\overline{C}$:

Lemma 8. *Let $\overline{C}/\mathbb{F}_q$ be a non-hyperelliptic curve of genus 4 and $\mathbb{F}_q$-gonality γ, and assume that q is odd. If the discriminant of $\overline{C}$ is 0 or 1 then $\gamma = 3$. If it is -1 and $\#\overline{C}(\mathbb{F}_{q^2}) > 0$ (which is guaranteed if $q > 7$) then $\gamma = 4$. Finally, if it is -1 and $\#\overline{C}(\mathbb{F}_{q^2}) = 0$ then $\gamma = 5$.*

Proof. By [26, Ex. IV.5.5.2] our curve carries one or two geometric g^1_3's, depending on whether the quadric $\overline{S}_2$ is singular (discriminant 0) or not. In the former case the quadric is a cone, and the g^1_3 corresponds to projection from the top. This is automatically defined over $\mathbb{F}_q$. In the latter case the quadric is $\mathbb{F}_{q^2}$-isomorphic to the hyperboloid $\mathbb{P}^1 \times \mathbb{P}^1 \subset \mathbb{P}^3$ and the g^1_3's correspond to the two rulings of the latter. If the isomorphism can be defined over $\mathbb{F}_q$ (discriminant 1) then the g^1_3's are $\mathbb{F}_q$-rational. In the other case (discriminant -1) the smallest field of definition is $\mathbb{F}_{q^2}$. So we can assume that the discriminant of $\overline{C}$ is -1, and therefore that $\gamma > 3$. Now suppose that $\#\overline{C}(\mathbb{F}_{q^2}) > 0$, which is guaranteed if $q > 7$ by [30, Thm. 2]. If there is an $\mathbb{F}_q$-point then let $\overline{\ell}$ be the tangent line to $\overline{C}$ at it. In the other case we can find two conjugate $\mathbb{F}_{q^2}$-points, and we let $\overline{\ell}$ be the line connecting both. In both cases $\overline{\ell}$ is defined over $\mathbb{F}_q$, and the pencil of planes through $\overline{\ell}$ cuts out a g^1_4, as wanted. The argument can be reversed: if there exists a g^1_4 containing some effective $\mathbb{F}_q$-rational divisor D, then by Riemann-Roch we find that $|K - D|$ is non-empty. In particular there exists an effective $\mathbb{F}_q$-rational divisor of degree $\deg(K - D) = 2$ on $\overline{C}$, and $\#\overline{C}(\mathbb{F}_{q^2}) > 0$. So if $\#\overline{C}(\mathbb{F}_{q^2}) = 0$ then $\gamma > 4$. Now note that $\#\overline{C}(\mathbb{F}_{q^5}) > 0$ by the Weil bound. So $\overline{C}$ carries an effective divisor D of degree 5. The linear system $|K - D|$ must be empty, for otherwise there would exist an $\mathbb{F}_q$-point on $\overline{C}$. But then Riemann-Roch implies that $\dim |D| = 1$, i.e. our curve carries an $\mathbb{F}_q$-rational g^1_5. □

Remark 9.

voorbeeld toevoegen van een kromme van gonaliteit 5?

To address Problem 1 in the non-hyperelliptic genus 4 case we make a case-by-case analysis.

$\chi_2(\det \overline{M}_2) = 0$ In this case $\overline{S}_2$ is a cone over a conic; further down we will view it as the embedding in $\mathbb{P}^3$ of the weighted projective plane $\mathbb{P}(1, 2, 1)$. A linear change of variables takes $\overline{S}_2$ to the standard form $WZ - X^2$; it is classical how to do this (diagonalization,

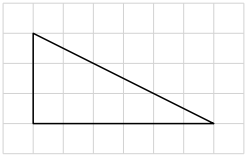
essentially). Projecting from $(0:0:0:1)$ on the XYZ-plane amounts to eliminating the variable W, to obtain

$$Z^3\overline{S}_3(X,Y,Z,\frac{X^2}{Z}) = \overline{S}_3(XZ,YZ,Z^2,X^2). \tag{2}$$

After dehomogenizing with respect to Z, renaming $X \leftarrow x$ and $Y \leftarrow y$ and rescaling if needed, we obtain an affine equation

$$\overline{f} = y^3 + \overline{f}_2(x)y^2 + \overline{f}_4(x)y + \overline{f}_6(x),$$

with $\overline{f}_i \in \mathbb{F}_q[x]$ of degree at most i. Its Newton polygon is contained in (and typically equals)



$(\Delta^0_{4,0})$

So Baker's bound is attained and we take for $f \in \mathcal{O}_K[x,y]$ a naive coefficient-wise lift.

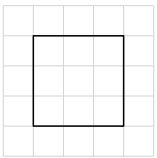
$\underline{\chi_2(\det \overline{M}_2) = 1}$ In this case $\overline{S}_2$ is a hyperboloid; alternatively one can view it as the Segre embedding of $\mathbb{P}^1 \times \mathbb{P}^1$ in $\mathbb{P}^3$. A linear change of variables takes $\overline{S}_2$ to the standard form $XY - ZW$. Projection from $(0:0:0:1)$ on the XYZ-plane amounts to eliminating the variable W, to obtain

$$Z^3\overline{S}_3(X,Y,Z,\frac{XY}{Z}) = \overline{S}_3(XZ,YZ,Z^2,XY).$$

Dehomogenizing with respect to Z and renaming $X \leftarrow x$ and $Y \leftarrow y$ we obtain an affine equation

$$\overline{f} = \overline{f}_0(x)y^3 + \overline{f}_1(x)y^2 + \overline{f}_2(x)y + \overline{f}_3(x)$$

with all $\overline{f}_i \in \mathbb{F}_q[x]$ of degree at most 3. Its Newton polygon is contained in (and typically equals)



$(\Delta^0_{4,1})$

So Baker's bound is attained and we can take for $f \in \mathcal{O}_K[x,y]$ a naive coefficient-wise lift of $\overline{f}$.

Algorithm 2 Lifting curves of genus 4: basic solution

Input non-hyperelliptic genus 4 curve $\overline{C}/\,\mathbb{F}_q$ of $\mathbb{F}_q$-gonality $\gamma \leq 4$

Output lift $f \in \mathcal{O}_K[x,y]$ satisfying (i), (ii), (iii) that is supported
- on $\Delta^0_{4,0}$ if the discriminant is 0, or else
- on $\Delta^0_{4,1}$ if the discriminant is 1, or else
- on $\Delta^6_{4,-1}$

$\overline{C} \leftarrow \text{CanonicalImage}(\overline{C})$ in $\mathbb{P}^3 = \text{Proj}\,\mathbb{F}_q[X,Y,Z,W]$;
$\overline{S}_2 \leftarrow$ unique quadric in $\text{Ideal}(\overline{C})$; $\overline{M}_2 \leftarrow \text{Matrix}(\overline{S}_2)$; $\chi \leftarrow \chi_2(\det \overline{M}_2)$
$\overline{S}_3 \leftarrow$ cubic that along with $\overline{S}_2$ generates $\text{Ideal}(\overline{C})$;
if $\chi = 0$ **then**
    apply automorphism of $\mathbb{P}^3$ transforming $\overline{S}_2 = 0$ into $WZ - X^2 = 0$
    return $\text{NaiveLift}(\text{Dehomogenization}_Z(\overline{S}_3(XZ, YZ, Z^2, X^2)))$
else if $\chi = 1$ **then**
    apply automorphism of $\mathbb{P}^3$ transforming $\overline{S}_2 = 0$ into $XY - ZW = 0$
    return $\text{NaiveLift}(\text{Dehomogenization}_Z(\overline{S}_3(XZ, YZ, Z^2, XY)))$
else
    $P := \text{Random}(\overline{C}(\mathbb{F}_{q^2}))$; $P' := \text{Conjugate}(P)$
    $\ell \leftarrow$ line through P and P' (tangent line if $P = P'$)
    apply automorphism of $\mathbb{P}^3$ transforming ℓ into $X = Z = 0$
    $S_2 \leftarrow \text{NaiveLift}(\overline{S}_2)$
    $S_3 \leftarrow$ lift of $\overline{S}_3$ satisfying $S_3(0,Y,0,W) = (aY + bW)S_2(0,Y,0,W)$ for $a, b \in \mathcal{O}_K$
    return $\text{Dehomogenization}_Z(\text{res}_W(S_2, S_3))$

$\underline{\chi_2(\det \overline{M}_2) = -1}$ This is our first case where, in general, no plane model can be found for which Baker's bound is attained [11, §6]. If $\overline{C}(\mathbb{F}_{q^2}) = \emptyset$ (or in other words if $\gamma = 5$) then unfortunately we do not know how to address Problem 1. We therefore assume that $\overline{C}(\mathbb{F}_{q^2}) \neq \emptyset$ and hence that $\gamma = 4$. This is guaranteed if $q > 7$, so for point counting purposes this is amply sufficient. We follow the proof of Lemma 8: by exhaustive search we find a point $P \in \overline{C}(\mathbb{F}_{q^2})$ along with its Galois conjugate P' and consider the line $\overline{\ell}$ connecting both (tangent line if $P = P'$). This line is defined over $\mathbb{F}_q$, so that modulo a projective transformation we can assume that $\overline{\ell} : X = Z = 0$.

When plugging in $X = Z = 0$ in $\overline{S}_2$ we find a non-zero quadratic expression in Y and W. Indeed: $\overline{S}_2$ cannot vanish identically on $\overline{\ell}$ because no three points of $\overline{S}_2(\mathbb{F}_q)$ are collinear. Because $\overline{C}$ intersects $\overline{\ell}$ in two points (counting multiplicities) we find that

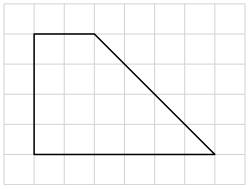
$$\overline{S}_3(0,Y,0,W) = (\overline{a}Y + \overline{b}W)\overline{S}_2(0,Y,0,W)$$

for certain $\overline{a}, \overline{b} \in \mathbb{F}_q$ that are possibly zero. Lift $\overline{S}_2$ coefficient-wise to a homogenous quadric $S_2 \in \mathcal{O}_K[X,Y,Z,W]$ and let $a, b \in \mathcal{O}_K$ reduce to $\overline{a}, \overline{b}$ mod p. We now construct $S_3 \in \mathcal{O}_K[X,Y,Z,W]$ as follows: for the coefficients at Y^3, Y^2W, YW^2, W^3 we make the unique choice for which

$$S_3(0,Y,0,W) = (aY + bW)S_2(0,Y,0,W),$$

while the other coefficients are randomly chosen lifts of the corresponding coefficients of $\overline{S}_3$. Then the genus 4 curve $C \subset \mathbf{P}^3$ defined by S_2 and S_3 is of gonality 4. Indeed, it is constructed such that the line $\ell : X = Z = 0$ intersects the curve in two points (possibly over a quadratic extension), and the pencil of planes through this line cuts out a g^1_4.

Now we project from $(0 : 0 : 0 : 1)$ to a curve in $\mathbf{P}^2$. This amounts to eliminating W from S_2 and S_3. By dehomogenizing the resulting sextic with respect to Z, and by renaming $X \leftarrow x$ and $Y \leftarrow y$ we end up with a polynomial $f \in \mathcal{O}_K[x, y]$ whose Newton polygon is contained in (and typically equals)

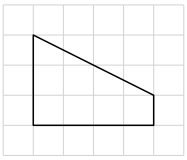


$(\Delta^6_{4,-1})$

Geometrically, what happens is that the points of C on ℓ are both mapped to $(0 : 1 : 0)$ under projection from $(0 : 0 : 0 : 1)$, creating a singularity there, which in terms of the Newton polygon results in 6Σ with its top chopped off. The polynomial f satisfies (i), (ii) and (iii) from Problem 1. Note that Baker's bound is usually *not* attained here: it gives an upper bound of 9. So it is crucial to lift the equations to $\mathcal{O}_K$ *before* projecting on the plane.

3.2.2 Optimizations

$\chi_2(\det \overline{M}_2) = 0$ By applying (1) to a polynomial with Newton polygon $\Delta^0_{4,0}$ one ends up with a polynomial that is monic in y and that has degree 6 in x. This can be improved as soon as $\overline{C}(\mathbb{F}_q) \neq 0$, which is guaranteed if $q > 49$ by [30, Thm. 2]. Namely we can view (2) as the defining equation of a smooth curve in the weighted projective plane $\mathbb{P}(1, 2, 1)$. Using an automorphism of the latter we can position a given $\mathbb{F}_q$-rational point P at $(1 : 0 : 0)$ and the corresponding tangent line at $X = 0$, in order to end up with a Newton polygon that is contained in (and typically equals)



$(\Delta^1_{4,0})$

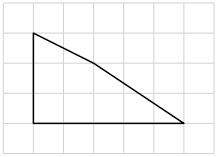
See Remark 10 below for how to do this in practice. So we find $\deg_x f = 4$, which is optimal because the g^1_3 is unique in the case of a singular $\overline{S}_2$. There is a caveat here, in that the tangent line at P might exceptionally be vertical, i.e. P might be a ramification point of our degree 3 map $(x, y) \mapsto x$. In this case it is impossible to position this line at $X = 0$, but in practice one can simply retry with another P. But in fact having a vertical tangent line is an even slightly better situation, as explained in Remark 11 below.

Remark 10. The automorphisms of $\mathbb{P}(1, 2, 1)$ can be applied directly to $\overline{f}$. They correspond to

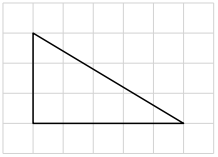
- substituting $y \leftarrow \overline{a}y + \overline{b}x^2 + \overline{c}x + \overline{d}$ and $x \leftarrow \overline{a}'x + \overline{b}'$ in $\overline{f}$ for some $\overline{a}, \overline{a}' \in \mathbb{F}_q^*$ and $\overline{b}, \overline{b}', \overline{c}, \overline{d} \in \mathbb{F}_q$,
- exchanging the line at infinity for the y-axis by replacing $\overline{f}$ by $x^6\overline{f}(x^{-1}, x^{-2}y)$,

or to a composition of both. For instance imagine that an affine point $P = (\overline{a}, \overline{b})$ was found with a non-vertical tangent line. Then $\overline{f} \leftarrow \overline{f}(x+\overline{a}, y+\overline{b})$ translates this point to the origin, at which the tangent line becomes of the form $y = \overline{c}x$. Substituting $\overline{f} \leftarrow \overline{f}(x, y + \overline{c}x)$ positions this line horizontally, and finally replacing $\overline{f}$ by $x^6\overline{f}(x^{-1}, x^{-2}y)$ results in a polynomial with Newton polygon contained in $\Delta^1_{4,0}$.

Remark 11. If P has a vertical tangent line then positioning it at $(1:0:0)$ results in a Newton polygon that is contained in (and typically equals) the first polygon below.



$(\Delta^2_{4,0})$



$(\Delta^3_{4,0})$

Even though $\deg_x f = 5$ here, this results in a slightly faster point count. Such a P will exist if and only if the ramification scheme of $(x, y) \mapsto x$ has an $\mathbb{F}_q$-rational point. Following the heuristics from Remark 7, we expect that this works in about $1-1/e \approx 63.2\%$ of the cases. If the ramification scheme has a rational singular point (i.e. a point of ramification index 3) then one can even end up inside the second polygon. This event is highly exceptional, but we included it in our discussion because this corresponds to the well-known class of $C_{3,5}$ curves.

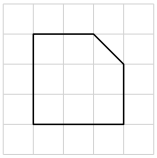
$\chi_2(\det \overline{M}_2) = 1$ By applying (1) to a polynomial with Newton polygon $\Delta^0_{4,1}$ one ends up with a polynomial that is monic in y and that has degree $3 + (\gamma - 1)3 = 9$ in x. This can be improved as soon as $\overline{C}(\mathbb{F}_q) \neq 0$, which is guaranteed if $q > 49$ by [30, Thm. 2]. Assume as before that $\overline{S}_2$ is in the standard form $XY - ZW$. So it is the image of the Segre embedding

$$\mathbb{P}^1 \times \mathbb{P}^1 \hookrightarrow \mathbb{P}^3 : ((X_0 : Z_0), (Y_0 : W_0)) \mapsto (X_0W_0 : Y_0Z_0 : Z_0W_0 : X_0Y_0). \tag{3}$$

That is: we can view $\overline{C}$ as the curve in $\mathbb{P}^1 \times \mathbb{P}^1$ defined by the bihomogeneous polynomial

$$\overline{S}_3(X_0W_0, Y_0Z_0, Z_0W_0, X_0Y_0)$$

of bidegree $(3, 3)$. Remark that if we dehomogenize with respect to both Z_0 and W_0 and rename $X_0 \leftarrow x$ and $Y_0 \leftarrow y$ then we get the polynomial $\overline{f}$ from before. Now if our curve has a rational point P, by applying an appropriate projective transformation in each component we can arrange that $P = ((1:0), (1:0))$. If we then dehomogenize we end up with a Newton polygon that is contained in (and typically equals)

 $(\Delta^1_{4,1})$

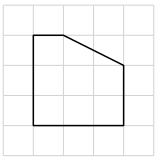
So Baker's bound is attained and we take for $f \in \mathcal{O}_K[x,y]$ a naive coefficient-wise lift. Now applying (1) typically results in a polynomial of degree $3+(\gamma-1)2 = 7$ in x.

Remark 12. The automorphisms of $\mathbb{P}^1 \times \mathbb{P}^1$ can be applied directly to $\overline{f}$. They correspond to

- substituting $y \leftarrow \overline{a}y + \overline{b}$ and $x \leftarrow \overline{a}'x + \overline{b}'$ in $\overline{f}$ for some $\overline{a}, \overline{a}' \in \mathbb{F}_q^*$ and $\overline{b}, \overline{b}' \in \mathbb{F}_q$,
- exchanging the x-axis for the horizontal line at infinity by replacing $\overline{f}$ by $y^3\overline{f}(x, y^{-1})$,
- exchanging the y-axis for the vertical line at infinity by replacing $\overline{f}$ by $x^3\overline{f}(x^{-1}, y)$,

or to a composition of these. For instance imagine that an affine point $P = (\overline{a}, \overline{b})$ was found, then $\overline{f} \leftarrow \overline{f}(x+\overline{a}, y+\overline{b})$ translates this point to the origin, and subsequently replacing $\overline{f}$ by $x^3y^3\overline{f}(x^{-1}, y^{-1})$ results in a polynomial with Newton polygon contained in $\Delta^1_{4,1}$.

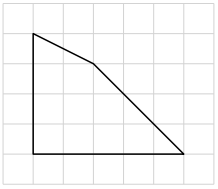
Remark 13. If one manages to let P be a point with a horizontal tangent line, i.e. if P is a ramification point of the projection map from $\overline{C}$ onto the second component of $\mathbb{P}^1 \times \mathbb{P}^1$, then the Newton polygon even becomes contained in (and typically equals)

 $(\Delta^2_{4,1})$

eventually resulting in a polynomial $f \in \mathcal{O}_K[x,y]$ of degree $3+(\gamma-1)1 = 5$ in x. As in the discriminant 0 case, we heuristically expect the probability of success to be about $1-1/e$. However, it is also sufficient to find a ramification point of the projection of $\overline{C}$ onto the first component of $\mathbb{P}^1 \times \mathbb{P}^1$, because we can change the role of (X_0, Z_0) and (Y_0, W_0) if wanted. Assuming independence of events, the percentage of non-hyperelliptic genus 4 curves with discriminant 1 that admit a Newton polygon of the form $\Delta^2_{4,1}$ should be approximately $1-1/e^2 \approx 86.4\%$.

$\chi_2(\det \overline{M}_2) = -1$ By applying (1) to a polynomial with Newton polygon $\Delta^6_{4,-1}$ we end up with a polynomial that is monic in y and that has degree $3+(\gamma-1)2 = 9$. This can be improved as soon as $\overline{C}(\mathbb{F}_q) \neq 0$, which is guaranteed if $q > 49$ by [30, Thm. 2]. In this case we redo the construction with $\overline{\ell}$ the tangent line to a point $P \in \overline{C}(\mathbb{F}_q)$. As before we apply a projective transformation to obtain $\overline{\ell} : X = Z = 0$, but in addition we make sure that $P = (0:0:0:1)$. This implies that $\overline{S}_2(0, Y, 0, W) = Y^2$, possibly after multiplication by a scalar. We now proceed as before, to find lifts $S_2, S_3 \in \mathcal{O}_K[X, Y, Z, W]$ that cut out

a genus 4 curve $C \subset \mathbf{P}^3$, still satisfying the property of containing $(0:0:0:1)$ with corresponding tangent line $\ell : X = Z = 0$. If we then project from $(0:0:0:1)$ we end up with a quintic in $\mathbf{P}^2$, rather than a sextic. The quintic will still pass through the point $(0:1:0)$, which is now non-singular: otherwise the pencil of lines through that point would cut out a K-rational g^1_3. We can therefore apply a projective transformation over K that maps the corresponding tangent line to infinity, while keeping the point at $(0:1:0)$. After having done so, we dehomogenize to find a polynomial $f \in \mathcal{O}_K[x,y]$ whose Newton polygon is contained in (and typically equals)



$(\Delta^5_{4,-1})$

It still satisfies (i), (ii) and (iii), while here $\deg_x f \leq 5$.

3.2.3 Implementation and timings

Again we load the code for a prime field $\mathbb{F}_p$:

```
load "goodmodels_p.m";
```

This time we generate a random quartic `S2` and a random cubic `S3` in 4 variables over the finite field $\mathbb{F}_{97}$ and compute the best lift `Q` to characteristic 0 of some model of the corresponding curve using the methods explained above (including all the optimisations):

```
p:=97;
S2,S3:=random_genus4(p,0);
Q:=optimal_model_genus4(S2,S3);
```

Note that here we have taken χ_2 to be 0, for the other cases the second input of `random_genus4` should be set to 1 or -1. Now we compute the numerator of the zeta function of the curve defined by `S2,S3` by calling the function `num_zeta` from `pcc_p`:

```
chi:=num_zeta(Q,p);
```

To repeat this example over the field $\mathbb{F}_{3^{10}}$, the commands are as follows:

```
load "goodmodels_q.m";
q:=3^10;
S2,S3:=random_genus4(q,0);
Q:=optimal_model_genus4(S2,S3);
chi:=num_zeta(Q,q);
```

For $\chi_2 = -1$, it is sometimes more efficient to replace the last two lines by:

```
Q,W0,Winf:=optimal_model_genus4(S2,S3:alternative_Winf:=true);
chi:=num_zeta(Q,q:W0:=W0,Winf:=Winf);
```

Alternatively, in both examples we can again compute the zeta function of the curve defined by `S2,S3` using a single command:

```
zeta:=zeta_genus4(S2,S3);
```

This function automatically selects (what it expects to be) the most efficient of the two options for the last two lines above.

The tables below contain timings and memory usage for $\chi_2 = 0, 1, -1$ and various values of p and $q = p^n$. All computations were carried out with MAGMA V2.21-8 using a single core on an i7-4910MQ CPU running at 2.90GHz. The code used to generate the tables can be found in the subdirectory `./profiling` of `goodmodels`.

The first column in each table contains the time used by `optimal_model_genus4`, i.e. to compute the lift `Q` to characteristic 0 averaged over 1000 random examples. Then the second column gives the time used by the point counting code `pcc` averaged over at least 10 different examples. Next, the third column contains the total memory used in the computation. Finally, the last column gives the number of examples out of the 1000 where we did not find a lift satisfying [50, Ass. 1].

$\chi_2 = \mathbf{0}$

p	time lift(s)	time pcc(s)	space (Mb)	fails /1000
11	0.01	0.5	32	130
67	0.01	2.5	32	2
521	0.01	25	73	1
4099	0.01	275	323	0
32771	0.01	3924	2236	0

q	time lift(s)	time pcc(s)	space (Mb)	fails /1000
3^5	0.04	12	32	5
7^5	0.05	25	64	0
17^5	0.1	67	76	0
37^5	0.1	143	118	0
79^5	0.1	343	209	0

q	time lift(s)	time pcc(s)	space (Mb)	fails /1000
3^{10}	0.3	74	73	0
7^{10}	0.4	152	112	0
17^{10}	0.6	476	197	0
37^{10}	0.7	1160	403	0
79^{10}	0.9	4350	867	0

$\chi_2 = \mathbf{1}$

p	time lift(s)	time pcc(s)	space (Mb)	fails /1000
11	0.01	0.6	32	169
67	0.02	2.7	32	1
521	0.02	28	73	0
4099	0.02	345	444	0
32771	0.02	3165	3066	0

q	time lift(s)	time pcc(s)	space (Mb)	fails /1000
3^5	0.1	15	32	0
7^5	0.1	31	64	0
17^5	0.2	82	80	0
37^5	0.2	191	124	0
79^5	0.2	456	288	0

q	time lift(s)	time pcc(s)	space (Mb)	fails /1000
3^{10}	0.7	93	76	0
7^{10}	1.2	238	118	0
17^{10}	1.9	668	241	0
37^{10}	2.4	1516	492	0
79^{10}	3.2	5601	1087	0

$\chi_2 = \mathbf{-1}$

p	time lift(s)	time pcc(s)	space (Mb)	fails /1000
11	0.06	2.9	32	0
67	0.02	11	32	0
521	0.02	119	80	0
4099	0.03	1660	719	0
32771	0.02	15089	5551	0

q	time lift(s)	time pcc(s)	space (Mb)	fails /1000
3^5	0.15	43	64	0
7^5	0.3	99	76	0
17^5	0.5	284	124	0
37^5	0.7	617	241	0
79^5	0.8	1581	492	0

q	time lift(s)	time pcc(s)	space (Mb)	fails /1000
3^{10}	2.7	375	118	0
7^{10}	6.6	920	165	0
17^{10}	12	2613	403	0
37^{10}	16	5670	887	0
79^{10}	21	29345	1924	0

Contrary to the genus 3 case, we see that for very small p or $q = p^n$, sometimes we do not find a lift satisfying [50, Ass. 1]. However, in these cases we can usually compute the zeta function by counting points naively, so not much is lost here in practice. Note that the point counting is considerably slower for $\chi_2 = -1$ than for $\chi_2 = 0, 1$ which is due to the map from the curve to $\mathbb{P}^1$ having degree 4 instead of 3 in this case.

3.3 Curves of genus five

3.3.1 Lifting curves of genus five

By Petri's theorem [40] a minimal set of generators for the ideal of a canonical model

$$\overline{C} \subset \mathbb{P}^4 = \text{Proj } \mathbb{F}_q[X, Y, Z, W, V]$$

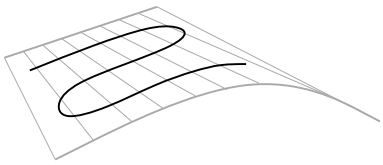
of a non-hyperelliptic genus 5 curve consists of

- three quadrics $\overline{S}_{2,1}, \overline{S}_{2,2}, \overline{S}_{2,3}$ and two cubics $\overline{S}_{3,1}, \overline{S}_{3,2}$ in the trigonal case,
- just three quadrics $\overline{S}_{2,1}, \overline{S}_{2,2}, \overline{S}_{2,3}$ in the non-trigonal case.

So given such a minimal set of generators, it is straightforward to decide trigonality. We denote the space of quadrics in the ideal of $\overline{C}$ by $\mathcal{I}_2(\overline{C})$. Then in both settings $\mathcal{I}_2(\overline{C})$ is a three-dimensional $\mathbb{F}_q$-vector space of which $\overline{S}_{2,1}, \overline{S}_{2,2}, \overline{S}_{2,3}$ form a basis.

Trigonal case Here Petri's theorem moreover tells us that $\mathcal{I}_2(\overline{C})$ cuts out a smooth irreducible surface $\overline{S}$ that is a rational normal surface scroll of type $(1, 2)$. This means that up to a linear change of variables, it is the image $\overline{S}(1, 2)$ of

$$\mathbb{P}^1 \times \mathbb{P}^1 \hookrightarrow \mathbb{P}^4 : ((s : t), (u : v)) \mapsto (vst : ut : vt^2 : us : vs^2),$$



i.e. it is the ruled surface obtained by simultaneously parameterizing a line in the YW-plane and a conic in the XZV-plane, each time drawing the rule through the points under consideration (each of these rules intersects our trigonal curve in three points, counting multiplicities). In other words, modulo a linear change of variables the space $\mathcal{I}_2(\overline{C})$ admits the basis

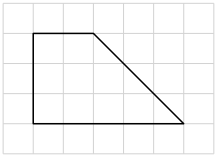
$$X^2 - ZV, \qquad XY - ZW, \qquad XW - YV. \tag{4}$$

To *find* such a linear change of variables we rely on the Lie algebra method for rewriting Severi-Brauer surfaces (such as rational normal surface scrolls) in standard form, as it was developed by de Graaf, Harrison, Pílniková and Schicho [15]. In fact for the particular case of surface scrolls of type $(1, 2)$ it is possible to use a more ad-hoc approach, but we omit the details. More background on rational normal scrolls will be given in Section 4. The Lie algebra method is recalled (and adapted to the finite field case) in Section 4.2.

Once our quadrics $\overline{S}_{2,1}, \overline{S}_{2,2}, \overline{S}_{2,3}$ are given by (4) we project from the line $X = Y = Z = 0$, which amounts to eliminating the variables V and W, in order to obtain the polynomials

$$\overline{S}^{\text{pr}}_{3,i} = Z^3 \overline{S}_{3,i}(X, Y, Z, \frac{X^2}{Z}, \frac{XY}{Z}) = \overline{S}_{3,i}(XZ, YZ, Z^2, X^2, XY)$$

for $i = 1, 2$. Dehomogenizing with respect to Z and renaming $X \leftarrow x$ and $Y \leftarrow y$ we obtain two polynomials $\overline{f}_1, \overline{f}_2 \in \mathbb{F}_q[x, y]$, whose zero loci intersect in the curve defined by $\overline{f} = \gcd(\overline{f}_1, \overline{f}_2)$. The Newton polygon of $\overline{f}$ is contained in (and typically equals)



$(\Delta^{0,0}_{5,\mathrm{trig}})$

Note that in particular $\overline{f}$ attains Baker's bound, and a naive Newton polygon preserving lift $f \in \mathcal{O}_K[x,y]$ satisfies (i), (ii) and (iii). The validity of the above reasoning follows for instance from [7, §3], to which we refer for more details on canonical ideals of trigonal curves and their connection with Newton polygons.

Non-trigonal case In the non-trigonal case, let us write the quadrics as

$$\overline{S}_{2,i} = \begin{pmatrix} X & Y & Z & W & V \end{pmatrix} \cdot \overline{M}_i \cdot \begin{pmatrix} X & Y & Z & W & V \end{pmatrix}^t, \qquad \overline{M}_i \in \mathbb{F}_q^{5\times 5},\ \overline{M}_i^t = \overline{M}_i.$$

The curve $\mathfrak{D}(\overline{C})$ in $\mathbb{P}^2 = \operatorname{Proj} \mathbb{F}_q[\lambda_1,\lambda_2,\lambda_3]$ defined by

$$\det(\lambda_1\overline{M}_1 + \lambda_2\overline{M}_2 + \lambda_3\overline{M}_3) = 0$$

parameterizes the singular members of $\mathcal{I}_2(\overline{C})$. It is a possibly reducible curve called the discriminant curve of $\overline{C}$, known to be of degree 5 and having at most nodes as singularities [2]. The non-singular points correspond to quadrics of rank 4, while the nodes correspond to quadrics of rank 3. For a point $P \in \mathfrak{D}(\overline{C})(\mathbb{F}_q)$, let us denote by $\overline{M}_P$ the corresponding (5×5)-matrix and by $\overline{S}_P$ the corresponding quadric, both of which are well-defined up to a scalar. We define

$$\chi : \mathfrak{D}(\overline{C})(\mathbb{F}_q) \to \{0,\pm 1\} : P \mapsto \begin{cases} \chi_2(\operatorname{pdet}(\overline{M}_P)) & \text{if } P \text{ is non-singular,} \\ 0 & \text{if } P \text{ is singular,} \end{cases}$$

where pdet denotes the pseudo-determinant, i.e. the product of the non-zero eigenvalues.

If we let $S_{2,i} \in \mathcal{O}_K[X,Y,Z,W,V]$ be homogeneous polynomials that reduce to $\overline{S}_{2,i}$ modulo p, then by [26, Ex. IV.5.5.3] these define a genus 5 curve $C \subset \mathbf{P}^4$ over K, thereby addressing (i) and (ii). But as mentioned in Section 2.1 we expect the K-gonality of C to be typically $2g-2 = 8$, which exceeds the $\mathbb{F}_q$-gonality of $\overline{C}$:

Lemma 14. *Let $\overline{C}/\mathbb{F}_q$ be a non-hyperelliptic non-trigonal curve of genus 5 and $\mathbb{F}_q$-gonality γ, and assume that q is odd. If there is a point $P \in \mathfrak{D}(\overline{C})(\mathbb{F}_q)$ for which $\chi(P) \in \{0,1\}$ then $\gamma = 4$. If there does not exist such a point and $\#\overline{C}(\mathbb{F}_{q^3}) > 0$ (which is guaranteed if $q > 3$) then $\gamma = 5$. If there does not exist such a point and $\#\overline{C}(\mathbb{F}_{q^3}) = 0$ then $\gamma = 6$.*

Proof. By [2, VI.Ex. F] the geometric g^1_4's are in correspondence with the singular quadrics containing $\overline{C}$. More precisely:

- Each rank 4 quadric is a cone over $\mathbb{P}^1 \times \mathbb{P}^1$. By taking its span with the top, each line on $\mathbb{P}^1 \times \mathbb{P}^1$ gives rise to a plane intersecting the curve in 4 points. By varying the line we obtain two g^1_4's, one for each ruling of $\mathbb{P}^1 \times \mathbb{P}^1$.

- Each rank 3 quadric is a cone with a 1-dimensional top over a conic. By taking its span with the top, every point of the conic gives rise to a plane intersecting the curve in 4 points. By varying the point we obtain a g^1_4.

There are no other geometric g^1_4's. Over $\mathbb{F}_q$, we see that there exists a rational g^1_4 precisely

- when there is a rank 4 quadric that is defined over $\mathbb{F}_q$, such that the base of the corresponding cone is $\mathbb{F}_q$-isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$, or
- when there is a rank 3 quadric that is defined over $\mathbb{F}_q$.

In terms of the discriminant, this amounts to the existence of a $P \in \mathfrak{D}(\overline{C})$ for which $\chi(P) \in \{0, 1\}$. So let us assume that $\gamma > 4$. If $\#\overline{C}(\mathbb{F}_{q^3}) > 0$, which by the Serre-Weil bound is guaranteed for $q > 3$, then there exists an effective $\mathbb{F}_q$-rational degree 3 divisor D on $\overline{C}$. Because our curve is non-trigonal we find $\dim |D| = 0$, so by the Riemann-Roch theorem we have that $\dim |K - D| \geq 1$, and because $\deg(K - D) = 5$ we conclude that there exists a rational g^1_5 on $\overline{C}$. (Remark: geometrically, this g^1_5 is cut out by the pencil of hyperplanes through the plane spanned by the support of D, taking into account multiplicities.) The argument can be reversed: if there exists a $g^1_5 \ni D$ for some $\mathbb{F}_q$-rational divisor D on $\overline{C}$, then Riemann-Roch implies that $|K - D|$ is non-empty, yielding an effective divisor of degree 3, and in particular $\#\overline{C}(\mathbb{F}_{q^3}) > 0$. So it remains to prove that if $\#\overline{C}(\mathbb{F}_{q^3}) = 0$ then there exists a rational g^1_6. We make a case distinction:

- If $\#\overline{C}(\mathbb{F}_{q^2}) > 0$ then there exists a rational effective divisor D of degree 2, and Riemann-Roch implies that $\dim |K - D| = 2$, yielding the requested rational g^1_6 (even a g^2_6, in fact).
- If $\#\overline{C}(\mathbb{F}_{q^2}) = 0$ then at least $\#\overline{C}(\mathbb{F}_{q^6}) > 0$ by the Weil bound, so there exists a rational effective divisor D of degree 6. Then $K - D$ is of degree 2 and by our assumption $|K - D|$ is empty. But then Riemann-Roch asserts that $\dim |D| = 1$, and we have our rational g^1_6.

This ends the proof. □

Remark 15.

voorbeeld toevoegen van een kromme van gonaliteit 6?

Remark 16. If q is large enough then it is very likely that $\mathfrak{D}(\overline{C})(\mathbb{F}_q)$ will contain a point P with $\chi(P) \in \{0, 1\}$, and therefore that $\gamma = 4$; see below for a discussion containing more precise statements. There do however exist counterexamples for every value of q, as the following construction shows; it was suggested to us by Jeroen Demeyer. Choose three $\mathbb{F}_q$-linearly independent elements $a_1, a_2, a_3 \in \mathbb{F}_{q^5}$ and let $\{\varepsilon_1, \ldots, \varepsilon_5\} \subset \mathbb{F}_{q^5}$ be a self-dual $\mathbb{F}_q$-basis, i.e. a basis with respect to which the trace pairing

$$\mathbb{F}_{q^5} \times \mathbb{F}_{q^5} \to \mathbb{F}_q : (x, y) \mapsto \langle x, y \rangle = \mathrm{Tr}_{\mathbb{F}_{q^5}/\mathbb{F}_q}(xy)$$

becomes the standard inner product. Such a basis always exists; see e.g. [35, Ch. 2, Notes 3] and the references therein. From $\langle a_i x, y \rangle = \langle x, a_i y \rangle$ one sees that the matrix $\overline{M}_i$ of the multiplication-by-a_i-map $\mathbb{F}_{q^5} \to \mathbb{F}_{q^5} : x \mapsto a_i x$ with respect to this basis is symmetric.

So the matrices $\overline{M}_1, \overline{M}_2, \overline{M}_3$ correspond to three quadrics in $\mathbb{F}_q[X, Y, Z, W, V]$. We claim that these cut out a canonical genus five curve. Assuming the claim, it is easy to see that the corresponding discriminant curve cannot have any rational points, because for $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_q$ one has

$$\det(\lambda_1 \overline{M}_1 + \lambda_2 \overline{M}_2 + \lambda_3 \overline{M}_3) = N_{\mathbb{F}_{q^5}/\mathbb{F}_q}(\lambda_1 a_1 + \lambda_2 a_2 + \lambda_3 a_3)$$

which is 0 only if $\lambda_1 = \lambda_2 = \lambda_3 = 0$, due to the $\mathbb{F}_q$-linear independence of the a_i. Now to prove the claim, note that the orthogonal matrix

$$\Pi = \left(\varepsilon_i^{q^{j-1}}\right)_{1 \leq i,j \leq 5}$$

simultaneously diagonalizes the matrices $\overline{M}_i$. Namely,

$$\Pi^t \overline{M}_i \Pi \;=\; \mathrm{diag}\left(a_i,\, a_i^q,\, a_i^{q^2},\, a_i^{q^3},\, a_i^{q^4}\right)$$

for $i = 1, 2, 3$. In terms of our quadrics, it follows that an invertible $\mathbb{F}_{q^5}$-linear transformation of $\mathbb{P}^4$ takes them to

$$\begin{cases} a_1 X^2 + a_1^q Y^2 + a_1^{q^2} Z^2 + a_1^{q^3} W^2 + a_1^{q^4} V^2, \\ a_2 X^2 + a_2^q Y^2 + a_2^{q^2} Z^2 + a_2^{q^3} W^2 + a_2^{q^4} V^2, \\ a_3 X^2 + a_3^q Y^2 + a_3^{q^2} Z^2 + a_3^{q^3} W^2 + a_3^{q^4} V^2. \end{cases}$$

An easy Jacobian computation shows that this concerns a non-singular complete intersection of quadrics, and hence a canonical genus 5 curve [26, IV. 5.5.3], if and only if each 3×3 minor of

$$\begin{pmatrix} a_1 & a_1^q & a_1^{q^2} & a_1^{q^3} & a_1^{q^4} \\ a_2 & a_2^q & a_2^{q^2} & a_2^{q^3} & a_2^{q^4} \\ a_3 & a_3^q & a_3^{q^2} & a_3^{q^3} & a_3^{q^4} \end{pmatrix}$$

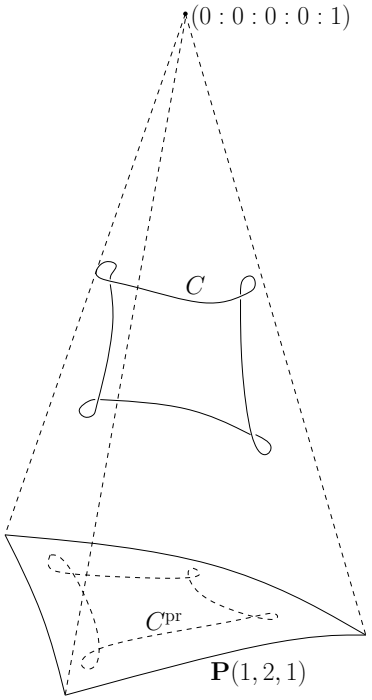
is non-zero. To see why the latter property holds, observe that the above matrix has rank 3, being a submatrix of an invertible 5×5 matrix, more precisely a matrix whose determinant squares to a field discriminant. Thus there exists at least one non-zero minor. But this forces all minors to be non-zero! Indeed, because Frobenius permutes the columns cyclically, every minor is conjugate to either the one spanned by C_1, C_2, C_3 or the one spanned by C_1, C_2, C_4, where C_i denotes the ith column. Now if there were a linear dependence between C_1, C_2, C_3, then Frobenius would imply a linear dependence between C_2, C_3, C_4 and eliminating C_3 from these dependencies would yield a linear dependence between C_1, C_2, C_4. Similarly a linear dependence between C_1, C_2, C_4 would imply a linear dependence between C_1, C_2, C_3, and our claim follows. For the sake of cultural completeness we note that canonical genus 5 curves whose defining quadrics can be simultaneously diagonalized are called *Humbert curves*, which are interesting from multiple points of view; we refer to [20] for some illustrations.

If q is large enough and $\mathfrak{D}(\overline{C})$ has at least one (geometrically) irreducible component that is defined over $\mathbb{F}_q$, then a point $P \in \mathfrak{D}(\overline{C})(\mathbb{F}_q)$ with $\chi(P) \in \{0, 1\}$ exists and therefore $\overline{C}$ has $\mathbb{F}_q$-gonality 4. To state a precise bound on q, let us analyze the (generic) setting where $\mathfrak{D}(\overline{C})$ is a non-singular plane quintic. In this case the 'good' points P are in a natural correspondence with pairs of $\mathbb{F}_q$-points on an unramified double cover of $\mathfrak{D}(\overline{C})$; see [3, §2(c)] for a related discussion. By Riemann-Hurwitz this cover is of genus 11, for which the lower Serre-Weil bound is positive from $q > 467$ on. The presence of an irreducible $\mathbb{F}_q$-component of lower degree can be studied in a similar way and leads to smaller bounds. There are two possible ways in which $\mathfrak{D}(\overline{C})$ does not have an irreducible $\mathbb{F}_q$-component: either it could decompose into two conjugate lines over $\mathbb{F}_{q^2}$ and three conjugate lines over $\mathbb{F}_{q^3}$, or it could decompose into five conjugate lines over $\mathbb{F}_{q^5}$. But in the former case the $\mathbb{F}_q$-rational point P of intersection of the two $\mathbb{F}_{q^2}$-lines satisfies $\chi(P) = 0$, so here too our curve $\overline{C}$ has $\mathbb{F}_q$-gonality 4.

Nog eens bekijken.

Let us now address Problem 1. Unfortunately in the case where $\gamma = 6$ we do not know how to do this. But because this can only occur when $q = 3$, for point counting purposes this is not a problem. We will also largely omit the case where $\gamma = 5$. Here Problem 1 can be addressed by following the proof of Lemma 14, similar to the way we treated the $\chi(\det \overline{M}_2) = -1$ case in genus four. Some pseudocode is available in Algorithm 3 but further details are suppressed, and from now on we assume that $\gamma = 4$, i.e. that there exists a point $P \in \mathfrak{D}(\overline{C})(\mathbb{F}_q)$ with $\chi(P) \in \{0, 1\}$. This can be decided quickly: if $q \leq 467$ then one can proceed by exhaustive search, while if $q > 467$ it is sufficient to verify whether or not $\mathfrak{D}(\overline{C})$ decomposes into five conjugate lines.

To *find* such a point, we first look for $\mathbb{F}_q$-rational singularities of $\mathfrak{D}(\overline{C})$: these are exactly the points P for which $\chi(P) = 0$. If no such singularities exist then we look for a point $P \in \mathfrak{D}(\overline{C})(\mathbb{F}_q)$ for which $\chi(P) = 1$ by trial and error. Once our point has been found, we proceed as follows.



$\chi(P) = 0$ In this case P corresponds to a rank 3 quadric, which using a linear change of variables we can assume to be in the standard form $\overline{S} = WZ - X^2$. Choose homogeneous quadratic polynomials

$$\overline{S}_2, \overline{S}_2' \in \mathbb{F}_q[X, Y, Z, W, V]$$

that along with $\overline{S}$ form a basis of $\mathcal{I}_2(\overline{C})$. (In practice one can usually take $\overline{S}_2 = \overline{S}_{2,1}$ and $\overline{S}_2' = \overline{S}_{2,2}$.) Let $S_2, S_2' \in \mathcal{O}_K[X, Y, Z, W, V]$ be quadrics that reduce to $\overline{S}_2, \overline{S}_2'$ modulo p. Along with

$$S = WZ - X^2 \in \mathcal{O}_K[X, Y, Z, W, V]$$

these cut out a canonical genus 5 curve $C \subset \mathbf{P}^4$. We view the quadric defined by S as a cone over the weighted

projective plane $\mathbf{P}(1,2,1)$ with top $(0:0:0:0:1)$. Our curve is then an intersection of two quadrics inside this cone, and by projecting from the top we obtain a curve C^{pr} in $\mathbf{P}(1,2,1)$. In terms of equations this amounts to eliminating V from S_2 and S_2' by taking the resultant

$$S_2^{\mathrm{pr}} := \mathrm{res}_V(S_2, S_2'),$$

which is a homogeneous quartic. Now as in (2) we further eliminate the variable W to end up with

$$S_2^{\mathrm{pr}}(XZ, YZ, Z^2, X^2).$$

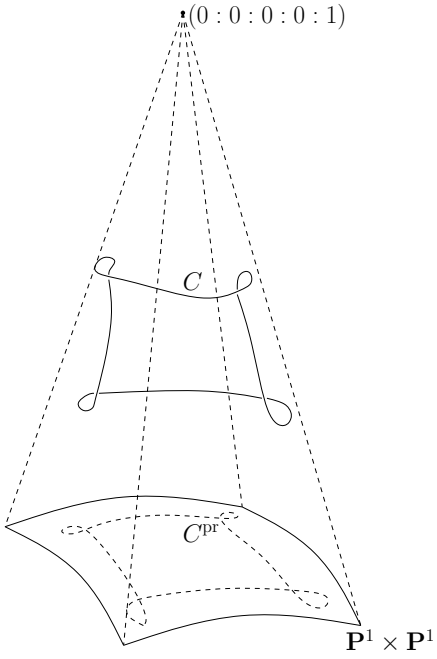
After dehomogenizing with respect to Z, renaming $X \leftarrow x$ and $Y \leftarrow y$ and rescaling if needed, we obtain an affine equation

$$f = y^4 + f_2(x)y^3 + f_4(x)y^2 + f_6(x)y + f_8(x),$$

with $f_i \in \mathcal{O}_K[x]$ of degree at most i. Its Newton polygon is contained in (and typically equals)

$(\Delta_{5,0}^0)$

Note that Baker's genus bound reads 9, so this exceeds the geometric genus by 4.



$\underline{\chi(P) = 1}$ In this case P corresponds to a rank 4 quadric whose pseudo-determinant is a square. Using a linear change of variables we can assume it to be in the standard form $\overline{S} = XY - ZW$, which is a cone over $\mathbb{P}^1 \times \mathbb{P}^1$ with top $(0:0:0:0:1)$. Choose homogeneous quadratic polynomials

$$\overline{S}_2, \overline{S}_2' \in \mathbb{F}_q[X, Y, Z, W, V]$$

that along with $\overline{S}$ form a basis of $\mathcal{I}_2(\overline{C})$. (In practice one can usually take $\overline{S}_2 = \overline{S}_{2,1}$ and $\overline{S}_2' = \overline{S}_{2,2}$.) Let $S_2, S_2' \in \mathcal{O}_K[X, Y, Z, W, V]$ be quadrics that reduce to $\overline{S}_2, \overline{S}_2'$ modulo p. Along with

$$S = XY - ZW \in \mathcal{O}_K[X, Y, Z, W, V]$$

these cut out a canonical genus 5 curve $C \subset \mathbf{P}^4$, which can be viewed as an intersection of two quadrics inside a cone over $\mathbf{P}^1 \times \mathbf{P}^1$ with top $(0 : 0 : 0 : 0 : 1)$. We first project from this top, to obtain

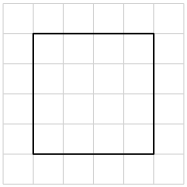
a curve C^{pr} in $\mathbf{P}^1 \times \mathbf{P}^1$. In terms of equations, this amounts to eliminating V from S_2 and S_2' by taking the resultant

$$S_2^{\mathrm{pr}} := \mathrm{res}_V(S_2, S_2'),$$

which is a homogeneous quartic. As in the discussion following (3), we conclude that C^{pr} is defined by the bihomogeneous polynomial

$$S_2^{\mathrm{pr}}(X_0W_0, Y_0Z_0, Z_0W_0, X_0Y_0) \tag{5}$$

of bidegree $(4,4)$. Let $f \in \mathcal{O}_K[x,y]$ be the polynomial obtained from (5) by dehomogenizing with respect to Z_0 and W_0 and by renaming $X_0 \leftarrow x$ and $Y_0 \leftarrow y$. Then the Newton polygon of f is contained in (and typically equals)

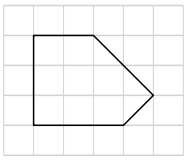


$(\Delta^0_{5,1})$

In particular $\deg_y f = 4$, as wanted. Here again Baker's bound reads 9, which exceeds the geometric genus by 4.

3.3.2 Optimizations

Trigonal case By applying (1) to a polynomial with Newton polygon $\Delta^{0,0}_{5,\mathrm{trig}}$ we end up with a polynomial $f \in \mathcal{O}_K[x,y]$ that is monic in y and that has degree $5 + (\gamma - 1)2 = 9$ in x. This can be improved as soon as our curve $\overline{C}/\,\mathbb{F}_q$ has a rational point P, which is guaranteed if $q > 89$ by the Serre-Weil bound (probably this bound is not optimal). The treatment below is very similar to the genus four case where $\chi_2(\det \overline{M}_2) = 0$, as elaborated in Section 3.2.2. The role of $\mathbb{P}(1,2,1)$ is now played by our scroll $\overline{S}(1,2)$. Recall that the latter is a ruled surface spanned by a line and a conic that are being parameterized simultaneously. Using an automorphism of $\overline{S}(1,2)$ we can position P at the point at infinity of the spanning conic, in such a way that the curve and the conic meet at P with multiplicity at least two. This results in a Newton polygon that is contained in (and typically equals)



$(\Delta^{0,1}_{5,\mathrm{trig}})$

See Remark 17 below for how this can be done in practice. Here an application of (1) typically results in $\deg_x f = 3 + (\gamma - 1)2 = 7$. There are two caveats here: our curve might exceptionally be tangent at P to a rule of the scroll, in which case it is impossible to make it tangent to the conic at that point. Or worse: our point P might lie on the spanning

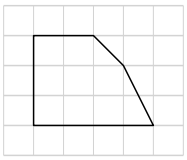
line, in which case it is just impossible to move it to the spanning conic. In these cases one can most likely just retry with another P. But in fact these two situations are even slightly better, as explained in Remark 18 below.

Remark 17. The automorphisms of $\overline{S}(1,2)$ can be applied directly to $\overline{f}$. They correspond to

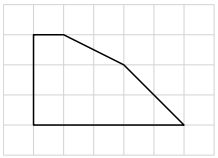
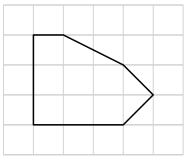
- substituting $y \leftarrow \overline{a}y+\overline{b}x+\overline{c}$ and $x \leftarrow \overline{a}'x+\overline{b}'$ in $\overline{f}$ for some $\overline{a}, \overline{a}' \in \mathbb{F}_q^*$ and $\overline{b}, \overline{b}', \overline{c} \in \mathbb{F}_q$,
- exchanging the rule at infinity for the y-axis by replacing $\overline{f}$ by $x^5\overline{f}(x^{-1}, x^{-1}y)$,

or to a composition of both. For instance imagine that an affine point $P = (\overline{a}, \overline{b})$ was found with a non-vertical tangent line. Then $\overline{f} \leftarrow \overline{f}(x+\overline{a}, y+\overline{b})$ translates this point to the origin, at which the tangent line becomes of the form $y = \overline{c}x$. Substituting $\overline{f} \leftarrow \overline{f}(x, y + \overline{c}x)$ positions this line horizontally, and finally replacing $\overline{f}$ by $x^5\overline{f}(x^{-1}, x^{-1}y)$ results in a polynomial with Newton polygon contained in $\Delta^{0,1}_{5,\mathrm{trig}}$.

Remark 18. As for the first caveat, if $\overline{C}$ turns out to be tangent at P to one of the rules of the scroll then moving P to the point at infinity of the spanning conic results in a Newton polygon that is contained in (and typically equals)

 $(\Delta^{0,2}_{5,\mathrm{trig}})$

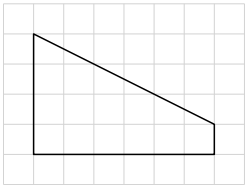
Even though this yields $\deg_x f = 4 + (\gamma - 1)2 = 8$, the corresponding point count is slightly faster. Such a P will exist if and only if the ramification scheme of $(x, y) \mapsto x$ has an $\mathbb{F}_q$-rational point. Following the heuristics from Remark 7 we expect that this works in about $1 - 1/e \approx 63.2\%$ of the cases. As for the second caveat, if P is a point on the spanning line of the scroll, we can move it the point at infinity of that line. This results in a Newton polygon that is contained in (and typically equals) the left polygon below.

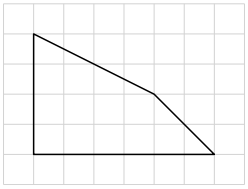
 $(\Delta^{1,0}_{5,\mathrm{trig}})$  $(\Delta^{1,1}_{5,\mathrm{trig}})$

This again gives us $\deg_x f = 5 + (\gamma - 1)1 = 7$, but here too the corresponding point count is faster. Because $\overline{C}$ intersects the spanning line in a scheme of degree 2, the probability of success should be about 50%. Now suppose that the rule through P intersects the curve in another rational point Q, let us say not a ramification point of the projection map $(x, y) \mapsto x$. The probability of this event should again be about 50%. Then Q can be treated as before, i.e. we can move it to the point at infinity of the spanning conic, in such a way that the curve and the conic meet at Q with multiplicity at least two. In this way we end up with a Newton polygon that is contained in (and typically equals) the right polygon above, yielding $\deg_x f = 4 + (\gamma - 1)1 = 6$. Because the good instances of P

generically arise in pairs, we can retry with the other point (and corresponding rule) in the case of failure. Overall we expect this to result in a chance of about 37.5% of being able to realize $\Delta^{1,1}_{5,\mathrm{trig}}$.

Non-trigonal case For point counting purposes it is advantageous to give preference to the case $\chi(P) = 0$, i.e. to use a singular point $P \in \mathfrak{D}(\overline{C})(\mathbb{F}_q)$ if it exists. Some optimizations over the corresponding discussion in Section 3.3.2 are possible, for instance generically one can replace $\Delta^0_{5,0}$ with the left polygon below


($\Delta^1_{5,0}$)


($\Delta^2_{5,0}$)

while with an estimated probability of about $1 - (3/8)^\rho$ one can even end up inside the right polygon. Here $10 \geq \rho \geq 1$ denotes the number of singular points $P \in \mathfrak{D}(\overline{C})(\mathbb{F}_q)$. We will spend a few more words on this in Remark 21 below, after having discussed the $\chi(P) = 1$ case. However usually such a singular $\mathbb{F}_q$-point P does not exist, i.e. $\rho = 0$. More precisely we expect that the proportion of curves for which $\mathfrak{D}(\overline{C})$ is a smooth plane quintic tends to 100% as $q \to \infty$. This is supported by a result over $\mathbf{C}$ stating that in terms of moduli the locus of (non-hyperelliptic, non-trigonal) genus five curves having a singular point on its discriminant curve has codimension one; see [47, 22]. For this reason we will focus our attention on the case $\chi(P) = 1$, and leave it to the interested reader to elaborate the remaining details.

Remark 19. Even though $\chi(P) = 0$ generically does not occur, our experience is that many genus five curves over $\mathbb{F}_q$ that pop up in practice, such as non-degenerate curves or certain modular curves, *do* admit such an $\mathbb{F}_q$-rational singular point on their discriminant curve.

As for the case $\chi(P) = 1$, note that by applying (1) to a polynomial with Newton polygon $\Delta^0_{5,1}$ one ends up with a polynomial that is monic in y and that has degree $4 + (\gamma - 1)4 = 16$ in x. This can most likely be reduced to 10, as we will explain now. The idea is to exploit the fact that in practice the discriminant curve $\mathfrak{D}(\overline{C})$ contains enough $\mathbb{F}_q$-rational points for there to be considerable freedom in choosing a P for which $\chi(P) = 1$. We want to select a suited such P, by which we mean the following.

By a good P we mean the following. As before, assume that an automorphism of $\mathbb{P}^4$ has been applied such that $\overline{S}_P = \overline{S} = XY - ZW$ and let $\overline{S}_2,\ \overline{S}'_2 \in \mathbb{F}_q[X, Y, Z, W, V]$ be quadrics that along with $\overline{S}$ cut out our curve $\overline{C}$. Now suppose that we would have projected $\overline{C}$ from the point $(0 : 0 : 0 : 0 : 1)$ *before* lifting to characteristic 0. Then we would have ended up with a curve $\overline{C}^{\mathrm{pr}}$ in

$$\mathbb{P}^1 \times \mathbb{P}^1 : \overline{S} = 0 \quad \text{in } \mathbb{P}^3 = \operatorname{Proj} \mathbb{F}_q[X, Y, Z, W].$$

This curve has arithmetic genus 9, because in fact that is what Baker's bound measures. Since the excess in genus is $9 - 5 = 4$ we typically expect there to be 4 nodes. Our point P

is 'suited' as soon as one of the singular points Q of $\overline{C}^{\mathrm{pr}}$ is $\mathbb{F}_q$-rational. If P is not suited, i.e. if there is no such $\mathbb{F}_q$-rational singularity, then we retry with another $P \in \mathfrak{D}(\overline{C})(\mathbb{F}_q)$ for which $\chi(P) = 1$. Heuristically we estimate the probability of success to be comparable to the chance that a univariate polynomial over $\mathbb{F}_q$ of degree 4 has a rational root, which is approximately $5/8 = 62.5\%$. In particular if there are enough candidates for P available, we should end up being successful very quickly with near certainty.

Given such a singular point $Q \in \overline{C}^{\mathrm{pr}}(\mathbb{F}_q) \subset \mathbb{P}^1 \times \mathbb{P}^1$ we can move it to the point $((1:0),(1:0))$, similar to what we did in the genus 4 case where $\chi_2(\det \overline{M}_2) = 1$. In terms of the coordinates X, Y, Z, W of the ambient space $\mathbb{P}^3$ this means moving the point to $(0:0:0:1)$, where we assume that $\mathbb{P}^1 \times \mathbb{P}^1$ is embedded using (3). Let's say this amounts to the change of variables

$$\begin{pmatrix} X \\ Y \\ Z \\ W \end{pmatrix} \leftarrow A \cdot \begin{pmatrix} X \\ Y \\ Z \\ W \end{pmatrix}$$

where $A \in \mathbb{F}_q^{4\times 4}$. Then we can apply the change of variables

$$\begin{pmatrix} X \\ Y \\ Z \\ W \\ V \end{pmatrix} \leftarrow \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} X \\ Y \\ Z \\ W \\ V \end{pmatrix}$$

directly on the defining polynomials $\overline{S}, \overline{S}_1, \overline{S}_2$ of $\overline{C}$ to obtain the curve $\overline{C}_{\mathrm{tr}}$ cut out by

$$\overline{S} = XY - ZW,\ \overline{S}_{2,\mathrm{tr}},\ \overline{S}_{2',\mathrm{tr}} \in \mathbb{F}_q[X, Y, Z, W, V].$$

Indeed the transformation affects $\overline{S}$ at most through multiplication by a non-zero scalar. If we would now project from $(0:0:0:0:1)$ as before, we would end up with a curve $\overline{C}^{\mathrm{pr}}_{\mathrm{tr}} \subset \mathbb{P}^1 \times \mathbb{P}^1$ having a singularity at $((1:0),(1:0))$, which is at $(0:0:0:1)$ in the coordinates X, Y, Z, W.

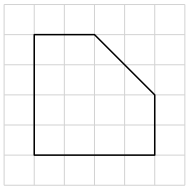
Recall that inside $\mathbb{P}^4$ we view $\overline{S}$ as the defining equation of a cone over $\mathbb{P}^1 \times \mathbb{P}^1$ with top $(0:0:0:0:1)$. The fact that the projected curve has a singularity at $(0:0:0:1)$ implies that the line $X = Y = Z = 0$ meets the curve at least twice, counting multiplicities (these points of intersection need not be $\mathbb{F}_q$-rational). Thus after multiplying $\overline{S}_{2,\mathrm{tr}}$ by a scalar if needed we find that

$$\overline{S}_{2,\mathrm{tr}}(0,0,0,W,V) = \overline{S}'_{2,\mathrm{tr}}(0,0,0,W,V) = \overline{a}W^2 + \overline{b}WV + \overline{c}V^2$$

for some $\overline{a}, \overline{b}, \overline{c} \in \mathbb{F}_q$. Now lift $\overline{S}_{2,\mathrm{tr}}$ and $\overline{S}_{2',\mathrm{tr}}$ in a consistent way, in order to obtain quadrics $S_2, S'_2 \in \mathcal{O}_K[X, Y, Z, W, V]$ satisfying

$$S_2(0,0,0,W,V) = S'_2(0,0,0,W,V) = aW^2 + bWV + cV^2$$

for elements $a, b, c \in \mathcal{O}_K$ that reduce to $\overline{a}, \overline{b}, \overline{c}$ modulo p. If we then proceed as before, we end up with a curve C^{pr} in $\mathbf{P}^1 \times \mathbf{P}^1$ having a singularity at $((1:0),(1:0))$. This eventually results in a defining polynomial $f \in \mathcal{O}_K[x,y]$ whose Newton polygon is contained in (and typically equals)



$(\Delta^0_{5,1})$

Applying (1) to f results in a polynomial having degree at most $4 + (\gamma - 1)2 = 10$ in x, as announced.

Remark 20.

Omdat er een ééndimensionale familie aan goeie P's bestaat is er eigenlijk nog een vrijheidsgraad over. Misschien kan het altijd (of in een bepaald percentage van de gevallen) geregeld worden dat je singuliere punt een horizontale branch heeft, waardoor je in

$$\mathrm{conv}\{(0,0),(4,0),(4,2),(3,3),(1,4),(0,4)\}$$

zou uitkomen. Dit zou dan leiden tot graad 8 in x. Maar ik weet niet hoe je die nog-betere P's actief kunt opsporen? En misschien is het effect voor het punten tellen verwaarloosbaar.

Remark 21. The same ideas apply to the case $\chi(P) = 0$, with the role of $\mathbb{P}^1 \times \mathbb{P}^1$ replaced by $\mathbb{P}(1,2,1)$.

- If the projection $\overline{C}^{\mathrm{pr}}$ of $\overline{C}$ to $\mathbb{P}(1,2,1)$ has an $\mathbb{F}_q$-rational singular point, then it can be arranged that the resulting curve $C^{\mathrm{pr}} \subset \mathbf{P}(1,2,1)$ has a singularity at $(1:0:0)$, eventually yielding a polynomial $f \in \mathcal{O}_K[x,y]$ whose Newton polygon is contained in $\Delta^2_{5,0}$. As in the $\chi(P) = 1$ case we expect that the probability that this works out for a given P to be about $5/8 = 62.5\%$. But unlike the $\chi(P) = 1$ case there is not much freedom to retry in the case of failure: we have ρ chances only. This explains our expected probability of $1 - (3/8)^\rho$ to be able to realize $\Delta^2_{5,0}$.
- If the foregoing fails every time then we can play the same game with a non-singular $\mathbb{F}_q$-rational point Q on $\overline{C}^{\mathrm{pr}}$ (guaranteed to exist if $q > 89$ because then $\overline{C}$ has an $\mathbb{F}_q$-rational point by the Serre-Weil bound). The result is a curve $C^{\mathrm{pr}} \subset \mathbf{P}(1,2,1)$ containing the point $(1:0:0)$. We can then use an automorphism of $\mathbf{P}(1,2,1)$ to make C^{pr} tangent to $X = 0$ at that point (unless the tangent line is vertical, in which case we simply retry with another Q). This is done similarly to the way we handled the case $\chi_2(\det \overline{M}_2)$ in Section 3.2.2: see in particular Remark 10. In this way one ends up in $\Delta^1_{5,0}$.

3.3.3 Implementation and timings

trigonal case

To compute the numerator `chi` of the zeta function of a random trigonal curve of genus 5 over $\mathbb{F}_{97}$ we type:

```
load "goodmodels_p.m";
p:=97;
f:=random_genus5_trigonal(p);
Q:=optimal_model_genus5_trigonal(f);
chi:=num_zeta(Q,p);
```

Note that `f` is a polynomial in $\mathbb{F}_p[x,y]$ with Newton polygon $\Delta^{0,0}_{5,\mathrm{trig}}$. This turns out to be more practical as input than the 3 quadrics and 2 cubics that define the canonical embedding.

To repeat this example over the field $\mathbb{F}_{3^{10}}$ the commands are as follows:

```
load "goodmodels_q.m";
q:=3^10;
f:=random_genus5_trigonal(q);
Q:=optimal_model_genus5_trigonal(f);
chi:=num_zeta(Q,q);
```

Alternatively, in both examples we can again compute the zeta function of the curve defined by `f` using a single command:

```
zeta:=zeta_genus5_trigonal(r);
```

The tables below contain timings and memory usage for various values of p and $q = p^n$. All computations were carried out with MAGMA V2.21-8 using a single core on an i7-4910MQ CPU running at 2.90GHz. The code used to generate the tables can be found in the subdirectory `./profiling` of `goodmodels`.

The first column in each table contains the time used by `optimal_model_genus5_trigonal`, i.e. to compute the lift `Q` to characteristic 0 averaged over 1000 random examples. Then the second column gives the time used by the point counting code `pcc` averaged over at least 10 different examples. Next, the third column contains the total memory used in the computation. Finally, the last column gives the number of examples out of the 1000 where we did not find a lift satisfying [50, Ass. 1].

p	time lift(s)	time pcc(s)	space (Mb)	fails /1000
11	0.01	0.8	32	206
67	0.01	3.7	32	45
521	0.01	38	73	4
4099	0.01	525	484	1
32771	0.01	5347	3501	0

q	time lift(s)	time pcc(s)	space (Mb)	fails /1000
3^5	0.1	31	32	6
7^5	0.1	64	73	0
17^5	0.2	163	112	0
37^5	0.2	376	197	0
79^5	0.3	1010	371	0

q	time lift(s)	time pcc(s)	space (Mb)	fails /1000
3^{10}	1.3	182	80	0
7^{10}	2.2	452	156	0
17^{10}	3.9	1364	320	0
37^{10}	4.7	4501	725	0
79^{10}	5.5	16037	1447	0

non-trigonal case

To compute the numerator `chi` of the zeta function of a non-trigonal curve of genus 5 over $\mathbb{F}_{97}$ the commands are as follows:

```
load "goodmodels_p.m";
p:=97;
S1,S2,S3:=random_genus5_nontrigonal(p);
Q:=optimal_model_genus5_trigonal(S1,S2,S3);
chi:=num_zeta(Q,p);
```

To repeat this example over $\mathbb{F}_{3^{10}}$, we type:

```
load "goodmodels_q.m";
q:=3^10;
S1,S2,S3:=random_genus5_nontrigonal(q);
Q:=optimal_model_genus5_trigonal(S1,S2,S3);
chi:=num_zeta(Q,q);
```

It is sometimes more efficient to replace the last two lines by:

```
Q,W0,Winf:=optimal_model_genus5_trigonal(S1,S2,S3:alternative_Winf:=true);
chi:=num_zeta(Q,q:W0:=W0,Winf:=Winf);
```

Alternatively, in both examples we can again compute the zeta function of the curve defined by `S1,S2,S3` using a single command:

```
zeta:=zeta_genus5_nontrigonal(S2,S3);
```

This function automatically selects (what it expects to be) the most efficient of the two options for the last two lines above.

The tables below contain timings and memory usage for various values of p and $q = p^n$. All computations were carried out with MAGMA V2.21-8 using a single core on an i7-4910MQ CPU running at 2.90GHz. The code used to generate the tables can be found in the subdirectory `./profiling` of `goodmodels`.

The first column in each table contains the time used by `optimal_model_genus5_nontrigonal`, i.e. to compute the lift `Q` to characteristic 0 averaged over 1000 random examples. Then the second column gives the time used by the point counting code `pcc` averaged over at least 10 different examples. Next, the third column contains the total memory used in the computation. Finally, the last column gives the number of examples out of the 1000 where we did not find a lift satisfying [50, Ass. 1].

p	time lift(s)	time pcc(s)	space (Mb)	fails /1000
11	0.1	3.0	32	7
67	0.1	13	32	0
521	0.2	141	118	0
4099	0.3	2000	1166	0
32771	0.2	23890	9208	0

q	time lift(s)	time pcc(s)	space (Mb)	fails /1000
3^5	2.4	149	76	0
7^5	4.3	343	118	0
17^5	10	995	209	0
37^5	14	2608	435	0
79^5	18	7569	823	0

q	time lift(s)	time pcc(s)	space (Mb)	fails /1000
3^{10}	20	1440	518	0
7^{10}	69	3806	800	0
17^{10}	154	13737	1325	0
37^{10}	186	46978	1760	0
79^{10}	370	193079	3524	0

4 Rational normal scrolls

4.1 Scroll associated to a map to $\mathbb{P}^1$

4.2 Lie algebra method

Also refer to [43] for a discussion that is specific to trigonal curves.

5 Curves of low gonality

5.1 Trigonal curves

5.2 Tetragonal curves

6 Conclusions

References

[1] D. Abramovich, *A linear lower bound on the gonality of modular curves*, International Mathematics Research Notices **1996**(20), pp. 1005-1011 (1996)

[2] E. Arbarello, M. Cornalba, P. Griffiths, J. Harris, *Geometry of algebraic curves: Volume I*, Grundlehren der mathematischen Wissenschaften **267**, Springer (2010)

[3] A. Beauville, *Prym varieties: a survey*, Proceedings of Symposia in Pure Mathematics **49**(1), pp. 607-620 (1989)

[4] P. Beelen, *A generalization of Baker's theorem*, Finite Fields and Their Applications **15**, pp. 558-568 (2009)

[5] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, Journal of Symbolic Computation **24**, pp. 235-265 (1997)

[6] W. Castryck, F. Cools, *Newton polygons and curve gonalities*, Journal of Algebraic Combinatorics **35**(3), pp. 345-366 + err. pp. 367-372 (2012)

[7] W. Castryck, F. Cools, *A minimal set of generators for the canonical ideal of a non-degenerate curve*, Journal of the Australian Mathematical Society **98**(3), pp. 311-323 (2015)

[8] W. Castryck, F. Cools, *Linear pencils encoded in the Newton polygon*, preprint

[9] W. Castryck, J. Denef, F. Vercauteren, *Computing zeta functions of nondegenerate curves*, International Mathematics Research Papers **2006**, pp. 1-57 (2006)

[10] W. Castryck, H. Hubrechts, F. Vercauteren, *Computing zeta functions in families of C_{ab} curves using deformation*, ANTS VIII – Lecture Notes in Computer Science **5011**, pp. 296-311 (2008)

[11] W. Castryck, J. Voight, *On nondegeneracy of curves*, Algebra & Number Theory **3**(3), pp. 255-281 (2009)

[12] P. Clark, *There are genus one curves of every index over every number field*, Journal für die Reine und Angewante Mathematik **594**, pp. 201-206 (2006)

[13] M. Coppens, G. Martens, *Linear pencils on real algebraic curves*, Journal of Pure and Applied Algebra **214**(6), pp. 841-849 (2010)

[14] D. Cox, J. Little, H. Schenck, *Toric varieties*, Graduate Studies in Mathematics **124**, American Mathematical Society (2011)

[15] W. de Graaf, M. Harrison, J. Pílniková, J. Schicho, *A Lie algebra method for rational parameterization of Severi-Brauer surfaces*, Journal of Algebra **303**(2), pp. 514-529 (2006)

[16] J. Denef, F. Vercauteren, *An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic* 2, Journal of Cryptology **19**(2), pp. 1-25 (2006)

[17] J. Denef, F. Vercauteren, *Computing zeta functions of C_{ab} curves using Monsky-Washnitzer cohomology*, Finite Fields and Their Applications **12**(1), pp. 78-102 (2006)

[18] M. Derickx, *Torsion points on elliptic curves and gonalities of modular curves*, master thesis, Universiteit Leiden (2012)

[19] M. Derickx, M. van Hoeij, *Gonality of the modular curve $X_1(N)$*, Journal of Algebra **417**, pp. 52-71 (2014)

[20] R. Donagi, *The fibers of the Prym map*, Proceedings of Curves, Jacobians and Abelian Varieties (Amherst, MA, 1990), Contemporary Mathematics **136**, American Mathematical Society, pp. 55-125 (1992)

[21] F. Feschet, *The exact lattice width of planar sets and minimal arithmetical thickness*, Combinatorial Image Analysis, Lecture Notes in Computer Science **4040**, pp. 25-33 (2006)

[22] C. Fontanari, E. Looijenga, *A perfect stratification of $\mathcal{M}_g$ for $g \leq 5$*, Geometriae Dedicata **136**, pp. 133-143 (2008)

[23] P. Gaudry, N. Gürel, *An extension of Kedlaya's point-counting algorithm to superelliptic curves*, ASIACRYPT 2001 – Lecture Notes in Computer Science **2248**, pp. 480-494 (2001)

[24] P. Gille, T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics **101**, Cambridge University Press (2006)

[25] M. Harrison, *An extension of Kedlaya's algorithm for hyperelliptic curves*, Journal of Symbolic Computation **47**(1), pp. 89-101 (2012)

[26] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Springer (1977)

[27] D. Harvey, *Kedlaya's algorithm in larger characteristic*, International Mathematics Research Notices **2007**(rnm095), rnm095-29 (2007)

[28] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, Journal of Symbolic Computation **33**(4), pp. 425-445 (2001)

[29] M. Homma, *Funny plane curves in characteristic $p > 0$*, Communications in Algebra **15**(7), pp. 1469-1501 (1987)

[30] E. Howe, K. Lauter, J. Top, *Pointless curves of genus three and four*, Arithmetic, geometry and coding theory (AGCT 2003), Sémin. Congr. **11**, Soc. Math. France, Paris, pp. 125-141 (2005)

[31] H. Hubrechts, *Point counting in families of hyperelliptic curves*, Foundations of Computational Mathematics **8**(1), pp. 137-169 (2008)

[32] L. Illusie, *Grothendieck's existence theorem in formal geometry, with a letter from Jean-Pierre Serre*, Fundamental Algebraic Geometry: Grothendieck's FGA explained, Mathematical Surveys and Monographs **112**, pp. 179-234 (2005)

[33] K. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, Journal of the Ramunajan Mathematical Society **16**(4), pp. 323-338 (2001) + errata, ibid. **18**, pp. 417-418 (2003)

[34] A. G. Khovanskii, *Newton polyhedra and toroidal varieties*, Functional Analysis and Its Applications **11**(4), pp. 289-296 (1977)

[35] R. Lidl, H. Niederreiter, *Finite Fields*, 2nd edition, Encyclopedia of Mathematics and its Applications **20**, Cambridge University Press (1997)

[36] M. Minzlaff, *Computing zeta functions of superelliptic curves in larger characteristic*, Mathematics in Computer Science **3**(2), pp. 209-224 (2010)

[37] G. Mullen, D. Panario (eds.), *Handbook of finite fields*, Discrete Mathematics and Its Applications, Chapman & Hall, CRC Press (2013)

[38] R. Pellikaan, *On the gonality of curves, abundant codes and decoding*, Proceedings of Coding Theory and Algebraic Geometry (Luminy, 1991), Lecture Notes in Mathematics **1518**, pp. 132-144 (1992)

[39] B. Poonen, *Gonality of modular curves in characteristic p*, Mathematics Research Letters **14**(4) (2007)

[40] B. Saint-Donat, *On Petri's analysis of the linear system of quadrics through a canonical curve*, Mathematische Annalen **206**, pp. 157-175 (1973)

[41] T. Satoh, *The canonical lift of an ordinary elliptic curve over a finite field and its point counting*, Journal of the Ramanujan Mathematical Society **15**(4), pp. 247-270 (2000)

[42] J. Schicho, F.-O. Schreyer, M. Weimann, *Computational aspects of gonal maps and radical parametrization of curves*, Applicable Algebra in Engineering, Communication and Computing **24**(5), pp. 313-341 (2013)

[43] J. Schicho, D. Sevilla, *Effective radical parametrization of trigonal curves*, Computational Algebraic and Analytic Geometry, Contemporary Mathematics **572**, American Mathematical Society, pp. 221-231 (2012)

[44] F.-O. Schreyer, *Syzygies of canonical curves and special linear series*, Mathematische Annalen **275**(1), pp. 105-137 (1986)

[45] F. Serrano, *Extension of morphisms defined on a divisor*, Mathematische Annalen **277**, pp. 395-413 (1987)

[46] A. V. Sutherland, *Torsion subgroups of elliptic curves over number fields*, notes available at `https://math.mit.edu/~drew/` (2012)

[47] M. Teixidor i Bigas, *The divisor of curves with a vanishing theta-null*, Compositio Mathematica **66**(1), pp. 15-22 (1988)

[48] M. Tsfasman, S. Vlăduţ, D. Nogin, *Algebraic geometric codes: basic notions*, Mathematical Surveys and Monographs **139**, American Mathematical Society (2007)

[49] J. Tuitman, *Counting points on curves using a map to* $\mathbb{P}^1$, Mathematics of Computation **85**, pp. 961-981 (2016)

[50] J. Tuitman, *Counting points on curves: the general case*, preprint

[51] J. Tuitman, *Counting points in families of nondegenerate curves*, Ph.D. thesis, KU Leuven (2010)

[52] G. Walker, *Computing zeta functions of varieties via fibration*, Ph.D. thesis, University of Oxford (2010)

Algorithm 3 Lifting curves of genus 5: basic solution

Input non-hyperelliptic genus 5 curve $\overline{C}/\,\mathbb{F}_q$ of $\mathbb{F}_q$-gonality $\gamma \leq 5$

Output lift $f \in \mathcal{O}_K[x,y]$ satisfying (i), (ii), (iii) that is supported
- on $\Delta^{0,0}_{5,\mathrm{trig}}$ if $\overline{C}$ is trigonal, or else
- on $\Delta^{0}_{5,0}$ if $\exists P \in \mathfrak{D}(\overline{C}) : \chi(P) = 0$, or else
- on $\Delta^{0}_{5,1}$ if $\exists P \in \mathfrak{D}(\overline{C}) : \chi(P) = 1$, or else
- on todo

$\overline{C} \leftarrow \mathrm{CanonicalImage}(\overline{C})$ in $\mathbb{P}^4 = \mathrm{Proj}\,\mathbb{F}_q[X,Y,Z,W,V]$;
if $\mathrm{Ideal}(\overline{C})$ is generated by quadrics **then**
  $\overline{S}_{2,1}, \overline{S}_{2,2}, \overline{S}_{2,3} \leftarrow$ quadrics that generate $\mathrm{Ideal}(\overline{C})$
  $\overline{M}_i \leftarrow \mathrm{Matrix}(\overline{S}_{2,i})$ $(i = 1,2,3)$
  $\mathfrak{D}(\overline{C}) \leftarrow$ curve in $\mathbb{P}^2 = \mathrm{Proj}\,\mathbb{F}_q[\lambda_1,\lambda_2,\lambda_3]$ defined by $\det(\lambda_1\overline{M}_1 + \lambda_2\overline{M}_2 + \lambda_3\overline{M}_3)$
  if $q \leq 467$ and $\neg\exists P \in \mathfrak{D}(\overline{C})(\mathbb{F}_q) : \chi(P) \in \{0,1\}$ (verified exhaustively)
        or $q > 467$ and $\mathfrak{D}(\overline{C})$ decomposes into five conjugate lines
    then goodpoints $\leftarrow$ false **else** goodpoints $\leftarrow$ true
  if goodpoints **then**
    if $\mathfrak{D}(\overline{C})$ has $\mathbb{F}_q$-rational singular point P **then**
      $\overline{S}_2, \overline{S}_2' \leftarrow$ quadrics such that $\langle \overline{S}_P, \overline{S}_2, \overline{S}_2' \rangle_{\mathbb{F}_q} = \langle \overline{S}_{2,1}, \overline{S}_{2,2}, \overline{S}_{2,3} \rangle_{\mathbb{F}_q}$
      apply automorphism of $\mathbb{P}^4$ transforming $\overline{S}_P$ into $WZ - X^2$
      $S_2 \leftarrow \mathrm{NaiveLift}(\overline{S}_2)$; $S_2' \leftarrow \mathrm{NaiveLift}(\overline{S}_2')$; $S_2^{\mathrm{pr}} \leftarrow \mathrm{res}_V(S_2, S_2')$
      return $\mathrm{Dehomogenization}_Z(S_2^{\mathrm{pr}}(XZ, YZ, Z^2, X^2))$
    else
      repeat $P \leftarrow \mathrm{Random}(\mathfrak{D}(\overline{C})(\mathbb{F}_q))$ **until** $\chi(P) = 1$
      $\overline{S}_2, \overline{S}_2' \leftarrow$ quadrics such that $\langle \overline{S}_P, \overline{S}_2, \overline{S}_2' \rangle_{\mathbb{F}_q} = \langle \overline{S}_{2,1}, \overline{S}_{2,2}, \overline{S}_{2,3} \rangle_{\mathbb{F}_q}$
      apply automorphism of $\mathbb{P}^4$ transforming $\overline{S}_P$ into $XY - ZW$
      $S_2 \leftarrow \mathrm{NaiveLift}(\overline{S}_2)$; $S_2' \leftarrow \mathrm{NaiveLift}(\overline{S}_2')$; $S_2^{\mathrm{pr}} \leftarrow \mathrm{res}_V(S_2, S_2')$
      return $\mathrm{Dehomogenization}_Z(S_2^{\mathrm{pr}}(XZ, YZ, Z^2, XY))$
  else
    todo
else
  apply automorphism of $\mathbb{P}^4$ transforming space of quadrics in $\mathrm{Ideal}(\overline{C})$ to
      $\langle X^2 - ZV, XY - ZW, XW - YV \rangle_{\mathbb{F}_q}$ (using Lie algebra method)
  $\overline{S}_{3,1}, \overline{S}_{3,2} \leftarrow$ cubics that along with quadrics generate $\mathrm{Ideal}(\overline{C})$
  $\overline{f}_i \leftarrow \mathrm{Dehomogenization}_Z(\overline{S}_{3,i}(XZ, YZ, Z^2, X^2, XY))$ $(i = 1,2)$
  return $\mathrm{NaiveLift}(\gcd(\overline{f}_1, \overline{f}_2))$