UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

A census for curves and surfaces with diophantine stability over finite fields

Brikena Vrioni

Polytechnic University of Catalonia
School of Mathematics and Statistics

A census for Curves and Surfaces with Diophantine Stability over Finite Fields

Brikena Vrioni

This thesis is presented for the Degree of
Doctor of Philosophy

July 2021

To the best of my knowledge and belief this thesis contains no material previously published by any other person except where due acknowledgement has been made. This thesis contains no material which has been accepted for the award of any other degree or diploma in any university.

Brikena Vrioni

“*Verily after hardship comes easy*”

— Qur’an 94:5

Acknowledgements

I am grateful to God for the chance, abilities and inspiration to complete this study.

I would like to thank my supervisor Prof. Joan-Carles Lario for his patience, suggestions and continuous professional advises.

I could not have finished this thesis without full support of my beloved husband, my parents and my sisters. Their love and encouragements have make me stronger and more motivated.

Abstract

An algebraic variety defined over a field is said to have Diophantine stability for an extension of this field if the variety does not acquire *new* points in the extension.

Diophantine stability has a growing interest due to recent conjectures of Mazur and Rubin linked to the well-known Lang conjectures, generalizing the celebrated Falting's theorem on rational points on curves of genus grater or equal than 2. Their framework is characteristic zero, and we shall focus on the analogous and related questions in positive characteristic.

More precisely, the aim of the thesis is to initiate the study of Diophantine stability for curves and surfaces defined over finite fields. First we prove the finiteness of the finite field extensions where an algebraic variety can exhibit Diophantine stability (DS) in terms of its Betti numbers (the genus in the case of curves, the Hodge diamond in the case of surfaces, etc.)

Then, we analyze the existence of curves with Diophantine stability. More precisely, for curves of genus $g \leq 3$ we give the complete list of (isomorphism classes of) DS-curves, and we also provide data on the candidate Weil polynomials for DS-curves of genus $g = 4$ and 5. For curves of large genus, we exhibit certain families of DS-curves: Deligne-Lusztig curves, Carlitz curves, ...

Finally, we also aim to make a contribution on surfaces defined over finite fields with Diophantine stability. From the classification of surfaces of Enriques-Munford-Bombieri we derive partial results and a census of DS-surfaces.

Keywords : Curves and surfaces over finite fields, Diophantine stability.

Contents

Chapter 1

Diophantine stability

In this chapter we introduce the basic terminology and some of the known facts about the objects that constitute the main characters of this memoir. In particular, we review the notions of the Hasse-Weil Zeta function attached to a projective non-singular algebraic variety along with its Weil polynomials, Betti numbers, closed points, etc. We also review the Künneth formula that will be used later. The key concept that shall be present through all chapters is that of Diophantine stability.

1.1 Zeta function

Let V be a non-singular d-dimensional projective algebraic variety over the finite field $\mathbb{F}_q$ of size q. The generating function

$$\zeta_V(t) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m} t^m\right)$$

where $N_m = \#V(\mathbb{F}_{q^m})$ is called the Zeta function of V. The Weil conjectures [41] proven by Dwork and Deligne [14], [10], [11] state:

1. (Rationality) We have

$$\zeta_V(t) = \frac{P_1(t)P_3(t)\dots P_{2d-1}(t)}{P_0(t)P_2(t)\dots P_{2d}(t)}$$

   where $P_i(t) \in \mathbb{Z}[t]$. Always, $P_0(t) = 1 - t$ and $P_{2d}(t) = 1 - q^d t$.

2. (Riemann hypothesis) Writing

$$P_i(t) = \prod_{j=1}^{\beta_i}(1 - \alpha_{ij}t)$$

   all the reciprocal roots satisfy $|\alpha_{ij}| = q^{i/2}$.

3. (Poincaré duality) One has the functional equation

$$\zeta_V(q^{-d}t^{-1}) = \pm q^{dE/2}t^E\zeta_V(t)$$

   where E is the Euler characteristic of V. In particular, the polynomials $P_i(t)$ and $P_{2d-i}(t)$ have the same degree and the sets of their reciprocal roots satisfy

$$\{\alpha_{i1}, \alpha_{i2}, \dots\} = \{\frac{q^d}{\alpha_{2d-i,1}}, \frac{q^d}{\alpha_{2d-i,2}}, \dots\}$$

4. (Betti numbers) If V can be seen as a good reduction of a non-singular projective algebraic variety Y over a number field embedded in the field of complex numbers, then the degree $\beta_i = \deg P_i(T)$ is the ith Betti number of $Y(\mathbb{C})$.

The Weil conjectures in the special case of algebraic curves were conjectured by Emil Artin (1924). The case of curves over finite fields was proved by Weil, finishing the project started by Hasse's theorem on elliptic curves over finite fields. The rationality part of the conjectures was proved first by Dwork (1960), using p-adic methods. Grothendieck (1965) and his collaborators established the rationality conjecture, the functional equation and the link to Betti numbers by using the properties of étale cohomology, a new cohomology theory developed by Grothendieck and Michael Artin for attacking the Weil conjectures. The analogue of the Riemann hypothesis was the hardest to prove. Finally, Deligne (1974) was able to prove it, using the machinery of Grothendieck and his school build up on initial suggestions from Serre.

First example. Consider the projective space $V = \mathbb{P}^d$. One shows that the even Betti numbers are $\beta_{2i} = 1$ and the odd $\beta_{2i+1} = 0$, so that we have

$$\zeta(t) = \frac{1}{(1-t)(1-qt)\dots(1-q^d t)} \,.$$

Indeed, the number of points is given by

$$\#\, \mathbb{P}^d(\mathbb{F}_{q^m}) = (q^{m(d+1)} - 1)/(q^m - 1) = 1 + q^m + q^{2m} + \dots + q^{dm} \,.$$

1.2 Betti numbers

Informally, Betti numbers refer to the number of times that an object can be "cut" before splitting into separate pieces. The β_i are called Betti numbers in honour of the Italian mathematician Enrico Betti, who had taken the first steps of this kind to extend Riemann's work. It was only in the late 1920s that the German mathematician Emmy Noether suggested how the Betti numbers might be thought of.

From the computational point of view, it might be worth to notice the difficulties to compute the Betti numbers for an arbitrary algebraic variety given by a system of defining equations. Also it is a difficult question to ask whether there are examples of algebraic varieties with a prescribed set of Betti numbers β_i.

However, for certain families of algebraic varieties, such as curves and abelian varieties, the corresponding Betti numbers are well known. Moreover, we dispose of certain properties of the Betti numbers. For instance, by Hodge symmetry, we know that $\beta_{2i+1} \equiv 0 \pmod 2$.

1.3 Weil polynomials

With regard to the polynomials $P_i(t) = \prod_{j=1}^{\beta_i}(1 - \alpha_{ij}t)$ with $|\alpha_{ij}| = q^{i/2}$, it is also common to consider the corresponding monic reciprocal polynomials

$$L_i(t) = \prod_{j=1}^{\beta_i}(t - \alpha_{ij}) \,,$$

The polynomials $L_i(t)$ are called Weil polynomials (or L-polynomials), and their roots α_{ij} are called Weil $q^{i/2}$-numbers. The relation between them is

$$L_i(t) = t^{\beta_i} P_i(1/t) \,.$$

The Weil polynomials can be seen as the characteristic polynomial of the Frobenius acting on the étale cohomology of the variety.

Observe that for a given Betti number β_i, there are only a finite number of Weil polynomial candidates $L_i(t)$. Indeed, the coefficients of the monic polynomial $L_i(t) = \sum_{k=0}^{\beta_i} a_{ik}t^k$ satisfy

$$|a_{ik}| \leq |\operatorname{sym}_k(\alpha_{i1}, \ldots, \alpha_{i\beta_i})| \leq \binom{\beta_i}{k} q^{ik/2} \,.$$

For instance, in the case of elliptic curves one has $L_1(t) = q^2 + at + t^2$ with $|a| \leq 2q^{1/2}$. There are smart techniques to compute a list of candidate Weil polynomials. For instance, in the case when i is even, notice that the polynomial $U_i(t) = L_i(q^{i/2}t)$ is a root-unitary polynomial (all roots in the unit circle) with integer coefficients and leading coefficient $q^{\beta_i i/2}$.

For future use, we also introduce the *real* Weil polynomials $h_i(x)$ that have roots the real numbers $\mu_j = \alpha_{ij} + \overline{\alpha}_{ij}$ for $1 \leq j \leq \beta_i$ whenever β_i is even. The real Weil polynomials have degree $\beta_i/2$ and satisfy

$$P_i(t) = t^{\beta_i/2} h_i\left(\frac{q^i t^2 + 1}{t}\right).$$

Given $P_i(t)$, we can find $h_i(x)$ by means of the t-resultant

$$\mathrm{Res}_t(q^i t^2 + 1 - tx, P_i(t) - t^{\beta_i/2} h_i(x)),$$

and vice versa, given $h_i(x)$, we can find $P_i(t)$ by means of the x-resultant

$$\mathrm{Res}_x(q^i t^2 + 1 - tx, P_i(t) - t^{\beta_i/2} h_i(x)).$$

1.4 Cohomology constrains

The cohomology of a particular type of varieties imposes further conditions among the reverse Weil polynomials $P_i(t)$. With regard to this, Tate was able to do some refinement of the Weil conjectures for certain types of varieties.

Let us just mention a couple of examples. For abelian varieties, all the polynomials $P_i(t)$ depend only on the first one $P_1(t)$. Indeed, if

$$P_1(t) = \prod_{j=1}^{2g}(1 - t\alpha_j)$$

then

$$P_i(t) = \prod_{1\le j_1<\cdots<j_i\le 2g}(1 - t\alpha_{j_1}\ldots\alpha_{j_i})$$

Moreover, Tate-Honda theorem describes the possibilities for the first polynomial $P_1(t)$ attached to simple abelian varieties over finite fields [39].

Another example in this direction is Taelman's results in [38] describing some constrains for the Weil polynomials attached to K3 surfaces, or Rybakov's observations in [34] for hyperelliptic surfaces as well. We also refer to [24] and [19] for related computational aspects of Zeta functions.

1.5 Naive inequality

From the Weil conjectures, the number of points $N_m = \#V(\mathbb{F}_{q^m})$ of a non-singular d-dimensional projective variety V over $\mathbb{F}_q$ satisfies the formula

$$N_m = \sum_{i=0}^{2d}(-1)^i \sum_{j=1}^{\beta_i} \alpha_{ij}^m \,.$$

We get the inequality

$$|N_m - (1+q^{dm})| = \left| \sum_{i=1}^{2d-1}(-1)^i \sum_{j=1}^{\beta_i} \alpha_{ij}^m \right| \le \sum_{i=1}^{2d-1} \sum_{j=1}^{\beta_i} |\alpha_{ij}^m| \le \sum_{i=1}^{2d-1} \beta_i q^{im/2} \,.$$

Since we have $\beta_i = \beta_{2d-i}$, we can rewrite the inequality as

$$|N_m - (1+q^{dm})| \le \sum_{i=1}^{d} \beta_i (q^{im/2} + q^{(2d-i)m/2}) \,.$$

Some questions arise: are the Betti numbers bounded for a fixed dimension d? Can one apply optimization (and dual optimization) à la Serre-Oesterlé for optimal varieties (those with maximum number of points over $\mathbb{F}_q$)? Are optimal varieties useful tools for Coding Theory as in the case of curves?

1.6 Diophantine stability

We borrow the term Diophantine stability from Mazur [28] and Mazur-Rubin [29]. The concept of Diophantine stability applies to a sprawling number of scenarios.

For a given algebraic variety V over a field K, we shall say that V has Diophantine stability (or V is a DS-variety) if there exists a proper extension L/K such that $V(L) = V(K)$.

Over number fields, Diophantine stability is closely related to the Lang Conjectures [26]. Just to mention one particular challenging open problem in this direction, we underline the question posed by Mazur-Rubin in the case of curves defined over a number field K: Does the set of number fields where the curve fails to have DS determines the curve up to K-isomorphism?

In this memoir, we shall concentrate on the study of non-singular projective varieties V with DS over finite fields $\mathbb{F}_q$. That is, we are looking at cases where the variety V verifies $V(\mathbb{F}_{q^m}) = V(\mathbb{F}_q)$ for some $m > 1$.

Proposition 1. *Let V be a non-singular projective variety of a given dimension d and given Betti numbers β_i over a finite field. If V is a DS-variety for $\mathbb{F}_{q^m}/\mathbb{F}_q$, then the pair (q, m) is chosen from a finite set.*

Proof. Suppose that $V(\mathbb{F}_q) = V(\mathbb{F}_{q^m})$ for some $m > 1$. One the one hand, we have that $N_1 = \#V(\mathbb{F}_q)$ belongs to the interval centered in $1 + q^d$ and radius $\sum_{i=1}^{2d-1} \beta_i q^{i/2}$ since

$$|N_1 - (1 + q^d)| \leq \sum_{i=1}^{2d-1} \beta_i q^{i/2} .$$

On the other hand, $N_m = \#V(\mathbb{F}_{q^m})$ belongs to the interval centered in $1 + q^{dm}$ and radius $\sum_{i=1}^{2d-1} \beta_i q^{im/2}$ since

$$|N_m - (1 + q^{dm})| \leq \sum_{i=1}^{2d-1} \beta_i q^{im/2} .$$

Since we are assuming that $N_1 = N_m$ with $m > 1$, we need to show that the intersection of these two intervals is always empty except for a finite number of pairs (q, m). Thus, let us show that if q and m are large enough, then

$$(1 + q^d) + \sum_{i=1}^{2d-1} \beta_i q^{i/2} < (1 + q^{md}) - \sum_{i=1}^{2d-1} \beta_i q^{im/2} .$$

The above inequality is equivalent to

$$\sum_{i=1}^{2d-1} \beta_i (q^{i/2} + q^{im/2}) < q^{md} - q^d .$$

Clearly, we have

$$\sum_{i=1}^{2d-1} \beta_i (q^{i/2} + q^{im/2}) < \sum_{i=1}^{2d-1} \beta_i (q^{(2d-1)/2} + q^{(2d-1)m/2}) < q^{md} - q^d$$

when $q^m \gg 0$. $\square$

1.7 Closed points

The Zeta function of an algebraic variety V over $\mathbb{F}_q$ admits the following product formula [35]. We have

$$\zeta_V(t) = \prod_{x \in V^{\mathrm{cl}}} (1 - t^{\deg(x)})^{-1}$$

where V^{cl} denotes the set of closed points of V and $\deg(x)$ is the degree of x. A closed point $x = [P]$ is an equivalent class of points P in $V(\overline{\mathbb{F}}_q)$ under the Galois action over $\mathbb{F}_q$. The degree of x is the degree of the field extension of $\mathbb{F}_q$ generated by the coordinates of P.

In practice, it is very useful also to write the Zeta function as

$$\zeta_V(t) = \prod_{d=1}^{\infty} (1 - t)^{-a_d}$$

where a_d denotes the number of closed points of V of degree d.

It follows that one has the relation with the number of points $N_m = |V(\mathbb{F}_{q^m})|$ given by:

$$N_m = \sum_{d|m} d\, a_d\,,$$

and using the Möebius inversion formula we also have

$$a_d = \frac{1}{d} \sum_{d'|d} \mu(d') N_{d'}\,.$$

1.8 Künneth formula

Let X and Y be two non-singular projective algebraic varieties over $\mathbb{F}_q$. The Künneth theorem [18] for the ℓ-adic cohomolgy states that for any integer k, one has an isomorphism

$$H^k(X \times Y; \mathbb{Q}_\ell) \cong \bigoplus_{i+j=k} H^i(X; \mathbb{Q}_\ell) \otimes H^j(Y; \mathbb{Q}_\ell).$$

For singular homology, the above isomorphism is a natural isomorphism. The map from the sum to the homology group of the product is called the cross product. More precisely, there is a cross product operation by which an i-cycle on X and a j-cycle on Y can be combined to create an $(i+j)$-cycle on $X \times Y$; so that there is an explicit linear mapping defined from the direct sum to $H_k(X \times Y)$.

A consequence of the above isomorphism is that the Betti numbers of $X \times Y$ can be determined from those of X and Y. More precisely, if

$$p_Z(t) = \sum_{k \geq 0} \beta_k(Z) t^k$$

denotes the Poincaré polynomial of a variety Z (the coefficients $\beta_k(Z)$ are the Betti numbers of Z), then one has the equality

$$p_{X \times Y}(t) = p_X(t) p_Y(t).$$

One can take advantage of this formula to derive partial knowledge on the Zeta function of $X \times Y$ in terms of the Zeta functions of X and Y.

Chapter 2

DS-Curves

In this chapter we focus on Diophantine stability for the case of curves. Of course, an important tool to this aim is the Zeta function of the curve. The rationality and the functional equation for the Zeta functions of curves are an easy consequence of the Riemann-Roch theorem. In particular, it can be deduced that the sign in the functional equation is always +1 for curves. Here we shall provide a census of DS-curves of low genus, and provide some other examples including Deligne-Lusztig curves and Carlitz modules.

2.1 Admissible intervals

By the Hasse-Weil-Serre bound, the number of points on a (projective, smooth, geometrically irreducible) curve C of genus $g \geq 1$ defined over a finite field $\mathbb{F}_q$ satisfies

$$|\#C(\mathbb{F}_{q^f}) - (q^f + 1)| \leq g \lfloor 2\sqrt{q^f} \rfloor ,$$

for every integer $f \geq 1$. In this chapter we are interested in the cases where C is Diophantine stable (or simply, C is a DS-curve) for a proper extension $\mathbb{F}_{q^f}/\mathbb{F}_q$; that is, it holds

$$C(\mathbb{F}_q) = C(\mathbb{F}_{q^f}) .$$

With this aim, we introduce the following notations

$$N_{q,f}(g) = \max_X \#X(\mathbb{F}_{q^f})$$

$$n_{q,f}(g) = \min_X \#X(\mathbb{F}_{q^f})$$

where X runs over the genus-g curves defined over $\mathbb{F}_q$. We denote as usual $N_q(g) = N_{q,1}(g)$, and also let $n_q(g) = n_{q,1}(g)$. A genus-g curve over $\mathbb{F}_q$ with $N_q(g)$ rational points is called optimal. A genus-g curve over $\mathbb{F}_q$ with $n_q(g)$ rational points will be called pessimal.

With regard to the optimal bound $N_q(g)$, there are many references available as well as the website manYPoints.org (see [36], [40]). In the cases of lack of information on $N_q(g)$, special mention deserves Oesterlé's bound $N_q(g) \leq B_q(g)$ since it can be used often to beat Serre-Weil's upper bound $q + 1 + g\lfloor 2\sqrt{q^f}\rfloor$. Optimal curves have centered (and still do) the attention of researchers for several decades due to its applications, such as in Coding Theory; however, notice that much less is known on pessimal curves.

For every $f > 1$, we shall consider the intervals

$$I_{q,f}(g) = [n_q(g), N_q(g)] \cap [n_{q,f}(g), N_{q,f}(g)]\,,$$

and we say that (q, f) is an admissible pair relative to g when

$$I_{q,f}(g) \neq \emptyset\,.$$

Admissible pairs encode the possible proper extensions $\mathbb{F}_{q^f}/\mathbb{F}_q$ where a genus-g curve has a chance to have DS (if there is any such a curve).

Proposition 2. *Let $g \geq 1$. The set of all admissible pairs (q, f) relative to g is a finite set.*

Proof. Assume that $I_{q,f}(g)$ is non-empty for some $f > 1$. By the Hasse-Weil bound theorem, the following inequalities hold:

$$q^f + 1 - 2\,g\,\sqrt{q^f} \le n_{q,f}(g) \le N_q(g) \le q + 1 + 2\,g\,\sqrt{q}\,.$$

Hence,

$$q^f \le q + 2\,g\,\sqrt{q} + 2\,g\,\sqrt{q^f}\,.$$

Taking logarithms with base q, one has

$$f \le \log_q \left(q + 2\,g\,\sqrt{q} + 2\,g\,\sqrt{q^f}\right) = \log_q \left(2\,g\,\sqrt{q^f}\left(1 + \frac{q + 2\,g\,\sqrt{q}}{2\,g\,\sqrt{q^f}}\right)\right).$$

By using $f \ge 2$, we get

$$f \le 2\,\log_q(2\,g) + 2\,\log_q \left(1 + \frac{q + 2\,g\,\sqrt{q}}{2\,g\,\sqrt{q^f}}\right) \le 2\,\log_q(2\,g) + 2\,\log_q \left(1 + \frac{q + 2\,g\,\sqrt{q}}{2\,g\,q}\right).$$

On the one hand, for a given finite field size q, we see that the number of possible degrees f is bounded above. On the other hand, the genus g being fixed, one has $f < 2$ as q grows due to the fact $\lim_{x\to\infty} \log_x a = \lim_{x\to\infty} \log a / \log x = 0$. We conclude that the number of admissible pairs (q, f) relative to g is finite. □

As we have already mentioned, in contrast with optimal curves, no much is known about pessimal curves, even for small values of g. For that reason, it is difficult to have exact information on the intervals $I_{q,f}(g)$. The following tables contain the values (q, f) satisfying the inequality

$$q^f + 1 - g\lfloor 2\sqrt{q^f}\rfloor \le q + 1 + g\lfloor 2\sqrt{q}\rfloor.$$

In particular, the tables include the set of admissible pairs (q, f) for genus $g \le 5$.

$g = 1$

q	f
2	$2, 3$
3	2
4	2

$g = 2$

q	f
2	$2, 3, 4$
3	$2, 3$
4	2
5	2

$g = 3$

q	f
2	$2, 3, 4, 5$
3	$2, 3$
4	$2, 3$
5	2
7	2
8	2
9	2

$g = 4$

q	f
2	$2, 3, 4, 5, 6$
3	$2, 3, 4$
4	$2, 3$
5	2
7	2
8	2
9	2
11	2

$g = 5$

q	f
2	$2, 3, 4, 5, 6$
3	$2, 3, 4$
4	$2, 3$
5	$2, 3$
7	2
8	2
9	2
11	2
13	2

Remark 1. *We do not claim that $I_{q,f}(g)$ is non-empty necessarily for all values in the above tables. But we do claim that if the interval $I_{q,f}(g)$ is non-empty then the admissible pair (q, f) should appear in the tables. Moreover, we warn the reader that it can happen that $I_{q,f}(g)$ is non-empty but there is no DS-curve of genus-g for the extension $\mathbb{F}_{q^f}/\mathbb{F}_q$. For instance, this is the case for genus-2 and the admissible pair $(4, 2)$ as we shall see.*

2.2 Genus 1

The case of elliptic curves is by far the easiest. In the following table (and successives), the first column displays the admissible pairs (q, f) relative to g for which there exist DS-curves; the second column shows defining equations of (representatives of the isomorphism classes of) DS-curves for $\mathbb{F}_{q^f}/\mathbb{F}_q$. The third column indicates the number of points $N = \#C(\mathbb{F}_q) = \#C(\mathbb{F}_{q^f})$.

Proposition 3. *The following table displays the set of (isomorphism classes of) genus one curves with DS.*

(q, f)	C	N
$(2, 2)$	$y^2 + y = x^3 + x$	5
$(2, 3)$	$y^2 + y = x^3 + 1$	4
	$y^2 + y = x^3 + x$	5
$(3, 2)$	$y^2 = x^3 + 2\,x + 1$	7
$(4, 2)$	$y^2 + y = x^3$	9

Proof. For every admissible pair (q, f) one proceeds by inspection of the isomorphism classes of elliptic curves over $\mathbb{F}_q$ which can be listed very easily. $\square$

Remark 2. *Notice that the elliptic curve $C : y^2 + y = x^3$ in the last row is in fact defined over $\mathbb{F}_2$ and satisfies $\#C(\mathbb{F}_4) = \#C(\mathbb{F}_{16}) = 9$ but $\#C(\mathbb{F}_2) = 3$.*

2.3 Genus 2

As for genus-2 curves over finite fields $\mathbb{F}_q$, the list of isomorphism classes is practicable for small values of q so that we can get easily the sublist of DS-curves for that genus.

Proposition 4. *The following table displays the isomorphism classes of DS-curves of genus $g = 2$ along with the admissible pairs (q, f).*

(q,f)	C	N
$(2,2)$	$y^2 + (x^2 + x)\,y = x^5 + x^3 + x^2 + x$	3
	$y^2 + x\,y = x^5 + x$	4
	$y^2 + y = x^5 + x^3$	5
	$y^2 + (x^3 + x + 1)\,y = x^5 + x^4 + x^3 + x$	6
$(2,3)$	$y^2 + y = x^5 + x^3 + 1$	1
	$y^2 + x\,y = x^5 + x^2 + x$	2
	$y^2 + y = x^5 + x^4$	5
$(3,2)$	$y^2 = x^5 + 2\,x^4 + 2\,x^3 + 2\,x$	5
$(3,3)$	$y^2 = x^6 + x^4 + x^2 + 1$	8
$(5,2)$	$y^2 = x^5 + 4\,x$	6

Proof. To create the table, we have used the database on isomorphism classes of curves of small genus over finite fields elaborated by Sutherland [37]. □

Remark 3. *According to the tables in Section 2.1, a priori the cases $(q, f) = (2, 4)$ and $(4, 2)$ have a chance to appear for genus-2 DS-curves. Both cases are excluded by inspection of the representatives of isomorphism classes of curves. For instance, in the case $(q, f) = (4, 2)$, it turns out that the interval $I_{4,2}(2) = [0, 10] \cap [7, 33]$ is non-empty, but there are not genus-2 curves over $\mathbb{F}_4$ with $N = \#C(\mathbb{F}_4) = \#C(\mathbb{F}_{16})$ for $N = 7, 8, 9$ or 10. The minimal difference $\#C(\mathbb{F}_{16}) - \#C(\mathbb{F}_4)$ among the genus-2 curves defined over $\mathbb{F}_4$ turns out to be 2 and it is attained by the curve*

$$y^2 + (x^2 + x)\,y = \alpha\,(x^5 + x^3 + x^2 + x)\,.$$

In the equation above and hereafter, for non-prime fields we let α denote a Conway generator of the finite field $\mathbb{F}_q = \mathbb{F}_p(\alpha)$; that is, α is a root of the Conway polynomial defining the extension $\mathbb{F}_q/\mathbb{F}_p$ where p is the prime characteristic.

2.4 Genus 3

For genus-3 curves, things begin to get more intricate. Still we can make use of Sutherland's database. However, the database does not cover yet all the isomorphism classes of genus-3 curves defined over the finite fields for all the cases with potential presence of Diophantine stability. To be more precise, from Sutherland's database, we lack the following isomorphism classes of genus-3 curves:

- Hyperelliptic curves over $\mathbb{F}_4$;
- Hyperelliptic curves over $\mathbb{F}_8$;
- Non-hyperelliptic curves over $\mathbb{F}_7$;
- Non-hyperelliptic curves over $\mathbb{F}_8$.

Luckily, we shall be able to either justify the absence of DS-curves or to find the ones with Diophantine stability in the isomorphism classes under-construction in Sutherland's database. Hence, we can (and do) provide the complete list of DS-curves of genus 3.

Theorem 1. *The following tables display, for every pair (q, f), all the genus-3 DS-curves over finite fields. We first display the hyperelliptic curves followed by the plane quartics defining equations for the non-hyperelliptic curves.*

(q,f)	C	N
$(2,2)$	$y^2+(x+x^2)\,y=x^7+x^6+x^5+x$	3
	$y^2+(x+x^2)\,y=x^7+x^6+x^5+x^4+x^2+x$	3
	$y^2+x\,y=x^7+x^6+x^2+x$	4
	$y^2+x\,y=x^7+x^6+x^5+x$	4
	$y^2+(x^2+x^4)\,y=x^5+x^4+x^3+x$	4
	$y^2+y=x^7+x^6$	5
	$y^2+(x^4+x^2+x+1)\,y=x^7+x^5+x^4+x^3$	5
	$y^2+(x^4+x^2+x)\,y=x^6+x^3+x^2+x$	5
	$y^2+(x^4+x+1)\,y=x^7+x^5+x^4+x^3+x^2+x$	6
	$x^4+x^3y+y^4+x^2y+y^3+x+1$	0
	$x^4+x^3y+y^4+x^3+x$	1
	$x^4+xy^3+y^4+x^3+x^2y+xy^2+x$	1
	$x^3y+xy^3+y^4+x^2y+x$	2
	$x^3y+xy^3+y^4+xy^2+x$	2
	$x^4+x^3y+xy^3+x^3+xy^2+y^2+x$	2
	$x^4+x^2y^2+xy^3+x^3+x^2y+y^2+x$	2
	$x^3y+xy^3+y^4+x^3+x$	3
	$x^4+x^3y+x^3+y^3+x$	3
	$x^3y+x^2y^2+x^2y+y^3+x$	4
	$x^3y+x^2y^2+x^3+y^3+y^2+x$	7

(q,f)	C	N
$(2,3)$	$y^2+(x^2+x+1)\,y=x^7+x^6+x^5+x^4+x^3+x+1$	1
	$y^2+(x^4+x+1)\,y=x^8+x^5+x+1$	2
	$y^2+(x^4+x)\,y=x^8+x^7+x^5+x$	2
	$y^2+x\,y=x^7+x^2+x$	2
	$y^2+(x^4+x^2)\,y=x^8+x^4+x^2+x$	2
	$y^2+(x^4+x^2+1)\,y=x^2+x+1$	2
	$y^2+(x^4+x+1)\,y=x^6+x^5+x^4+x^3+1$	2
	$y^2+(x^2+x)\,y=x^7+x^6+x^5+x$	3
	$y^2+y=x^7$	3
	$y^2+(x^2+x+1)\,y=x^7+x^6+x^5+x^2+x+1$	3
	$y^2+y=x^7+x^6+x^4+1$	3
	$y^2+x\,y=x^7+x^6+x^5+x$	4
	$y^2+(x^4+x+1)\,y=x^6+x^4+x^3+x^2+x+1$	4
	$y^2+(x^3+1)\,y=x^7+x^4$	4
	$y^2+(x^4+x^2)\,y=x^4+x$	4
	$y^2+(x^4+x+1)\,y=x^8+x^4+x^2+x$	4
	$y^2+(x^4+x^2+1)\,y=x^4+x$	6
	$y^2+(x^4+x+1)\,y=x^6+x^5+x^3+x$	6
	$x^4+x^2y^2+y^4+x^2y+xy^2+x$	3
	$x^2y^2+x^3+y^3+x^2+xy+x$	4
	$x^4+xy^3+x^2y+y^2+x$	4
	$x^3y+y^4+x^3+x$	5
	$x^2y^2+y^4+x^3+x^2y+xy^2+x$	5

(q,f)	C	N
$(2,4)$	$x^3y+x^2y^2+x^3+y^3+y^2+x$	7
$(2,5)$	$y^2+(x^4+x+1)\,y=x^8+x^6+x^5+x^4+x^3+x^2$	4
	$y^2+(x^4+x^2+1)\,y=x^4+x$	6
	$x^4+x^2y^2+y^4+x^2y+xy^2+x^2+xy+y^2+1$	0
$(3,2)$	$y^2=x^7+2x^6+x^5+x^4+x^3+2x^2+1$	5
	$y^2=x^8+2x^5+2x^4+2x^2+2x$	6
	$y^2=2x^7+2x^4+2x^3+2x^2+1$	6
	$y^2=x^7+x^6+2x^5+x^4+x^3+2x^2+2x$	6
	$y^2=x^7+2x^6+2x^5+x^3+x^2+2x+1$	7
	$y^2=x^8+2x^7+x^6+2x^3+2x^2+1$	7
	$y^2=x^8+2x^6+x^4+2x^3+2x^2+x+1$	8
	$x^4-x^2y^2-y^4+x^3-x$	1
	$x^4+x^2y^2-y^4+x^3-x$	1
	$x^4-x^3y-y^4+x^3-xy-x$	1
	$x^4-x^3y-y^4+xy^2-x$	2
	$x^4+x^3y-y^4+x^3-x^2y+xy^2-x$	2
	$x^4+x^3y+x^2y^2+y^4-x^2+xy+x$	2
	$x^4+x^3y-xy^3+x^3+x^2y-y^2-x$	2
	$x^4+x^3y+x^2y^2-xy^3-x^3-x^2-y^2-x$	2
	y^4-x^3+x	4
	$x^3y+y^4-xy^2+x$	5
	$x^2y^2-y^4+x^3-x$	10
$(3,3)$	$y^2=2x^8+2x^7+x^6+2x^5+x^4+2x^2+x+2$	3
	$y^2=x^8+2x^7+2x^6+2x^5+x^2+x$	4
	$y^2=x^7+x^6+2x^5+x^4+x^3+x^2+2x$	4
	$y^2=x^8+x^4+2x^2+1$	4
	$y^2=x^8+2x^7+2x^5+2x^4+x^3+x+1$	8

(q,f)	C	N
$(4,2)$	$y^2 + (x^2 + x + 1)\, y = x^7 + x^6 + x^5 + x^3 + x^2 + x$	7
	$y^2 + (x^4 + x^2 + 1)\, y = x^5 + x^2$	8
	$y^2 + (x^4 + x^2 + x + 1)\, y = x^5 + x^3 + x^2 + x$	9
	$\alpha\, x^4 + \alpha\, x^3\, y + \alpha\, x^2\, y^2 + x + y^4$	1
	$\alpha\, x^4 + \alpha^2\, x^3\, y + \alpha^2\, x^2\, y^2 + x + y^4$	1
	$\alpha^2\, x^4 + \alpha\, x^3 y + \alpha\, x\, y^3 + x + y^4$	2
	$\alpha\, x^4 + \alpha^2\, x^3\, y + \alpha^2\, x\, y^3 + x + y^4$	2
	$\alpha^2\, x^4 + x^3\, y + \alpha\, x^2\, y^2 + \alpha^2\, x^2\, y + x\, y^3 + \alpha\, x\, y^2 + x\, y + x + y^2$	2
	$x^4 + x^3 + \alpha\, x^2\, y^2 + \alpha\, x^2\, y + x\, y^3 + \alpha^2\, x\, y^2 + x\, y + x + y^2$	2
	$x^3 y + x^2 y^2 + x^3 + y^3 + y^2 + x$	7
	$x^4 + x y^3 + x^2 y + y^2 + x$	14
	$x^4 + x^2 y^2 + y^4 + x^2 y + x y^2 + x^2 + x y + y^2 + 1$	14
$(5,2)$	$y^2 = x^7 + x^5 + 3\, x^3 + x$	10
$(9,2)$	$x^4 + y^4 + z^4$	28

Proof. The proof follows the same arguments as for genus ≤ 2 by inspection but, in addition, we must analyze the cases not covered in Sutherland's database. To do so, we shall explain in Sections 2.5 and 2.6 how to obtain the list of all candidate L-polynomials for (potential) DS-curves of genus g attached to the pair (q,f). If the list is empty, we are done. It happens to be so in all the cases under-construction on Sutherland's database, except for the genus-3 cases: hyperelliptic with $(q,f) = (4,2)$, and non-hyperlliptic with $(q,f) = (7,2)$.

As for the case hyperelliptic with $(q,f) = (4,2)$, we proceed to build the census of all (isomorphism classes of) hyperelliptic curves over $\mathbb{F}_4$. We present the Magma code in the Appendix, which is an adaption of the code provided by Xarles in [42] for hyperlliptic curves over $\mathbb{F}_2$. There are 2162 isomorphism classes of hyperelliptic curves over $\mathbb{F}_4$, of which three are DS-curves for $\mathbb{F}_{4^2}/\mathbb{F}_4$; in fact, these three DS-curves can be defined over $\mathbb{F}_2$.

With regard to the non-hyperelliptic case with $(q, f) = (7, 2)$, we proceed as follows. By using the Algorithm Two in Section 2.6, one finds that there is a unique candidate L-polynomial:

$$L(t) = (t^2 + 5\,t + 7)(t^4 - 13\,t^2 + 49)\,.$$

The real Weil polynomial of $L(t)$ turns out to be:

$$h(x) = P_1(x)P_2(x) = (x + 5)(x^2 - 27)\,.$$

Recall that the roots of the real Weil polynomial $h(x)$ are $\mu_i = \alpha_i + \overline{\alpha}_i$, where α_i are the roots of $L(t)$. Since the resultant of $P_1(x)$ and $P_2(x)$ equals -2, we can apply Theorem 1 and Theorem 2 in [21]. Thus, if there is a genus-3 curve C with the given Weil polynomial, then it must be a double cover of a curve D such that either:

(a) D is a genus-2 curve with Weil polynomial $t^4 - 13t^2 + 49$, or

(b) D is a genus-1 curve with Weil polynomial $t^2 + 5t + 7$.

Case (a) does not work, because there is no genus-2 curve with Weil polynomial $t^4 - 13t^2 + 49$, by using either Algorithm Two again or by the Theorem on page 335 of [27].

So we must be in case (b). Note that $\#D(\mathbb{F}_7) = 13$. We can ask how many of these rational points of D split in the double cover $C \longrightarrow D$, and how many ramify, and how many are inert. Since we have $\#C(\mathbb{F}_7) = 13$ and $\#C(\mathbb{F}_{49}) = 13$, no rational points of D are inert, so every rational point either splits or is ramified in the double cover $C \longrightarrow D$. If we let S be the number of split points and R be the number of ramified points, then

$$\begin{aligned} S + R &= \#D(\mathbb{F}_7) = 13 \\ 2S + R &= \#C(\mathbb{F}_7) = 13, \end{aligned}$$

so $S = 0$ and $R = 13$. But from the Riemann–Hurwitz formula, we see that only 4 geometric points of D ramify. Thus, (b) cannot hold either.

We reach to the conclusion that such quartic curve over $\mathbb{F}_7$ with the above Weil polynomial does not exist and this completes the classification of DS-curves of genus 3 over finite fields. □

The task of supplying the isomorphism classes of curves for genus $g \geq 4$ defined over finite fields (even of small size) gets quickly impracticable and it is at present out of reach; with the exception for genus $g = 4$ over $\mathbb{F}_2$, for which Xarles has been able to elaborate the complete list of isomorphism classes in [43]. In fact, we shall deal with this case in Section 2.7. Before discussing cases with larger genus, we manage two algorithms to produce the list of candidates for the L-polynomials of DS-curves of a fixed genus.

2.5 Algorithm One

The following algorithm offers a first approach to examine the presence or absence of DS-curves over finite fields.

Input: An integer $g \geq 1$ and a pair (q, f) where q is a prime power and $f > 1$.

Output: A complete list of L-polynomial candidates for DS-curves of genus g for $\mathbb{F}_{q^f}/\mathbb{F}_q$. The empty list means the absence of DS-curves for these values.

Let a_d denote the number of places (closed points) of degree d for a curve of genus g defined over $\mathbb{F}_q$. Clearly, the DS condition implies that some number a_d

must be zero since one has

$$N_n = \#C(\mathbb{F}_{q^n}) = \sum_{d|n} da_d \,.$$

However, observe that the converse is not necessarily true: one could have $a_6 = 0$ and absence of DS, since it might happen the number of points over $\mathbb{F}_{q^6}$ to be $N_6 = a_1 + 2a_2 + 3a_3 + 6a_6$ with $a_1a_2a_3 \neq 0$. We do not know such an example.

The Algorithm One consists in the following steps:

Step 1. Create the list of integers a_1 in $[q^f + 1 - g\lfloor 2q^{(f/2)}\rfloor, N_g(q)]$ provided that the interval is non-empty, whenever we know the optimal value $N_g(q)$; otherwise, we use Oesterlé's bound or $q + 1 + g\lfloor 2q^{1/2}\rfloor$ instead.

Step 2. Choose a double-positive function $F(t) \gg 0$, $F(t) = 1+2\sum_{n\geq 1} c_n \cos(nt)$. We can (and do) take $F(t)$ such that $c_n = 0$ for all $n > g$ and $c_1 \neq 0$. From the Weil-Serre explicit formulas (see [36], page 96), on has

$$\sum_{d\geq 2} da_d \left(\sum_{d|n} c_n q^{-n/2}\right) \leq g + \sum_{n\geq 1} c_n q^{n/2} + (1 - a_1) \sum_{n\geq 1} c_n q^{-n/2} \,,$$

so that we get the list of all positive integers $[a_1, a_2, a_3, \ldots, a_g]$ satisfying the inequality above. Since all the coefficients of the a_d in the above inequality are non-zero for $d \leq g$, we can guarantee that the list of candidates $[a_1, a_2, a_3, \ldots, a_g]$ is a finite list. Whenever $f \leq g$, we keep only the candidates $[a_1, a_2, a_3, \ldots, a_g]$ such that $a_f = 0$ (if any).

Step 3. For each candidate $[a_1, a_2, a_3, \ldots, a_g]$, we form the real Weil polynomial

$$h(x) = \prod_{i=1}^{g} (x - u_i) \in \mathbb{Z}[x]$$

with $u_i = \pi_i + \overline{\pi}_i$. To this end, we first compute the reverse of the L-polynomial

$P(t) = \prod_{i=1}^{g}(1-\pi_i t)(1-\overline{\pi}_i t)$ by using the Zeta function of the eventual curve

$$Z(t) = \prod_{d\geq 1} \frac{1}{(1-t^d)^{a_d}} = \frac{P(t)}{(1-t)(1-qt)}\,.$$

Step 4. We pass a Sturm filter; that is, we form the Sturm sequence attached to $h(x)$ in order to check whether or not all the roots of $h(x)$ are real and belong to the interval $[-2\sqrt{q}, 2\sqrt{q}]$. In this step the most part of candidates $[a_1, a_2, a_3, \ldots, a_g]$ are suppressed.

Step 5. Finally, we discard all the cases where the polynomials $h(x)$ are not "strongly relatively prime". That is, if $h(x)$ factors over $\mathbb{Z}[x]$ as $P_1(x)P_2(x)$ with resultant $\mathrm{Res}_x(P_1, P_2) = \pm 1$ then $h(x)$ does not arise from a curve. See Serre's book [36], Theorem 2.4.1.

Step 6. If $f > g$ then compute a_f from $[a_1, a_2, a_3, \ldots, a_g]$ and the rational expression of the Zeta function $Z(t)$ in order to check whether a_f is zero or not. More precisely, we can use the Möebius inversion formulas

$$N_n = \sum_{d|n} d a_d \quad \text{and} \quad a_n = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d}) N_d\,.$$

where $N_d = q^d + 1 - s_d$ with $s_d = \sum_{i=1}^{2g} \pi_i^d$ and $|\pi_i| = q^{1/2}$.

There are two delicate points in the above algorithm. The first one is choosing an appropriate double-positive function in Step 2. Even with a good choice of $F(t) \gg 0$, it can happen that we end up with an enormous list of candidates $[a_1, a_2, \ldots, a_g]$ making the algorithm unfeasible. Indeed, observe that every a_d should range from 0 up to a certain bound which makes the algorithm explode very quickly if the bound is not sharp enough. To avoid these problems, we can proceed with an alternative route as presented in the next Section. The idea is to select the candidates just letting each a_d range over a shorter interval of positive integers.

2.6 Algorithm Two

To improve the above algorithm collecting the candidate reverse L-polynomials $P(t)$ for DS-curves, we fix g and q, and then start with the formal identity

$$\frac{(1-t)(1-qt)}{(1-t)^{a_1}(1-t^2)^{a_2}\dots(1-t^g)^{a_g}} = P(t)\prod_{d\geq g}(1-t^d)^{a_d}\,,$$

where again a_d denotes the number of places of degree d. The rational function on the left-hand side of the equality has no pole at $t=0$ (it takes the value 1) so that we can rewrite it as $\sum_{n=0}^{g} A_n t^n + O(t^{g+1})$. As for the right-hand side, it takes the form $P(t)[g]+O(t^{g+1})$, where $P(t)[g]$ is the truncated polynomial cut-off of $P(t)$ up to degree g. The q-palindromic properties of the L-polynomial allow us to reconstruct the degree-$2g$ polynomial $P(t)$ from $\sum_{n=0}^{g} A_n t^n$. Here, we are considering the coefficients $A_i = A_i(a_1,\dots,a_g)$ as formal polynomial expressions in the variables $a_1, \dots, a_g$.

Now, by means of the resultant

$$\mathrm{Res}_t(q\,t^2 - t\,x + 1, P(t) - t^g h(x))\,,$$

we get the (potential) real Weil polynomial

$$h(x) = x^g + H_1x^{g-1} + \cdots + H_{g-2}x^2 + H_{g-1}x + H_g$$

where each $H_i = H_i(a_1,\dots,a_g)$ is a polynomial expression in $\mathbb{Q}[a_1,\dots,a_g]$.

Proposition 5. *For every $1\leq i\leq g$, the polynomial $H_i(a_1,\dots,a_g)$ has multi-degree $(1,0,\dots,0)$ in the variables $(a_i,a_{i+1},\dots,a_g)$. In other words, we can write $H_i = H_i(a_1,a_2,\dots,a_i)$ linearly in the variable a_i.*

Proof. First, we prove that the degree g polynomial $P(t)[g] = \sum_{n=0}^{g} A_n t^n$, truncated of the reverse L-polynomial $P(t)$ up to $O(t^{g+1})$ with indeterminate coefficients $A_k = A_k(a_1,a_2,\dots,a_g)$, satisfies the reverse statement. That is, we want to show that every polynomial $A_k = A_k(a_1, a_2, \ldots, a_g) = A_k(a_1, a_2, \ldots, a_k)$ does not depend on $a_{k+1}, \ldots, a_g$ and it is of degree one in the variable a_k. We have $A_0(a_1, a_2, \ldots, a_g) = 1$ and $A_1(a_1, a_2, \ldots, a_g) = a_1 - (q+1)$. The polynomial $A_k(a_1, a_2, \ldots, a_g)$ is the kth coefficient of the Taylor series of

$$\frac{(1-t)(1-qt)}{(1-t)^{a_1}(1-t^2)^{a_2}\ldots(1-t^g)^{a_g}} =$$

$$(1-t)(1-qt)(1-t)^{-a_1}(1-t^2)^{-a_2}\ldots(1-t^g)^{-a_g} =$$

$$(1-t)(1-qt)\left(\sum_{n=0}^{\infty}\binom{-a_1}{n}(-t)^n\right)\left(\sum_{n=0}^{\infty}\binom{-a_2}{n}(-t)^{2n}\right)\left(\sum_{n=0}^{\infty}\binom{-a_g}{n}(-t)^{gn}\right)$$

where $\binom{\alpha}{n}$ denotes the generalized binomial number. To compute the coefficient of t^k we only need to take care of the partial product

$$(1-(q+1)t-qt^2)\prod_{i=1}^{k}\left(\sum_{n=0}^{\infty}\binom{-a_i}{n}(-t)^{in}\right).$$

Therefore $A_k = A_k(a_1, a_2, \ldots, a_g) = A_k(a_1, a_2, \ldots, a_k)$ does not depend on the variables $a_{k+1}, \ldots, a_g$. The unique contribution of a_k into the coefficient of t^k occurs in

$$(1-(q+1)t-qt^2)\left(\sum_{n=0}^{\infty}\binom{-a_k}{n}(-t)^{kn}\right)$$

and it is equal to $-\binom{-a_k}{1} = a_k$.

The claim on the coefficients of the real Weil polynomial $h(x)$ follows from the equality

$$P(t) = t^g h\left(\frac{qt^2+1}{t}\right).$$

Indeed, letting $P(t) = \sum_{n=0}^{2g} A_n t^n$ with $A_k = q^{k-g}A_{2g-k}$ for $k > g$, and

$h(x) = \sum_{n=0}^{g} H_n x^{g-n}$ with $H_0 = 1$, one has

$$\sum_{n=0}^{2g} A_n t^n = t^g \left(\sum_{n=0}^{g} H_n \left(\frac{qt^2+1}{t} \right)^{g-n} \right) = \sum_{n=0}^{g} H_n (qt^2+1)^{g-n} t^n =$$

$$\sum_{n=0}^{g} H_n \sum_{k=0}^{g-n} \binom{g-n}{k} q^k t^{2k+n} = \sum_{n=0}^{2g} \left(\sum_{\substack{k=0 \\ k \equiv n(2)}}^{n} H_k \binom{g-k}{(n-k)/2} q^{(n-k)/2} \right) t^n .$$

Hence, for $0 \leq n \leq 2g$, it holds

$$A_n = \sum_{\substack{k=0 \\ k \equiv n(2)}}^{n} H_k \binom{g-k}{(n-k)/2} q^{(n-k)/2} .$$

The matrix of the corresponding linear system is lower triangular and invertible. Thus, the inverse matrix is upper triangular and it follows that $H_i = H_i(a_1, \ldots, a_i)$ and of degree one in a_i as desired, since we have proved the same property for the polynomials $A_i = A_i(a_1, \ldots, a_i)$ for $i \leq g$ and $A_i = q^{i-g} A_{2g-i}$ for $i > g$. $\square$

The roots of $h(x)$ must be real and contained in the interval $[-2\sqrt{q}, 2\sqrt{q}]$. The same assertion holds also for the derivatives of $h(x)$. Then, we proceed by recursion as follows.

Start with a candidate of length one $[a_1]$, with a_1 in the Hasse-Weil-Serre interval. By increasing i from 2 to g, suppose we have the list of partial candidate sequences of length $i-1$. For each one of the candidates $[a_1, a_2, \ldots, a_{i-1}]$, we substitute these values it into the $(g-i)$th derivative

$$h^{(g-i)}(x) = T_i(x) + t(a_i)$$

where $T_i(x)$ is a degree-i polynomial in $\mathbb{Q}[x]$ with no constant term, and $t(a_i) = (g-i)!\, H_i(a_1, \ldots, a_{i-1}, a_i)$ is a linear polynomial in $\mathbb{Q}[a_i]$ due to Proposition 5.

Obviously, we do not know how to compute the roots of $h^{(g-i)}(x)$ since we do not know the value of a_i, but we can (and do) compute the roots of $T_i(x)' \in \mathbb{Q}[x]$.

Let $\alpha_1, \ldots, \alpha_{i-1}$ be the roots of $T_i(x)'$. By recursion, we know that all of them are real and belong to the interval $[-2\sqrt{q}, 2\sqrt{q}]$ since they are also the roots of $h^{(g-i+1)}(x)$. We also let $\alpha_0 = -2\sqrt{q}$ and $\alpha_i = 2\sqrt{q}$. For even i, let denote

$$m = \max_{j \text{ odd}}\{T_i(\alpha_j)\} \qquad M = \min_{j \text{ even}}\{T_i(\alpha_j)\}$$

and, for odd i, let

$$m = \max_{j \text{ even}}\{T_i(\alpha_j)\} \qquad M = \min_{j \text{ odd}}\{T_i(\alpha_j)\}\,.$$

Finally, it remains to solve the linear inequalities in integers

$$0 \leq a_i\,, \quad t(a_i) \leq \min\{M, |m|\}$$

when i is even, or

$$0 \leq a_i\,, \quad t(a_i) \leq \min\{|M|, m\}$$

when i is odd, since we want the translates $h^{(g-i)}(x) = T_i(x) + t(a_i)$ to have all the roots in $[-2\sqrt{q}, 2\sqrt{2}]$.

Let us illustrate the Algorithm Two with an example.

The elephant silhoutte. Take genus $g = 5$ and finite field of size $q = 2$. Assume we start with $[a_1] = [9]$. Formally, the real Weil polynomial is given by

$$\begin{aligned} h(x) = \;& x^5 + 6x^4 + (10 + a_2)\,x^3 + (6a_2 + a_3)\,x^2 + \\ & \frac{1}{2}\left(a_2^2 + 29a_2 + 12a_3 - 20 + 2a_4\right)x + \\ & (3\,a_2^2 + a_2a_3 + 27a_2 + 16a_3 + 6a_4 - 12 + a_5)\,. \end{aligned}$$

The fourth derivative $h^{(4)}(x) = 24(6 + 5x)$ has root $\alpha = -6/5$, and the third derivative is

$$h^{(3)}(x) = 6(10x^2 + 24x) + 6(10 + a_2)\,.$$

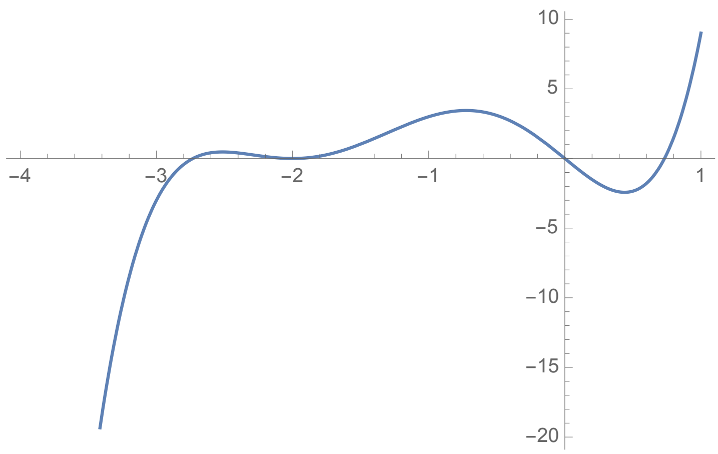
So $T_2(x) = 6(10x^2 + 24x)$ and $T_2(-6/5) = -432/5$. Hence, we want

$$6(10 + a_2) \leq 432/5 = 86.4$$

which amounts to $a_2 \leq 4$. At this point, our list of partial length 2 candidates is $[9,0]$, $[9,1]$, $[9,2]$, $[9,3]$, and $[9,4]$. Keep going on the procedure, at some point we get the partial candidate $[9,0,0,2]$. A priori, since we know that $N_5 = a_1 + 5a_5 \leq 2^5 + 1 + 2g\sqrt{2^5} = 89.5685$, we must have $a_5 \leq 16$. But our strategy performs better. The real Weil polynomial attached to the sequence $[9,0,0,2,a_5]$ is

$$h(x) = x^5 + 6x^4 + 10x^3 - 8x + a_5\,.$$

In the figure below, the elephant silhouette corresponds to the plot of the polynomial $T_5(x) = x^5 + 6x^4 + 10x^3 - 8x$ and it suggests that the possible values of a_5 (if any) are very limited once we have obtained the previous values $[a_1, a_2, a_3, a_4]$.



Indeed, one has that the unique polynomial $h(x)$ obtained as a translation by positive integers from $T_5(x)$ and having the five reals roots in $[-2\sqrt{2}, 2\sqrt{2}]$ is achieved by $a_5 = 0$.

The example above corresponds to the DS-curve of genus 5 over $\mathbb{F}_2$ with $[a_1, a_2, a_3, a_4, a_5] = [9,0,0,2,0]$ given by the affine equation

$$y^4 + (x^2 + x + 1)y^2 + (x^2 + x)y + x^7 + x^3 = 0\,.$$

Its reverse L-polynomial is:

$$32t^{10} + 96t^9 + 160t^8 + 192t^7 + 184t^6 + 144t^5 + 92t^4 + 48t^3 + 20t^2 + 6t + 1\,.$$

Remark 4. *We present in the Appendix the code of a Mathematica program that we have elaborated to perform the search of candidate L-polynomials following the above Algorithm Two. It should be notice that, a posteriori, we learned the inclusion of the function* `Weil_polynomials()` *in Sagemath [13] (after version 9.1). However, it should be noticed that this Sage function is less efficient with regard our purposes since its functionality does not require the sequence of numbers of points for the (eventual) curve to be a sequence of positive integers.*

2.7 Genus 4

Recall that the list of admissible pairs (q, f) for curves of genus $g = 4$ is given by the values in the table:

$g = 4$

q	f
2	$2, 3, 4, 5, 6$
3	$2, 3, 4$
4	$2, 3$
5	2
7	2
8	2
9	2
11	2

Xarles in [43] gives an algorithm to build the complete list of isomorphism classes of genus-4 curves over $\mathbb{F}_2$. Hence, we can extract from that list the genus-4 DS-curves over $\mathbb{F}_2$.

When the size of the finite field is $q > 2$, we must content ourselves producing the list of candidate L-polynomials for DS-cruves by means of the Algorithm Two presented in Section 2.6. Serre and Howe-Lauter's resultant methods allow us to eliminate some candidates. Nonetheless, the final list of curves (over $\mathbb{F}_2$) along with the list of candidate L-polynomials (for $q > 2$) is too large to be included in this memoir. Instead, we refer to the web page:

`https://web.mat.upc.edu/joan.carles.lario/DS.html`

where the corresponding data can be read.

Now, we display the data about the ratio between candidate L-polynomials with DS and the total amount of candidate L-polynomials:

$(q.m)$	# DS	# total
$(2,2)$	188	1 645
$(2,3)$	193	1 645
$(2,4)$	36	1 645
$(2,5)$	44	1 645
$(2,6)$	0	1 645
$(3,2)$	457	10 963
$(3,3)$	110	10 963
$(3,4)$	0	10 963
$(4,2)$	693	45 763
$(4,3)$	9	45 763
$(5,2)$	409	132 839
$(7,2)$	41	705 593
$(8,2)$	8	1 371 739
$(9,2)$	4	2 484 783
$(11,2)$	0	6 718 947

Let us illustrate how results of Serre and Howe-Lauter can be used to discard some of the DS-candidates. To this end, we shall recall the criteria used to eliminate the existence of curves with certain real Weil polynomials or to ensure the existence of double-covers with real Weil polynomial a factor of the given one.

Throughout, we shall make use of the isogeny class of abelian varieties attached to the real Weil polynomial by the Tate-Honda theorem (see [39], [17]). First, we have the following Serre's criterion in [36].

Theorem 2 (Serre (2020), Theorem 2.4.1)**.** *Suppose the real Weil polynomial h of an abelian variety factors in $\mathbb{Z}[x]$ as $h_1 h_2$, where h_1 and h_2 are nonconstant polynomials with* $\text{resultant}(h_1, h_2) = \pm 1$. *Then there is no curve with real Weil polynomial h.*

Howe in [20] gives a method to tell whether or not an isogeny class of ordinary abelian varieties contains a principally polarized variety. An isogeny class that does not contain principally polarized varieties does not contain Jacobians. Thus, we can use this criterion to eliminate DS-candidates.

Recall that equivalent conditions for a g-dimensional abelian variety A over $\mathbb{F}_q$ to be ordinary are:

(i) The coefficient of t^g in its Weil polynomial is coprime to q.

(ii) The constant term of its real Weil polynomial h is coprime to q.

(iii) If p is the prime divisor of q, then the p-torsion subscheme $A[p]$ is the product of a reduced group scheme and a local group scheme with reduced dual.

The above results of Howe were generalized and, in particular, derived in the following practical criterion:

Theorem 3 (Howe-Lauter (2012), see [22])**.** *If a curve C has real Weil polynomial $h = h_1 h_2$, where the reduced resultant of h_1 and h_2 is 2, then C is a double cover of a curve D whose real Weil polynomial is either h_1 or h_2.*

Here, the reduced resultant of h_1 and h_2 is defined as follows. Let r_i be the radical of h_i; that is, the product of the prime factors of h_i. Let n be the positive generator of the ideal $(r1, r2) \cap \mathbb{Z}$. We call n the reduced resultant of h_1 and h_2.

Let us apply these criteria to the case $(q, m) = (4, 3)$. For every DS-candidate, we list its Weil polynomial along with its real Weil polynomial:

Case	$L(t)$	$h(x)$
a	$(t-2)^4(t^2+2t+4)^2$	$(x-4)^2(x+2)^2$
b	$(t-2)^2(t^2+t+4)(t^2+2t+4)^2$	$(x+2)(x^3+x^2-13x-23)$
c	$(t^2+2t+4)^2(t^4-2t^3+t^2-8t+16)$	$(x-4)(x+3)(x+2)^2$
d	$(t^2+2t+4)(t^6-14t^3+64)$	$(x+2)^2(x^2-2x-7)$
e	$(t^2+2t+4)(t^6+t^5-t^4-15t^3-4t^2+16t+64)$	$(x+2)(x^3-12x-14)$
f	$(t-2)^2(t^2+3t+4)(t^2+2t+4)^2$	$(x-4)(x+1)(x+2)^2$
g	$(t^2+t+4)^2(t^2+2t+4)^2$	$(x+2)^2(x+3)^2$
h	$(t^2+t+4)(t^2+3t+4)(t^2+2t+4)^2$	$(x+1)(x+3)(x+2)^2$
i	$(t^2+2t+4)^2(t^2+3t+4)^2$	$(x+1)^2(x+2)^2$

Case a: The reduced resultant of $h_1(x) = (x-4)^2$ and $h_2(x) = (x+2)^2$ is equal to 6. Thus, we cannot apply neither Serre's or Howe-Lauter criteria.

Case b: The resultant of $h_1(x) = x+2$ and $h_2(x) = x^3+x^2-13x-23$ is equal to -1. Serre's criterion applies so that there is not any DS-curve in this case.

Case c: The different choices of h_1 and h_2 give rise to reduced resultants -6, 7, and 42 so that we cannot apply the above criteria.

Case d: The resultant of $h_1(x) = (x+2)^2$ and $h_2(x) = x^2-2x-7$ is equal to 1. Serre's criterion applies so that there is not any DS-curve in this case.

Case e: The resultant of $h_1(x) = x+2$ and $h_2(x) = x^3-12x-14$ is equal to 2. Howe-Lauter criterion ensures that C is a double-cover of a curve D with real Weil polynomial either $x+2$ or $x^3-12x-14$. From the real Weil polynomials we obtain the following possibilities:

# of points over $\mathbb{F}_q$	$\mathbb{F}_4$	$\mathbb{F}_{4^2}$	$\mathbb{F}_{4^3}$
genus$(C) = 4$	8	18	8
genus$(D) = 1$	7	21	49
genus$(D) = 3$	6	14	24

The Hurwitz formula yields to

$$2\,\text{genus}(C) - 2 = 2(2\,\text{genus}(D) - 2) + R$$

where R denotes the number of ramified points in the double-cover $C \longrightarrow D$. Since $R \geq 0$, it follows that the case genus$(D) = 3$ cannot occur. The other possibility is that D is an elliptic curve over $\mathbb{F}_4$ and $R = 6$. From the values of the above table, we deduce that the ramified points of D in C should be defined over $\mathbb{F}_4$. Hence, all 21 points in $D(\mathbb{F}_{4^2})$ must split in $C(\mathbb{F}_{4^2})$ but $C(\mathbb{F}_{4^2})$ has only 18 points. Thus, we also get a contradiction in this case.

Case f: The different choices of h_1 and h_2 give rise to reduced resultants -5, 6, and 30 so that we cannot apply the above criteria.

Case g: The resultant of $h_1(x) = (x+2)^2$ and $h_2(x) = (x+3)^2$ is equal to 1. Serre's criterion applies so that there is non DS-curve in this case.

Case h: The reduced resultant of $h_1(x) = x + 1$ and $h_2(x) = (x+3)(x+2)^2$ is equal to 2. Howe-Lauter criterion ensures that C is a double-cover of a curve D with real Weil polynomial either $x + 1$ or $(x+3)(x+2)^2$. From the real Weil polynomials we obtain the following possibilities:

# of points over $\mathbb{F}_q$	$\mathbb{F}_4$	$\mathbb{F}_{4^2}$	$\mathbb{F}_{4^3}$
genus$(C) = 4$	13	31	13
genus$(D) = 1$	6	24	54
genus$(D) = 3$	12	24	24

Again the Hurwitz formula yields to a contradiction when genus$(D) = 3$. Thus, we can assume that D is an elliptic curve with $\#D(\mathbb{F}_4) = 6$. Since C is a double-cover of D, in this case, $\#C(\mathbb{F}_4) \leq 12$ which is a contradiction.

Case i: The resultant of $h_1(x) = (x+1)^2$ and $h_2(x) = (x+2)^2$ is equal to 1. Serre's criterion applies so that there is non DS-curve in this case.

Summarizing, in this case we have reduced the number of candidates form 9 to 3.

2.8 Genus 5

Recall that the list of admissible pairs (q, f) for genus $g = 5$ is given by the values in the table:

$g = 5$

q	f
2	$2, 3, 4, 5, 6$
3	$2, 3, 4$
4	$2, 3$
5	$2, 3$
7	2
8	2
9	2
11	2
13	2

The aim of this section is to present the statistics of candidate L-polynomials, along with some examples of genus-5 DS-curves.

In the following tables, for every admissible pair (q, f), the first row displays the number of points $N_1 = a_1 = \#C(\mathbb{F}_q)$ of an eventual DS-curve C, and the second row gives the number of candidate L-polynomials obtained through our Algorithm Two.

$(q,f)=(2,2)$										
N_1	0	1	2	3	4	5	6	7	8	9
$\#L$	26	80	176	275	311	234	115	39	9	1

$(q,f)=(2,3)$										
N_1	0	1	2	3	4	5	6	7	8	9
$\#L$	45	105	200	272	258	171	82	28	9	1

$(q,f)=(2,4)$										
N_1	0	1	2	3	4	5	6	7	8	9
$\#L$	47	107	135	132	108	75	29	9	2	0

$(q,f)=(2,5)$										
a_1	0	1	2	3	4	5	6	7	8	9
$\#L$	13	3	30	61	42	13	16	6	3	1

$(q,f)=(2,6)$										
N_1	0	1	2	3	4	5	6	7	8	9
$\#L$	3	8	13	5	6	7	4	0	0	0

$(q, f) = (3, 2)$														
N_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$\#L$	88	276	649	1225	1869	2187	1999	1584	1132	503	194	63	21	9

$(q, f) = (3, 3)$														
a_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$\#L$	28	94	226	388	503	421	394	354	268	94	22	6	6	0

$(q, f) = (3, 4)$														
a_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$\#L$	1	3	2	10	9	11	2	3	1	0	0	0	0	0

$(q, f) = (4, 2)$										
N_1	0	1	2	3	4	5	6	7	8	9
$\#L$	184	475	1041	1824	2706	3901	4904	4983	4284	3356
N_1	10	11	12	13	14	15	16	17		
$\#L$	2604	1987	910	368	152	66	29	11		

$(q, f) = (4, 3)$										
N_1	0	1	2	3	4	5	6	7	8	9
$\#L$	1	5	22	41	40	12	6	33	52	72
N_1	10	11	12	13	14	15	16	17		
$\#L$	51	19	4	2	1	1	1	1		

$(q,f) = (5,2)$										
N_1	0	1	2	3	4	5	6	7	8	9
$\#L$	40	225	713	1469	2017	1959	2089	4219	5983	5849
N_1	10	11	12	13	14	15	16	17	18	19
$\#L$	4539	3089	2013	1523	1367	502	169	56	21	7
N_1	20									
$\#L$	4									

$(q,f) = (5,3)$										
N_1	0	1	2	3	4	5	6	7	8	9
$\#L$	0	0	0	0	0	0	0	0	0	0
N_1	10	11	12	13	14	15	16	17	18	19
$\#L$	0	0	0	0	0	0	1	0	0	0
N_1	20									
$\#L$	0									

$(q,f) = (7,2)$										
N_1	0	1	2	3	4	5	6	7	8	9
$\#L$	0	1	42	202	410	224	11	1	1	11
N_1	10	11	12	13	14	15	16	17	18	19
$\#L$	291	2343	3107	2312	1204	471	183	79	71	188
N_1	20	21	22	23	24	25	26	27	28	
$\#L$	225	72	25	9	4	2	2	1	1	

$(q,f)=(8,2)$										
N_1	0	1	2	3	4	5	6	7	8	9
$\#L$	0	0	0	11	57	26	0	0	0	0
N_1	10	11	12	13	14	15	16	17	18	19
$\#L$	0	0	49	965	1071	544	145	15	0	0
N_1	20	21	22	23	24	25	26	27	28	29
$\#L$	0	0	41	38	10	2	1	0	0	0

$(q,f)=(9,2)$										
N_1	0	1	2	3	4	5	6	7	8	9
$\#L$	0	0	0	1	9	4	0	0	0	0
N_1	10	11	12	13	14	15	16	17	18	19
$\#L$	0	0	0	0	15	252	213	91	20	1
N_1	20	21	22	23	24	25	26	27	28	29
$\#L$	0	0	0	0	1	81	31	13	7	4
N_1	30	31	32	33	34	35				
$\#L$	2	1	1	1	1	1				

$(q,f)=(11,2)$										
N_1	0	1	2	3	4	5	6	7	8	9
$\#L$	0	0	0	0	0	0	0	0	0	0
N_1	10	11	12	13	14	15	16	17	18	19
$\#L$	0	0	0	0	0	0	0	0	0	0
N_1	20	21	22	23	24	25	26	27	28	29
$\#L$	0	0	0	0	0	0	0	0	0	0
N_1	30	31	32	33	34	35	36	37	38	
$\#L$	0	0	0	0	0	0	0	0	0	

$(q,f)=(13,2)$										
N_1	0	1	2	3	4	5	6	7	8	9
$\#L$	0	0	0	0	0	0	0	0	0	0
N_1	10	11	12	13	14	15	16	17	18	19
$\#L$	0	0	0	0	0	0	0	0	0	0
N_1	20	21	22	23	24	25	26	27	28	29
$\#L$	0	0	0	0	0	0	0	0	0	0
N_1	30	31	32	33	34	35	36	37	38	39
$\#L$	0	0	0	0	0	0	0	0	0	0
N_1	40	41	42	43	44					
$\#L$	0	0	0	0	0					

Some examples of genus-5 curves with DS taken from [40] and [31]:

(q, f)	Defining equation of a genus-5 DS-curve	$[a_1, a_2, a_3, a_4, a_5]$
$(2, 2)$	$x^6 + x^5y + x^3y^3 + y^6 + x^5 + x^4y + x^3y + x^2y^2 + xy^3 + y^4 + x^2y + xy^2 + y^3 + xy + x + y + 1$	$[4, 0, 6, 4, 3]$
$(2, 5)$	$y^4 + (x^2 + x + 1)y^2 + (x^2 + x)y + x^7 + x^3$	$[9, 0, 0, 2, 0]$

2.9 Delinge-Lusztig curves

In the middle 70's, Delinge and Lusztig were able to give an explicit description of the irreducible representations of the semi-simple finite groups of Lie type [12]. These representations can be read from the ℓ-adic cohomology of the so-called Deligne-Lusztig algebraic varieties which are defined over finite fields. In this section, we make the observation that, in the one-dimensional case, Deligne-Lusztig curves turn out to be DS-curves.

2.9.1 Hermitian curves (type ${}^2A_2$).

Here q denotes a square prime-power, and $q_0 = q^{1/2}$. The hermitian curve is defined by the affine equation:

$$C\colon x^{q_0+1} + y^{q_0+1} + z^{q_0+1} = 0\,.$$

It is an optimal curve (in fact, it is a maximal curve) of genus $g = (q - q_0)/2$ over $\mathbb{F}_q$. Its Weil polynomial is

$$L(t) = (t + q_0)^{2g}\,.$$

An easy computation shows that

$$\#C(\mathbb{F}_q) = \#C(\mathbb{F}_{q^2}) = q_0^3 + 1 = q + 1 + 2gq^{1/2}\,.$$

2.9.2 Suzuki curves (type ${}^2B_2$)

Here, $q = 2^{2e+1}$ and $q_0 = 2^e$ for $e \geq 1$. The Suzuki curve is defined by the affine equation:

$$C\colon y^q - y = x^{q_0}(x^q - x)\,.$$

It has genus $g = q_0(q - 1)$ and its Weil polynomial is

$$L(t) = \left(t - q^{1/2}\frac{-1+i}{\sqrt{2}}\right)^g \left(t - q^{1/2}\frac{-1-i}{\sqrt{2}}\right)^g = (t^2 + 2q_0 t + q)^g\,.$$

An easy computation shows that

$$\#C(\mathbb{F}_q) = \#C(\mathbb{F}_{q^2}) = \#C(\mathbb{F}_{q^3}) = q^2 + 1\,.$$

2.9.3 Ree curves (type ${}^2G_2$)

Now, we take $q = 3^{2s+1}$, $q_0 = 3^s$ for $s \geq 1$. The Ree curve is given by the equations

$$C\colon\; y^q - y = x^{q_0}(x^q - x)\;\;,\;\;\; z^q - z = x^{q_0}(y^q - y)$$

It has genus $g = \frac{3}{2}q_0(q-1)(q+q_0+1)$. Its Weil polynomial is

$$L(t) = (t^2+q)^{\frac{1}{2}q_0(q-1)(q+3q_0+1)}(t^2+3q_0t+q)^{q_0(q^2-1)}$$

One readily checks that

$$\#C(\mathbb{F}_q) = \#C(\mathbb{F}_{q^2}) = \#C(\mathbb{F}_{q^3}) = \#C(\mathbb{F}_{q^4}) = \#C(\mathbb{F}_{q^5}) = 1 + q^3\,.$$

2.10 Carlitz curves

Carlitz initiated the study of functions fields that play an analogous role to that of cyclotomic fields in algebraic number theory (see [8], [7]). In this section, we shall deal with no-singular curves attached to the Carlitz modules. Our aim is to point out that Carlitz curves can be a good source of DS-curves. First, we recall their definition. We refer to [32], [9], [16], and [1] for detailed expositions on the arithmetic of Carlitz extensions.

Let $M \in \mathbb{F}_q[t]$ be a monic polynomial of degree ≥ 1. The M-torsion Carlitz module

$$\Lambda_M = \{\gamma \in \overline{\mathbb{F}_q(t)}\colon [M](\gamma) = 0\} = \langle \lambda_M \rangle$$

is a finite 1-dimensional $\mathbb{F}_q[t]$-module via the Carlitz action determined by recursion and linearly:

$$[t](x) = x^q + tx\,, \quad [t^n](x) = [t]([t^{n-1}](x))\,, \quad [1](x) = x\,.$$

Let $K_M = \mathbb{F}_q(t, \lambda_M)$. The Carlitz extension $K_M/\mathbb{F}_q(t)$ attached to M is an abelian extension unramified outside the primes dividing $M\infty$. The Carlitz action induces an isomorphism between $(\mathbb{F}_q[t]/M)^*$ and the Galois group $\mathrm{Gal}(K_M/\mathbb{F}_q(t))$:

$$(\mathbb{F}_q[t]/M)^* \longrightarrow \mathrm{Gal}(K_M/\mathbb{F}_q(t))\,, \quad Q \mapsto \sigma_Q \colon \lambda_M \mapsto [Q](\lambda_M)\,.$$

Let $\Phi_M(x)$ be the M-th Carlitz polynomial defining the extension K_M; that is,

$$\Phi_M(x) = \frac{[M](x)}{\prod_{Q|M} \Phi_Q(x)}$$

where Q runs the monic polynomials dividing M of degree less than $\deg M$, and $\Phi_1(x) = x$. The minimal polynomial of λ_M over $\mathbb{F}_q(t)[x]$ is the irreducible Carlitz polynomial $\varPhi_M(x)$.

The M-torsion field K_M can be regarded as the function field of an algebraic curve defined over $\mathbb{F}_q$, that we shall denote here by $\mathcal{X}_M$ and call it the Carlitz curve of level M. Our aim is to show the Diophantine stability of $\mathcal{X}_M$ in a particular example for an specific M. We should point out that experimentally we have found that Carlitz curves tend to be DS-curves and, with no doubt, this deserves further study.

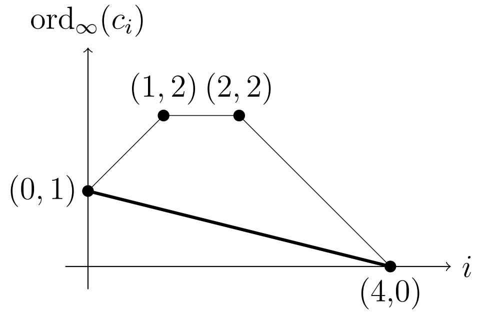
We shall take $M = t^3$ in $\mathbb{F}_2[t]$. The corresponding Carlitz extension is $K_M = \mathbb{F}_2(t, \Lambda_M) = \mathbb{F}_2(t)[x]/(x^4 + (t^2 + t)x^2 + t^2 x + t)$. The unique places that can be ramified are t and the infinite place $\infty = 1/t$. It is well-known that the integral closure of $\mathbb{F}_q[t]$ in K_M is $\mathbb{F}_q[t][\lambda_M]$ (see [32], Proposition 12.9, page 207).

Thus, we can argue as follows. As for t, one checks that

$$\Phi_M(x) = x^4 + (t^2 + t)x^2 + t^2 x + t \equiv x^4 \bmod t$$

so that t ramifies with ramification index 4. As for the infinite place $1/t$, we must look at the corresponding Newton polygon attached to

$$\begin{aligned}\Phi_M(x) = \textstyle\sum_{i=0}^{4} c_i x^i &= x^4 + (t^2 + t)x^2 + t^2 x + t \\ &= x^4 + (1/t)^{-2}(1 + 1/t)x^2 + (1/t)^{-2}x + (1/t)^{-1}\end{aligned}$$



Since there is a unique segment of slope $-1/4$ and base of length 4 that means that the quartic polynomial $\Phi_M(x)$ has four different roots of valuation $1/4$ with respect to the place at infinity. In other words, the infinite place of $\mathbb{F}_q(t)$ splits completely in K_M.

Let g be the genus of the Carlitz curve $\mathcal{X}_M$ of level M. In this case, the different of the Carlitz extension K_M is $\mathcal{D} = (t)^8$. By the Hurwitz genus formula, we have: $2g - 2 = 4\,(2 \cdot 0 - 2) + \deg(\mathcal{D}) = -8 + 8 = 0$. It follows that $g = 1$. The Zeta-function of the curve $\mathcal{X}_M$ is given by

$$Z_M(T) = \prod_{d \geq 1} \frac{1}{(1 - T^d)^{a_d}}\,,$$

where a_d denotes the number of places of $\mathcal{X}_M$ of degree d. For $n \geq 1$, let $N_n = \#\mathcal{X}_M(\mathbb{F}_{q^n})$. Recall that $N_n = \sum_{d|n} d a_d$ and $a_d = \frac{1}{d}\sum_{d'|d} \mu(\frac{d}{d'}) N_{d'}$.

Here, all prime polynomials will be assumed implicitly to be monic. The following table displays the factorization of $\Phi_M(x)$ mod π in $(\mathbb{F}_2[t]/\pi)[x]$, for primes $\pi \in \mathbb{F}_2[t]$ of degree $d \leq 5$; the third column labeled "type" indicates the degrees of the irreducible factors of the quartic polynomial $\Phi_M(x)$ mod π. The fourth column displays the number a_d of places of $\mathcal{X}_M$ of degree d.

d	π	type	a_d
1	t	$[1]^4$	$a_1 = 5$
1	$t+1$	$[4]$	
1	$\infty = 1/t$	$[1,1,1,1]$	
2	t^2+t+1	$[4]$	$a_2 = 0$
3	t^3+t+1	$[4]$	$a_3 = 0$
3	t^3+t+1	$[2,2]$	
4	t^4+t+1	$[4]$	$a_4 = 5$
4	t^4+t^3+1	$[1,1,1,1]$	
4	$t^4+t^3+t^2+1$	$[4]$	
5	t^5+t^2+1	$[2,2]$	$a_5 = 4$
5	t^5+t^3+1	$[1,1,1,1]$	
5	$t^5+t^3+t^2+t+1$	$[4]$	
5	$t^5+t^4+t^2+t+1$	$[4]$	
5	$t^5+t^4+t^3+t+1$	$[4]$	
5	$t^5+t^4+t^3+t^2+1$	$[2,2]$	

Observe that the elliptic curve $\mathcal{X}_M$ over $\mathbb{F}_2$ is a DS-curve. Indeed, we have $a_2 = a_3 = 0$ and therefore $\mathcal{X}_M(\mathbb{F}_2) = \mathcal{X}_M(\mathbb{F}_4) = \mathcal{X}_M(\mathbb{F}_8)$. It is worth to explain why $a_4 = 5$. One should analyze the primes π in $\mathbb{F}_2[t]$ of degree d' dividing 4. First, we get four rational places lying over the prime $\pi = t^4 + t^3 + 1$ of degree $d' = 4$ since $\Phi_M(x)$ mod π splits completely in $(\mathbb{F}_2[t]/\pi)[x]$. Second, one more place arises from the prime $\pi = t + 1$ of degree $d' = 1$: indeed, the polynomial

$\Phi_M \bmod t+1$ is irreducible in $\mathbb{F}_2[x]$ and it factors as

$$\Phi_M(x) \bmod t+1 = (x+\alpha)(x+\alpha+1)(x+\alpha^2)(x+\alpha^2+1)$$

in $\mathbb{F}_{2^4}[x]$. Here, α denotes the Conway generator of $\mathbb{F}_{2^4}^*$. Finally, we must consider the prime $\pi = t^2+t+1$ of degree $d' = 2$. The polynomial $\Phi_M \bmod \pi$ factors into irreducibles as

$$(x^2+(\alpha^2+\alpha)x+\alpha^3+\alpha+1)(x^2+(\alpha^2+\alpha)x+\alpha^3+\alpha^2+1)$$

in $\mathbb{F}_{2^4}[x]$. Thus, this prime does not give any contribution to places of degree 4. Summing up, one gets $a_4 = 5$. As for degree-5 places, one gets that $a_5 = 4$ since it only incorporates the four places over the prime $\pi = t^5+t^3+1$. The sequence of numbers of places extends as:

$$[a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, \ldots] = [10, 20, 25, 60, 100, 180, 345, \ldots].$$

Of course, the number of points N_n and the number of places a_d are determined by the first $N_1 = a_1$ in this example, since the curve $\mathcal{X}_M$ has genus one.

For the general case (any M), the refinement of the analogous Dirichlet theorem for function fields asserts that there are always primes π in $\mathbb{F}_q[t]$ with $\pi \equiv 1 \bmod M$ and $\deg(\pi) = d$ for every degree $d \geq d_0$, with d_0 effectively computable in terms of the genus of $\mathcal{X}_M$. Hence, $a_d \neq 0$ for d large enough. However, as it has been mentioned, Carlitz curves tend to be DS-curves.

Chapter 3

DS-surfaces

Max Noether(1844-1921) said in the book of Federigo Enriques [15]: "Algebraic curves are created by God, algebraic surfaces are created by devil."

Noether initiated the systematic study of algebraic surfaces, and Castelnuovo proved important parts of the classification. Enriques completed the classification of complex projective surfaces. Later, Kodaira extended the classification including non-algebraic compact surfaces. The analogous classification of surfaces in positive characteristic was achieved by Mumford and Bombieri-Mumford in a series of three articles [30], [5], [6].

In this chapter, the letter X will denote a non-singular projective algebraic surface. Some general references for the theory of surfaces are [2], [3] and [44]. We also refer to [4] for computational aspects related to surfaces.

Among the most important birational invariants of X there are the plurigenera $P_n = \dim H^0(K^n)$, for $n \geq 1$, where K denotes the canonical bundle of X. The Kodaira dimension κ of X is defined in terms of the growth rate of their plurigenera. More precisely, $\kappa = -1$ if all $P_n = 0$, and otherwise is the smallest number such that P_n/n^κ is bounded. It turns out that the Kodaira dimension κ is either -1, 0, 1, or 2.

For $0 \leq i,\, j \leq 2$, the Hodge numbers of X are $h^{i,j} = \dim H^j(X, \Omega^i)$, where Ω^i is the sheaf of differential i-forms. They are arranged in the so-called Hodge diamond:

$$\begin{array}{ccccc} & & h^{0,0} & & \\ & h^{1,0} & & h^{0,1} & \\ h^{2,0} & & h^{1,1} & & h^{0,2} \\ & h^{2,1} & & h^{1,2} & \\ & & h^{2,2} & & \end{array}$$

By Serre duality, we have $h^{0,0} = h^{2,2} = 1$ and $h^{i,j} = h^{2-i,2-j}$. All Hodge numbers are birational invariants, except $h^{1,1}$ which increases by 1 under blowing up a single point. If the surface is Kähler then $h^{i,j} = h^{j,i}$. Since we are interested in projective algebraic surfaces, the shape of the Hodge diamond is

$$\begin{array}{ccccc} & & 1 & & \\ & h^{1,0} & & h^{1,0} & \\ h^{2,0} & & h^{1,1} & & h^{2,0} \\ & h^{1,0} & & h^{1,0} & \\ & & 1 & & \end{array}$$

For complex surfaces, the Betti numbers of X are defined by $\beta_i = \dim H^i(X)$. They can be obtained from the Hodge diamond by adding the Hodge numbers for each row:

$$\beta_0 = \beta_4 = 1\,, \qquad \beta_1 = \beta_3 = 2h^{1,0}\,, \qquad \beta_2 = h^{1,1} + 2h^{2,0}\,.$$

The Euler characteristic of X is defined by $E(X) = \sum_{i=0}^{4}(-1)^i\beta_i$. The irregularity $q = q(X)$ of X is the dimension of the Picard variety and the Albanese variety associated with X. For complex surfaces (but not always for positive characterisitic) we have $q = h^{1,0}$. The holomorphic Euler characteristic is $\chi(X) = h^{0,2} - h^{0,1} + 1$. Finally, $c_2 = E$ and $c_1^2 = K^2 = 12\chi - E$ are called the Chern numbers of X.

Any surface is birational to a non-singular surface. A non-singular surface is called minimal if it cannot be obtained from another non-singular surface by blowing up a point.

Every surface X is birational to a minimal non-singular surface, and this minimal non-singular surface is unique if X has Kodaira dimension ≥ 0 (or is not algebraic). Algebraic surfaces of Kodaira dimension -1 may be birational to more than one minimal non-singular surface.

3.1 Sign of the functional equation

At the beginning of Chapter 2, we mentioned that the Riemann-Roch theorem implies the rationality and the functional equation of the Zeta function for curves. In particular, for that case one also obtains that the sign of the functional equation is always +1. In the usual references, it is common not to give further information on the sign of the functional equation for varieties of larger dimension. For future use, let us compute the sign in the case of surfaces.

Let X over $\mathbb{F}_q$ be a non-singular projective surface. Its Zeta function

$$\zeta_X(t) = \frac{P_1(t)P_3(t)}{P_0(t)P_2(t)P_4(t)}$$

is a rational function and satisfies the functional equation:

$$\zeta_X\left(\frac{1}{q^2 t}\right) = \pm q^E t^E \zeta_X(t)\,.$$

We want to determine the sign ± 1. We have

$$P_i(t) = \prod_{j=1}^{\beta_i}(1 - \alpha_{ij}t)$$

with $|\alpha_{ij}| = q^{i/2}$. In particular, one has $P_0(t) = 1 - t$ and $P_2(t) = 1 - q^2 t$. Recall that $E = E(X)$ denotes the Euler characteristic of the surface X; that is, the alternate sum $\beta_0 - \beta_1 + \beta_2 - \beta_3 + \beta_4$.

Proposition 6. *With the above notations, the sign of the functional equation for $\zeta_X(t)$ is $(-1)^E$.*

Proof. Let us compute

$$\zeta\left(\frac{1}{q^2t}\right) = \frac{P_1\left(\frac{1}{q^2t}\right) P_3\left(\frac{1}{q^2t}\right)}{P_0\left(\frac{1}{q^2t}\right) P_2\left(\frac{1}{q^2t}\right) P_4\left(\frac{1}{q^2t}\right)}.$$

On the one hand, we have

$$P_0\left(\frac{1}{q^2t}\right) = -P_4(t)/(q^2t)$$

and

$$P_4\left(\frac{1}{q^2t}\right) = -P_0(t)/t, .$$

As for the middle term $P_2(t)$, we compute

$$\begin{aligned} P_2\left(\tfrac{1}{q^2t}\right) &= \prod_{j=1}^{\beta_2}\left(1 - \alpha_{2j}\frac{1}{q^2t}\right) = \frac{\prod_{j=1}^{\beta_2}(q^2t - \alpha_{2j})}{q^{2\beta_2}t^{\beta_2}} \\ &= \frac{\prod_{j=1}^{\beta_2}(\alpha_{2j}\overline{\alpha}_{2j}t - \alpha_{2j})}{q^{2\beta_2}t^{\beta_2}} = \frac{\prod_{j=1}^{\beta_2}\alpha_{2j}\prod_{j=1}^{\beta_2}(\overline{\alpha}_{2j}t - 1)}{q^{2\beta_2}t^{\beta_2}} \\ &= \frac{q^{\beta_2}(-1)^{\beta_2}\prod_{j=1}^{\beta_2}(1 - t\overline{\alpha}_{2j})}{q^{2\beta_2}t^{\beta_2}} = \frac{q^{\beta_2}(-1)^{\beta_2}P_2(t)}{q^{2\beta_2}t^{\beta_2}}. \end{aligned}$$

Similarly, we get

$$\begin{aligned} P_1\left(\tfrac{1}{q^2t}\right) &\quad (-1)^{\beta_1}q^{-\beta_1}t^{-\beta_1}P_3(t) \\ P_3\left(\tfrac{1}{q^2t}\right) &\quad (-1)^{\beta_1}q^{-\beta_1}t^{-\beta_1}P_1(t). \end{aligned}$$

Putting altogether, we obtain

$$\zeta_X\left(\frac{1}{q^2 t}\right) = (-1)^{\beta_2}(qt)^{2-2\beta_1+\beta_2}\zeta_X(t)$$

as we wanted. □

3.2 Minimal surfaces

The old italian school realized that birational equivalence is a sensible relation up to which algebraic varieties may be classified. Two algebraic varieties are birational if they contain isomorphic dense Zariski-open subsets. Any birational morphism between smooth surfaces can be factored as a finite sequence of blowups.

A surface X is minimal if any birational morphism $X \to X'$ to any other surface X' is an isomorphism. As we already mentioned in the introduction of this chapter, every smooth surface Y is birational to a minimal non-singular surface X. If Y is of nonnegative Kodaira dimension, then there exists a unique minimal model X of Y, and X can be constructed from iterated blow downs of (-1)-curves.

The Minimal Model Program for algebraic varieties of arbitrary dimension seeks to construct birational models which are as simple as possible. It is currently an active research area within algebraic geometry. In the case of surfaces, the program has been achieved: any surface can be obtained as a blow-up of a minimal surface X. Except for Kodaira dimension -1, minimal surfaces are unique within birational equivalence classes.

As a consequence, the classification (up to birational equivalence) of surfaces can be reduced to the classification of minimal surfaces, and this goal was attained by Enriques (charcateristic 0) and Bombieri-Mumford (characteristic > 0).

As we shall see, in our aim to search for DS-surfaces over finite fields we can restirct ourselves to minimal surfaces as well.

3.3 Enriques-Bombieri-Mumford's classification

In a series of three papers Bombieri-Mumford extended the Enqrique's classification of minimal surfaces to positive characteristic. From now on, we assume that X is a minimal non-singular projective surface. We can read the classification from the following table:

$\kappa(X)$	X
-1	rational ($q = 0$) or ruled ($q > 0$)
0	K3, Enriques, abelian surfaces, hyperelliptic (bielliptic)
1	some cases of elliptic surfaces
2	surfaces of general type

3.3.1 Kodaira dimension -1

If the irregularity of X is $q = 0$, then X is a rational surface (Castelnuovo's theorem). A rational surface means that it is birational to the projective plane $\mathbb{P}^2$. The minimal rational surfaces are $\mathbb{P}^2$ itself and Hirzebruch surfaces Σ_n for $n = 0$ or $n \geq 2$. The possible Hodge diamonds are:

$$\begin{matrix} & & 1 & & \\ & 0 & & 0 & \\ 0 & & 1 & & 0 \\ & 0 & & 0 & \\ & & 1 & & \end{matrix}$$

for the projective plane, and

$$\begin{array}{ccccc} & & 1 & & \\ & 0 & & 0 & \\ 0 & & 2 & & 0 \\ & 0 & & 0 & \\ & & 1 & & \end{array}$$

for the Hirzebruch surfaces.

Examples of rational surfaces are: $\mathbb{P}^2$, $\mathbb{P}^1 \times \mathbb{P}^1 = \Sigma_0$, Hirzebruch surfaces Σ_n, quadrics, cubic surfaces, del Pezzo surfaces, the Veronese surface. Many of these examples are non-minimal.

If the irregularity $q > 0$, then X is a ruled surface. In that case, there is a smooth morphism $X \to C$, where C is a curve of genus $g \geq 1$ (the case $g = 0$ corresponds to the Hirzebruch surfaces and are rational). Any ruled surface is birationally equivalent to $\mathbb{P}^1 \times C$ for a unique curve C. Their Hodge diamond is:

$$\begin{array}{ccccc} & & 1 & & \\ & g & & g & \\ 0 & & 2 & & 0 \\ & g & & g & \\ & & 1 & & \end{array}$$

Examples of ruled surfaces are: the product of any curve of genus $g > 0$ with $\mathbb{P}^1$.

3.3.2 Kodaira dimension 0

The following table displays the classification due to Mumford-Bombieri-Munford for positive characteristic.

β_1	β_2	X
0	22	$K3$
0	10	Enriques
4	6	abelian surfaces
2	2	hyperelliptic

It should be noticed that there are non-classical Enriques surfaces (only in characteristic 2) and quasi-hyperelliptic surfaces (only in characteristics 2 and 3), meaning that there is a variation on the corresponding Hodge diamond although this fact is not apparent with regard to the Betti numbers.

Examples of K3 surfaces: degree-4 hypersurfaces in $\mathbb{P}^3$, and Kummer surfaces (quotients of abelian surfaces by the automorphism -1, then blowing up the 16 singular points).

Examples of Enriques surfaces: quotients of K3 surfaces by a group of order 2 acting without fixed points (when chacrateisitic $\neq 2$).

Examples of abelian surfaces: a product of two elliptic curves, the Jacobian of a genus-2 curve, modular abelian surfaces.

Examples of hyperelliptic surfaces: over the complex field, they are quotients of two elliptic curves by a finite group of automorphisms, giving rise to seven families of such surfaces. Over fields of characteristic 2 and 3 there are some extra families given by taking quotients by non-étale group schemes.

3.3.3 Kodaira dimension 1

Every surface of Kodaira dimension 1 is an elliptic surface; that means, there is a surjective morphism $X \to B$, where B is a base curve and the fibers are all but finitely many irreducible curves of genus one. In characteristic 2 and 3 we should relax the condition to quasi-elliptic surfaces meaning that they admit degenerate elliptic curves as fibers; that is, rational curves with a single node. The converse is not true: an elliptic surface can have Kodaria dimension -1, 0, or 1. Whenever

B has genus at least 2, X has Kodaira dimension 1. However, it can happen B to have genus 0 or 1 and the Kodaira dimension of X to be $\kappa = 1$.

Examples of surfaces of Kodaira dimension 1: $E \times B$, where E is an elliptic curve and B a curve of genus at least 2.

3.3.4 Kodaira dimension 2

These are called surfaces of general type, and it turns out that they are the majority. For any fixed values of the Chern numbers c_1^2 and c_2, there is a quasi-projective scheme classifying the surfaces of general type with these Chern numbers. But very little is known about these moduli spaces. There are several constrains on the Chern numbers of a minimal surface of general type: c_1^2, $c_2 > 0$, $c_1^2 \leq 3c_2$ (Bogomolov-Miyaoka-Yau inequality), $5c_1^2 - c_2 + 36 \geq 0$ (Noether inequality), $c_1^2 + c_2 \equiv 0 \pmod{12}$.

Examples of surfaces of Kodaira dimension 2: the product of two curves of genus at least 2, a hypersurface of degree at least 5 in $\mathbb{P}^3$, Hilbert modular surfaces, etc.

3.4 DS-surfaces are minimal

In this section, we want to show that in order to find DS-surfaces we can restrict ourselves to minimal surfaces.

Proposition 7. *If X is a DS-surface, then X is a minimal surface.*

Proof. Suppose that X is not minimal. With no loss of generality, we can assume that X is obtained by blowing up a point P of a minimal surface X_0 over $\mathbb{F}_q$. According to Rybakov (see Lemma 2.7 [33]), we have

$$Z_X(t) = Z_{X_0}(t)\,(1 - q^r t)^{-1}$$

where r is equal to the degree of the point P. Now, taking logarithms we get

$$\log Z_X(t) = \log Z_{X_0}(t) - \log(1 - q^r t)$$

Thus, we have

$$\sum_{n\geq 1} \widetilde{N}_n \frac{t^n}{n} = \sum_{n\geq 1} N_n \frac{t^n}{n} + \sum_{n\geq 1} q^{rn} \frac{t^n}{n}$$

where

$$\widetilde{N}_n = \#X(\mathbb{F}_{q^n}), \qquad N_n = \#X_0(\mathbb{F}_{q^n}).$$

Therefore, for all $n \geq 1$, it follows

$$\widetilde{N}_n = N_n + q^{rn}, \qquad \widetilde{N}_1 = N_1 + q^r.$$

If X is a DS-surface, then we should have $\widetilde{N}_1 = \widetilde{N}_n$ for some $n > 1$. This implies

$$N_n = N_1 + q^r - q^{rn} < N_1$$

which is a contradiction since $n > 1$. □

3.5 Hirzebruch surfaces

As we have already mention, Hirzerbruch surfaces Σ_n, for $n = 0$ or $n \geq 2$, have Hodge diamond

$$\begin{array}{ccccc} & & 1 & & \\ & 0 & & 0 & \\ 0 & & 2 & & 0 \\ & 0 & & 0 & \\ & & 1 & & \end{array}$$

so that their non-zero Betti numbers are $\beta_0 = 1$ and $\beta_2 = 2$. Some other surfaces (minimal or not) share the same Hodge diamond, among others: quadratic surfaces, and Beauville surfaces (which are of general type). Over $\mathbb{F}_q$, all of them have Zeta function that looks like:

$$\zeta_X(t) = \frac{1}{(1-t)P_2(t)(1-q^2t)}$$

with $P_2(t) = \prod_{j=1}^{2}(1-\alpha_j t)$ in $\mathbb{Z}[t]$ satisfying $|\alpha_j| = q$. The number of points is

$$N_m = 1 + q^{2m} + \alpha_1^m + \alpha_2^m$$

and hence $|N_m - (1+q^{2m})| \leq 2q^m$.

Proposition 8. *There are not Hirzebruch surfaces with DS.*

Proof. First, we note that the chance for a Hirzebruch surface to have DS occurs only for $q = 2$ and $N_1 = N_2 = 9$. Therefore, we get $\alpha = 2(1+\sqrt{3}i)$. But, $|\alpha| = 4$ and it should be 2. □

3.6 Ruled surfaces

As it was already mentioned, any (minimal) ruled surface X is isomorphic to $\mathbb{P}^1 \times C$ for a unique curve C of genus $g \geq 1$. Since we have

$$\#X(\mathbb{F}_q) = \#\mathbb{P}^1(\mathbb{F}_q) \cdot \#C(\mathbb{F}_q)\,,$$

the only possibility for X to have DS is when $\#C(\mathbb{F}_q) = \#C(\mathbb{F}_{q^m}) = 0$ for some $m > 1$.

This rises the question of classifying all curves having DS due to the absence of points. Examples of these curves can be found in Chapter 1 Section 2.4. For instance, the genus-3 curves:

(q,m)	C	N
$(2,2)$	$x^4+x^3y+y^4+x^2y+y^3+x+1$	0
$(2,5)$	$x^4+x^2y^2+y^4+x^2y+xy^2+x^2+xy+y^2+1$	0

3.7 Hyperelliptic surfaces

Let $X/\mathbb{F}_q$ be a hyperelliptic surface. According to the Betti numbers of X, its Zeta function must be

$$\zeta_X(t) = \frac{P_1(t)P_3(t)}{(1-t)P_2(t)(1-q^2t)},$$

with

$$P_1(t) = 1 - bt + qt^2$$
$$P_3(t) = 1 - qbt + q^3t^2$$
$$P_2(t) = 1 - at + q^2t^2$$

for some integers a, b satisfying $|a| \le 2q$ and $|b| \le 2\sqrt{q}$. From this, one readily checks that the unique extensions $\mathbb{F}_{q^m}/\mathbb{F}_q$ where X can have Diophantine stablility are limited to $q = 2$ with $m = 2$, 3, or $q = 3$ with $m = 2$.

By inspection, we get the information of the possible Zeta functions arising from hyperelliptic surfaces with Diophantine stability:

$q=2\;\; m=2$	$\zeta_X(t)$	$N_1 = N_2$
$(a,b) = (-1,-2)$	$\dfrac{(1+2t+2t^2)(1+4t+8t^2)}{(1-t)(1+t+4t^2)(1-4t)}$	10
$(a,b) = (2,-2)$	$\dfrac{(1+2t+2t^2)(1+4t+8t^2)}{(1-t)(1-2t+4t^2)(1-4t)}$	13

$q=2 \;\; m=3$	$\zeta_X(t)$	$N_1=N_3$
$(a,b)=(-4,-1)$	$\frac{(1+t+2t^2)(1+2t+8t^2)}{(1-t)(1+2t)^2(1-4t)}$	4
$(a,b)=(1,-1)$	$\frac{(1+t+2t^2)(1+2t+8t^2)}{(1-t)(1-t+4t^2)(1-4t)}$	9
$(a,b)=(2,-2)$	$\frac{(1+2t+2t^2)(1+4t+8t^2)}{(1-t)(1-2t+4t^2)(1-4t)}$	13
$(a,b)=(3,-1)$	$\frac{(1+t+2t^2)(1+2t+8t^2)}{(1-t)(1-3t+4t^2)(1-4t)}$	11

Observe that for this case $(a,b)=(2,-2)$, one has $N_1=N_2=N_3=13$ so that the eventual hyperelliptic surface will have Diophantine stability for $\mathbb{F}_{2^2}/\mathbb{F}_2$ and $\mathbb{F}_{2^3}/\mathbb{F}_2$.

After analyzing the finite number of cases for $q=3$, we reach to the conclusion that there are no candidates for Zeta functions corresponding to hyperelliptic DS-surfaces defined over $\mathbb{F}_3$.

Remark 5. *It should be pointed out that we have taken into consideration also the quasi-hyperelliptic surfaces that occur in Munford-Bombieri classification and which are defined over finite fields of characteristic* 2 *and* 3. *These surfaces do not arise as reduction of surfaces defined over fields of characteristic zero.*

3.8 Enriques surfaces

An Enriques surface X over $\mathbb{F}_q$ is characterized by the fact that its Kodaira dimension $\kappa=\kappa(X)$ equals 0 and has Betti numbers are $\beta_1=0$, $\beta_2=10$. The Zeta function of X looks like

$$\zeta_X(t)=\frac{1}{(1-t)P_2(t)(1-q^2t)}$$

where $P_2(t)$ is a degree-10 polynomial in $\mathbb{Z}[t]$ with reciprocal roots α_j satisfying $|\alpha_j| = q$ and $P_2(0) = 1$. The number of points satisfies

$$N_m = \#X(\mathbb{F}_{q^m}) = 1 + q^{2m} + \sum_{j=1}^{10} \alpha_j^m \,.$$

Hence, we have

$$|N_m - (1 + q^{2m})| \leq 10 q^m \,.$$

For $q = 2$ and 3, we get the following admissible intervals

q	N_1	N_2	N_3	N_4	N_5
2	$[0, 25]$	$[0, 57]$	$[0, 145]$	$[97, 417]$	$[705, 1345]$

q	N_1	N_2	N_3
3	$[0, 40]$	$[0, 172]$	$[460, 1000]$

For $q \geq 4$ there is no room to achieve DS, therefore the unique options are in characteristic 2 for $\mathbb{F}_{2^m}/\mathbb{F}_2$ with $m \leq 3$ and characteristic 3 for $\mathbb{F}_{3^m}/\mathbb{F}_3$ with $m \leq 2$.

Again, in order to get all possible Zeta functions for the Enriques surfaces with DS, we explore the first integer coefficients of their Weil polynomials

$$L_2(t) = \prod_{j=1}^{10} (t - \alpha_j) = t^{10} + a_1 t^9 + a_2 t^8 + a_3 t^7 + \cdots \in \mathbb{Z}[t] \,.$$

Using the Girard-Newton formulas, we have

$$\begin{aligned}
N_1 &= 1 + q^2 + \sum_{j=1}^{10} \alpha_j = 1 + q^2 - a_1 \\
N_2 &= 1 + q^4 + \sum_{j=1}^{10} \alpha_j^2 = 1 + q^4 + a_1^2 - 2a_2 \\
N_3 &= 1 + q^6 + \sum_{j=1}^{10} \alpha_j^3 = 1 + q^6 + a_1^3 + 3a_1 a_2 + 3a_3
\end{aligned}$$

and also

$$a_1 = 1 + q^2 - N_1$$

$$a_2 = -\left(a_1^2 + 1 + q^4 - N_2\right)/2$$

$$a_3 = \left(3a_1a_2 - a_1^3 + 1 + q^6 - N_3\right)/3\,.$$

In order to have $N_1 = N_2$, we need

$$a_2 = 6 + \frac{a_1(a_1+1)}{2} \qquad \text{for } q = 2;$$

$$a_2 = 36 + \frac{a_1(a_1+1)}{2} \qquad \text{for } q = 3.$$

In order to have $N_1 = N_3$, we need necessarily $q = 2$ and

$$a_3 = 20 + \frac{a_1(1 + 3a_2 - a_1^2)}{3}\,.$$

The above discussion helps us to list the candidate L-polynomials of all the DS-Enriques surfaces. We display the results obtained with the help of Sage in the following tables. Since the Euler characteristic is even in the case of Enriques surfaces, we should take into account only the sing +1 in the functional equation.

$q=2$	$N_1 = N_2$	$\#DS$
	0	1364
	1	3069
	2	5927
	3	10107
	4	15106
	5	19250
	6	20726
	7	18839
	8	14610
	9	9760
	10	5617
	11	2836
	12	1281
	13	551
	14	220
	15	89
	16	36
	17	16
	18	6
	19	2
	20	0
	21	0
	22	0
	23	0
	24	0
	25	0

$q=2$	$N_1 = N_3$	$\#DS$
	0	1
	1	5
	2	23
	3	43
	4	41
	5	15
	6	9
	7	40
	8	67
	9	82
	10	63
	11	26
	12	9
	13	4
	14	3
	15	1
	16	2
	17	1
	18	1
	19	0
	20	1
	21	0
	22	0
	23	0
	24	0
	25	0

$q = 3$	$N_1 = N_2$	$\#DS$
	0	0
	1	0
	2	0
	3	1
	4	6
	5	31
	6	108
	7	306
	8	653
	9	1138
	10	1697
	11	2168
	12	2433
	13	2433
	14	2168
	15	1697
	16	1138
	17	653
	18	306
	19	108
	20	31
	21	6
	22	1
	23	0
	24	0
	25	0
	$\vdots$	$\vdots$
	40	0

3.9 K3 surfaces

There is an abundant literature on K3 surfaces; among them, we refer to [23]. Let X be a K3 surface over $\mathbb{F}_q$; that is, a non-singular projective surface with trivial canonical bundle and irregularity zero. Its Zeta function looks like

$$\zeta_X(t) = \frac{1}{(1-t)P_2(t)(1-q^2t)}$$

where $P_2(t)$ is a degree-22 polynomial in $\mathbb{Z}[t]$ with reciprocal roots α_j satisfying $|\alpha_j| = q$ and $P_2(0) = 1$. For every $m \geq 1$, the number of points satisfies

$$N_m = \#X(\mathbb{F}_{q^m}) = 1 + q^{2m} + \sum_{j=1}^{22} \alpha_j^m \, .$$

Hence, we have

$$|N_m - (1 + q^{2m})| \leq 22q^m \, .$$

The following table displays the intervals with the admissible number of points:

	N_1	N_2	N_3	N_4	N_5	N_6
$q=2$	$[0,49]$	$[0,105]$	$[0,241]$	$[0,609]$	$[321,1729]$	$[2689,5505]$
$q=3$	$[0,76]$	$[0,280]$	$[136,1324]$	$[4780,8344]$	$\dots$	
$q=4$	$[0,105]$	$[0,609]$	$[2689,5505]$	$\dots$		
$q=5$	$[0,136]$	$[76,1176]$	$[12876,18376]$	$\dots$		

For $q \geq 7$ one gets always empty intersections. The only extensions where a K3 surface can have DS are given by:

$$\begin{aligned}
&[\mathbb{F}_{2^m} : \mathbb{F}_2] && \text{for } m = 2,3,4;\\
&[\mathbb{F}_{3^m} : \mathbb{F}_3] && \text{for } m = 2;\\
&[\mathbb{F}_{4^m} : \mathbb{F}_4] && \text{for } m = 2;\\
&[\mathbb{F}_{5^m} : \mathbb{F}_5] && \text{for } m = 2.
\end{aligned}$$

As before, we can manage to count the number of candidate L-polynomials for K3 surfaces with DS. For example, we display only the results for $(q, m) = (2, 2)$, where it turns out that the number of points a priori can be between 34 and 49.

$q = 2$	$N_1 = N_2$	$\#DS$
	34	3581
	35	805
	36	173
	37	41
	38	9
	39	2
	40	0
	41	0
	42	0
	43	0
	44	0
	45	0
	46	0
	47	0
	48	0
	49	0

3.10 Quartic surfaces

Smooth quartic surfaces are a particular type of K3 surfaces. In [25] we can find the complete list of isomorphism classes of quartic surfaces over $\mathbb{F}_2$. There are 528,257 classes, among them we find the 16 cases with DS (fifteen cases for $\mathbb{F}_4/\mathbb{F}_2$ and one for $\mathbb{F}_9/\mathbb{F}_3$).

Quartic	N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8	N_9	N_{10}	N_{11}	N_{12}
2158255080	5	5	65	169	1345	4145	16385	65569	262145	1063105	4194305	16768129
2292308406	5	5	89	201	945	4049	16161	66593	263105	1050945	4192897	16791681
2158252442	5	5	89	265	1105	4241	17057	67105	260801	1054785	4204161	16786561
2292308388	5	5	89	265	1105	4241	17057	67105	260801	1054785	4204161	16786561
2158810705	5	5	89	297	945	3761	16609	68129	263105	1042625	4195713	16779393
2158811781	5	5	89	297	945	4145	16609	66081	263105	1047745	4195713	16816257
2159336387	6	6	72	210	1056	4098	16288	65026	260064	1058626	4193184	16774530
2159366278	6	6	72	210	1056	4098	16288	65026	260064	1058626	4193184	16774530
2685782397	6	6	72	210	1056	4098	16288	65026	260064	1058626	4193184	16774530
2159836282	6	6	84	258	1156	4410	16764	65058	261876	1064586	4197804	16789554
2159836276	6	6	108	258	996	3834	16764	65058	263412	1049226	4197804	16850994
2159336401	6	6	108	322	996	3834	16764	68130	263412	1049226	4197804	16818226
2285460784	6	6	108	322	996	3834	16764	68130	263412	1049226	4197804	16818226
2300755192	9	9	69	257	1169	4209	16417	65793	265281	1067009	4187137	16771841
2283076006	10	10	70	210	1150	4090	16390	70434	263950	1050250	4196950	16752690
2291256562	10	34	10	354	1210	5074	16810	68034	257050	1053874	4202890	16853154

To obtain the equation of the quartic, one should proceed as follows. The digits of "Quartic" written as a 35-bit integer are the coefficients of the quartic monomials in lexicographically order to form the homogenous quartic $f \in \mathbb{F}_2[w, x, y, z]$

defining the quartic surface. For instance, the third quartic surface 2158252442 is given the equation

$$w^3z + wx^3 + wy^3 + wyz^2 + wz^3 + xy^2z + xyz^2 + xz^3 + y^4 + yz^3 + z^4 \,.$$

3.11 Campedelli surfaces

The non-singular projective surfaces X of general type sharing the Hodge diamond:

$$\begin{array}{ccccc} & & 1 & & \\ & 0 & & 0 & \\ 0 & & 8 & & 0 \\ & 0 & & 0 & \\ & & 1 & & \end{array}$$

are called numerical Campedelli surfaces. The Zeta function of X over $\mathbb{F}_q$ is

$$\zeta_X(t) = \frac{1}{(1-t)P_2(t)(1-q^2t)}$$

where $P_2(t)$ is a degree-8 polynomial in $\mathbb{Z}[t]$ with reciprocal roots α_j satisfying $|\alpha_j| = q$ and $P_2(0) = 1$. The number of points satisfies

$$N_m = \#X(\mathbb{F}_{q^m}) = 1 + q^{2m} + \sum_{j=1}^{8} \alpha_j^m \,.$$

Hence, we have

$$|N_m - (1 + q^{2m})| \leq 8q^m \,.$$

By inspection of the admissible intervals, the chances to have DS are reduced to the cases:

$q = 2$	$N_1 = N_2 \in [0, 21]$
	$N_1 = N_3 \in [1, 21]$
$q = 3$	$N_1 = N_2 \in [10, 34]$

In order to get all possible Zeta functions for the numerical Campedelli surfaces with DS, we explore the first integer coefficients of the Weil polynomial

$$L_2(t) = \prod_{j=1}^{8}(t - \alpha_j) = t^8 + a_1 t^7 + a_2 t^6 + a_3 t^5 + \cdots \in \mathbb{Z}[t]\,.$$

Using the Girard-Newton formulas, we have

$$\begin{aligned} N_1 &= 1 + q^2 + \sum_{j=1}^{8} \alpha_j = 1 + q^2 - a_1 \\ N_2 &= 1 + q^4 + \sum_{j=1}^{8} \alpha_j^2 = 1 + q^4 + a_1^2 - 2a_2 \\ N_3 &= 1 + q^6 + \sum_{j=1}^{8} \alpha_j^3 = 1 + q^6 + a_1^3 + 3a_1 a_2 + 3a_3 \end{aligned}$$

and also

$$\begin{aligned} a_1 &= 1 + q^2 - N_1 \\ a_2 &= -\left(a_1^2 + 1 + q^4 - N_2\right)/2 \\ a_3 &= \left(3a_1 a_2 - a_1^3 + 1 + q^6 - N_3\right)/3\,. \end{aligned}$$

In order to have $N_1 = N_2$, we need

$$a_2 = 6 + \frac{a_1(a_1+1)}{2} \qquad \text{for } q = 2;$$

$$a_2 = 36 + \frac{a_1(a_1+1)}{2} \qquad \text{for } q = 3.$$

In order to have $N_1 = N_3$, we need necessarily $q = 2$ and

$$a_3 = 20 + \frac{a_1(1 + 3a_2 - a_1^2)}{3}\,.$$

We have used the resultant of polynomials in order to derive the above conditions on the coefficients.

This is helpful in order to speed the search of Weil polynomials arising from DS. The following Sage code provides the candidate Weil polynomials for $q = 2$. Notice that the sign in the functional equation should be $+1$ since β_2 is even.

```
from sage.rings.polynomial.weil.weil_polynomials import WeilPolynomials

q = 2
for N1 in range(22):
    a1 = (1+q^2)-N1
    a2 = 6 + a1*(a1+1)/2
    WP = WeilPolynomials(8,q^2,sign=1,lead=[1,a1,round(a2)])
    it = iter(WP)
    s  = 0
    for wp in it:
        s+=1
        # print(wp)
    print(N1,'  ',s)
}
```

The following tables provide the counting for the number of candidates of L-polynomials attached to the DS-surfaces of numerical Campedelli type.

$q=2$	$N_1=N_2$	$\#DS$
	0	24
	1	64
	2	124
	3	202
	4	281
	5	354
	6	390
	7	356
	8	280
	9	190
	10	116
	11	65
	12	31
	13	17
	14	8
	15	4
	16	1
	17	0
	18	0
	19	0
	20	0
	21	0

$q=2$	$N_1=N_3$	$\#DS$
	0	0
	1	1
	2	0
	3	0
	4	0
	5	0
	6	1
	7	2
	8	2
	9	0
	10	0
	11	1
	12	0
	13	1
	14	0
	15	1
	16	0
	17	0
	18	0
	19	0
	20	0
	21	0

$q = 3$	$N_1 = N_2$	$\#DS$
	10	1
	11	1
	12	1
	13	1
	14	1
	15	0
	16	0
	17	0
	18	0
	19	0
	20	0
	21	0
	22	0
	23	0
	24	0
	25	0
	26	0
	27	0
	28	0
	29	0
	30	0
	31	0
	32	0
	33	0
	34	0

3.12 General type

From the moduli point of view, surfaces of general type are those less understood among the classification of surfaces. Examples of surfaces of general type are the products $X \times Y$ where X and Y are curves of genus ≥ 2. For that reason, it is worth to link the Zeta function of $X \times Y$ with the Zeta function of each.

Proposition 9. *Let X, Y be curves over $\mathbb{F}_q$ of genus g and g', respectively. Then, we have*

$$\zeta_{X\times Y}(t) = \frac{P_1(t)P_1(qt)}{(1-t)P_2(t)(1-q^2t)}$$

with

$$P_1(t) = P_{1,X}(t)P_{1,Y}(t)$$
$$P_2(t) = (1-qt)^2 \prod_{\substack{1\leq i\leq g\\ 1\leq j\leq g'}} (1-\alpha_i\beta_j t)$$

where $P_{1,X}(t) = \prod_{1\leq i\leq g}(1-\alpha_i t)$ and $P_{1,Y}(t) = \prod_{1\leq j\leq g'}(1-\beta_j t)$ are the numerators of the Zeta functions of X and Y, respectively.

Proof. The formula is a direct application of the Künneth formula presented in Section 1.8. □

Example. Consider the genus-2 curves over $\mathbb{F}_2$ defined by:

$$X:\ y^2 + x\,y = x^5 + x$$
$$Y:\ y^2 + y = x^5 + x^3\,.$$

Their respective Zeta functions are

$$\zeta_X(t) = \frac{4t^4+2t^3+t+1}{(1-t)(1-2t)}$$
$$\zeta_Y(t) = \frac{4t^4+4t^3+2t^2+2t+1}{(1-t)(1-2t)}\,.$$

The Zeta function of $X \times Y$ turns out to be:

$$\zeta_{X\times Y}(t) = 20\,t + 10\,t^2 + \frac{272\,t^3}{3} + 54\,t^4 + 120\,t^5 + \frac{2080\,t^6}{3} + \frac{12760\,t^7}{7} + \cdots$$

The sequences of number of points are:

$$\begin{aligned} N_X &= [4, 4, 16, 24, 24, 64, 88, 288, 520, 1104, 2072, 3936, 8168, 16048, \ldots] \\ N_Y &= [5, 5, 17, 9, 25, 65, 145, 289, 449, 1025, 1985, 4353, 8065, 16385, \ldots] \\ N_{X\times Y} &= [20, 20, 272, 216, 600, 4160, 12760, 83232, 233480, 1131600, 4112920, \ldots] \end{aligned}$$

Notice that the curves X and Y are DS-curves, and also $X \times Y$ is a DS-surface.

Proposition 10. *Let X and Y be curves over $\mathbb{F}_q$. Then $X \times Y$ is a DS-surface for $\mathbb{F}_{q^m}/\mathbb{F}_q$ if and only if both X and Y are DS-curves for $\mathbb{F}_{q^m}/\mathbb{F}_q$.*

Proof. The claim follows from the equalities

$$\#\,(X \times Y)(\mathbb{F}_{q^m}) = \#\,X(\mathbb{F}_{q^m}) \cdot \#\,Y(\mathbb{F}_{q^m}) \geq \#\,X(\mathbb{F}_q) \cdot \#\,Y(\mathbb{F}_q) = \#\,(X \times Y)(\mathbb{F}_q)$$

along with $\#\,X(\mathbb{F}_{q^m}) \geq \#\,X(\mathbb{F}_q)$ and $\#\,Y(\mathbb{F}_{q^m}) \geq \#\,Y(\mathbb{F}_q)$. $\square$

Appendices

Appendix A

Code: Genus-3 Hyperelliptic Curves over $\mathbb{F}_4$

Here we present the Magma program code used to find the complete list of isomorphism classes of genus-3 hyperelliptic curves defined over $\mathbb{F}_4$:

```
// The fields and polynomial ring
K:=GF(4);
K2:=GF(4^2);
K3:=GF(4^3);
K4:=GF(4^4);
A<x>:=PolynomialRing(K);

// The genus
g:=3;

//First we compute all hyperelliptic curves:
//Hyperelliptic Genus g curves can be written as
// y^2+q*y=p
//where deg(q)<=g+1 and deg(p)<=2*g+2
```

```
//if max(2*deg(q),deg(p))=2*g+1 or 2*g+2
//(plus some conditions for non singularity)

//The set of polynomials of degree <= 2*g+2 -- K^(2*g+3)
V11:=VectorSpace(K, 2*g+3);
//The set of polynomials of degree g+1 -- K^(g+2)
V5:=VectorSpace(K,g+2);
P4:=Sort([&+[v[i]*x^(i-1): i in [1..g+2]]: v in V5]);

//We take out the zero polynomial
Exclude(~P4,A!0);

//Now we compute one degree <g+2 polynomial under the action of PGL(2,K)

PP4:=Seqset(P4);
P4:=[];

GL2:=GL(2,K);

while not(IsEmpty(PP4)) do
    p:=Rep(PP4);
    PPp:={Numerator((A[2,1]*x+A[2,2])^(g+1)*Evaluate(p,(A[1,1]*x+A[1,2])/(A[2,1]*x+A[2
    p:=Min(PPp);
    Append(~P4,p);
    PP4 diff:=PPp;
end while;

Sort(~P4);
P4;
```

```
//The set of possible A-numbers for hyperelliptic curves will be ANumbers
//The hyperelliptic curves (as two polynomials) will be saved in CurvesH

ANumbers:={};
CurvesH:={};

//First we compute all curves and save the A-numbers
//and the curves

for q in P4 do
 //for any pol u of deg<g+2, we have iso
 //preserving q given by
 //[p,q] to [q,p+u^2+q*u]
 Gq:=[A: A in GL2 | Numerator((A[2,1]*x+A[2,2])^(g+1)*Evaluate(q,(A[1,1]*x+A[1,
 V11q:=[];
 SVq:=Set(V11);
 Vq:=[];
 for v in V5 do
  u:=&+[v[i+1]*x^i: i in [0..g+1]];
  uq:=u^2+q*u;
  Append(~Vq,V11![Coefficient(uq,i): i in [0..2*g+2]]);
 end for;
 while not(IsEmpty(SVq)) do
    v:=Rep(SVq);
    Sv:={v+u: u in Vq};
    Sv:={&+[v[i+1]*x^i: i in [0..2*g+2]]: v in Sv};
    Sv:={Numerator((A[2,1]*x+A[2,2])^(2*g+2)*Evaluate(v,(A[1,1]*x+A[1,2])/(A[2,
    Sv:={V11![Coefficient(v,i): i in [0..2*g+2]]: v in Sv};
```

```
    Append(~V11q,Min(Sv));
    SVq diff:=Sv;
 end while;
 for v in V11q do
    p:=&+[v[i]*x^(i-1): i in [1..2*g+3]];
    if Max([2*Degree(q),Degree(p)]) gt 2*g then
    try D:=HyperellipticCurve(p,q);
      if Genus(D) eq g then
        Ns:=[#Points(BaseChange(D,GF(#K^i))): i in [1..g]];
        Include(~ANumbers,Ns);
        Include(~CurvesH,[p,q]);
      end if;
    catch e;
    end try;
    end if;
 end for;
end for;

DS:=[];
CDS:=[];
corbes:=SetToSequence(CurvesH);
for c in corbes do
D:= HyperellipticCurve(c[1],c[2]);
       Ns:=[#Points(BaseChange(D,GF(#K^i))): i in [1..g]];
if Ns[1] eq Ns[2] then
    Include(~DS,Ns);
    Include(~CDS,c);
end if;
end for;
```

```
q1<t> := PolynomialRing(RationalField());
z4<x,y,z,w> := PolynomialRing(IntegerRing(),4);
f := x^2*y^2*z^2+w^2*y^2*z^2+w^2*x^2*z^2+w^2*x^2*y^2+x*y*z*w*(x^2+w^2);
Nm := [];
for m := 1 to 3 do
    P3 := ProjectiveSpace(GF(2^m),3);
    S := Scheme(P3,f);
    time
    Nm[m] := #Points(S) ;
end for;
Nm;
```

Appendix B

Code: Algorithm Two

In this appendix we represent the code for Algorithm Two discussed in Section 2.6. We have used Mathematica software.

```
Inter[g_,q_,f_]:={q^f+1-g Floor[2Sqrt[q^f]],q+1+g Floor[2Sqrt[q]]}


DivisorsPol[pol_]:=Module[{fac},
 fac = First@Transpose@Drop[FactorList[pol],1];
 Return@Map[Apply[Times,#]&,Drop[Subsets@fac,1]]]


Strongly[p_]:=Module[{dd,P1,P2,res},
 dd = Drop[DivisorsPol@p,-1];
 For[i=1,i<=Length@dd,i++,
  P1 = dd[[i]];
  P2 = Factor[p/P1];
  res = Resultant[P1,P2,x];
 If[res==-1 || res==1,Return[False]]];
Return[True]]
```

```
LPoly[g_,q_,N_,f_]:=Module[{HL,TT,TC,coefL,L},
 HL = Series[(1-qt)/((1-t)^(N-1)*
   Apply[Times,Table[(1-t^i)^f[[i-1]],{i,2,g}]]),{t,0,g}]//Normal;
 TT = CoefficientList[HL,t];
 If[Length@TT < g+1, TT=Join[TT,Table[0,{i,1,g+1-Length@TT}]]];
 TC = Table[TT[[i]] q^(g+1-i),{i,g,1,-1}];
 coefL = Join[TT,TC];
 Return@Apply[Plus,Table[coefL[[i]] t^(i-1), {i,1,2g+1}]]]

HPoly[g_,q_,N_,f_]:=Module[{tmp,H,th,coefh},
 tmp = First@Last@FactorList@Resultant[qt^2+1-tx,LPoly[g,q,N,f]-t^g H,t];
 th  = Coefficient[tmp,H];
 coefh = CoefficientList[(th H-tmp)/th,x];
 Return@(Apply[Plus,Table[coefh[[i]] x^(i-1),{i,1,g+1}]]//Factor)]

Candidates[g_,q_,a1_,f_]:=Module[{},
 h = HPoly[g,q,a1,Table[a[i],{i,2,g}]];
 l  = {{a1}};
 ll = {};
 For[i=2,i<=g,i++,
  For[k=1,k<=Length@l,k++,
   H = D[h,{x,g-i}]/. Table[a[j] -> l[[K]][[j]],{j,1,i-1}];
   alpha= x/. NSolve[D[H,x],Reals,50];
   ti = Coefficient[H,x,0];
   T  = Expand[H-ti];
   gt = Length@(CoefficientList[T, x])-1;
```

```
If[gt==3,
 yesq  = Floor@Simplify@(T/. x -> N[- 2Sqrt@q,50]);
 ydret = Ceiling@Simplify@(T/. x -> N[ 2Sqrt@q,50]);
 tmp = Numerator@Factor@((ti /. a[i] -> c));
 aa = (c /. Solve[- ydret <= tmp && tmp <= - yesq && c >= 0, Integers]);
 For[s=1,s <= Length@aa,s++,
  G = (H /. a[i] -> aa[s]);
  If[CountRoots[G,{x,-2N[Sqrt[q],50],2N[Sqrt[q],50]}] == i ,
   AppendTo[ll,Flatten[{l[[k]], aa[[s]]}]];
  ];
 ];
];

If[gt==4,
 extm = Map[(T/.x -> #) &,N[alpha,50]];
 vals = Join[{(T/.x -> N[-2Sqrt@q,50])},extm,{(T/.x -> N[2Sqrt@q,50])}];
 valmax = Min[vals[[1]],vals[[3]],vals[[5]]];
 valmin = Max[vals[[2]],vals[[4]]];
  If[valmin <= valmax,
  tmp = Numerator@Factor@((ti /. a[i] -> c));
  aa = (c /.Solve[-Floor@valmax-1 <= tmp && tmp <= -Floor@valmin+1 && c >= 0, I
  For[s=1,s <= Length@aa,s++,
   G = (H /. a[i] -> aa[[s]]);
   If[CountRoots[G,{x,N[-2Sqrt[q],50], N[2Sqrt[q],50]}] == i,
    AppendTo[ll,Flatten[{l[[k]],aa[[s]]}]]]
  ];
 ];
];
```

```
If[gt==5,
 extm = Map[(T /. x → #) &,N[alpha,50]];
 vals = Join[{(T /. x → N[-2Sqrt@q,50])},extm,{(T /. x → N[2Sqrt@q,50])}];
 valmax = Min[vals[[2]],vals[[4]],vals[[6]]];
 valmin = Max[vals[[1]],vals[[3]],vals[[5]]];
If[ valmin <= valmax,
 tmp = Numerator@Factor@((ti /. a[i] -> c));
 aa = (c /.Solve[-Floor@valmax-1<=tmp && tmp<=-Floor@valmin+1 && c>=0, Integers]);
 For[s=1,s <= Length@aa,s++,
  G = (H /. a[i] -> aa[[s]]);
   If[CountRoots[G,{x,N[-2Sqrt[q],50],N[2Sqrt[q],50]}] == i,
    AppendTo[ll,Flatten[{l[[k]],aa[[s]]}]]
   ];
  ];
 ];
];

If[ gt != 3 && gt != 4 && gt != 5,
 vals = Map[Simplify@(T /. x -> #) &,N[alpha, 50]];
 valmax = Max@vals;
 valmin = Min@vals;
 tmp = Numerator@Factor@((ti /. a[i] -> c) - Floor@Max[Abs@valmax,Abs@valmin]);
 aa = (c /. Solve[tmp <= 0 && c >= 0,Integers]);
 For[s=1,s<=Length@aa,s++,
  G = (H /. a[i] -> aa[[s]]);
  If[CountRoots[G,{x,N[-2Sqrt[q],50],N[2Sqrt[q],50]}] == i ,
   AppendTo[ll,Flatten[{l[[k]],aa[[s]]}]];
   ];
  ];
```

```
 ];
];

 If[f <= i, l = Select[ ll, #[[f]] == 0 &], l = ll];
 ll = {};
];
Return[l]]

Serre[g_,q_,a_]:=Strongly@HPoly[g,q,a[[1]],Table[a[[i]],{i,2,g}]]



//Example: counting

Inter[4, 3, 2]
{- 14, 16}

Table[{i, Count[Map[Serre[4, 3, #] &, Candidates [4, 3, i, 2]], True]}, {i, 0,
{{0, 4}, {1, 6}, {2, 21}, {3, 48}, {4, 68}, {5, 79}, {6, 84}, {7, 78},
{8, 40}, {9, 17}, {10, 8}, {11, 3}, {12, 1}, {13, 0}, {14, 0}, {15, 0}, {16, 0

tot = % // Transpose // Last
{4, 6, 21, 48, 68, 79, 84, 78, 40, 17, 8, 3, 1, 0, 0, 0, 0}
Apply[Plus, tot]
457
```

```
//Example:

Select[Candidates[5,2,0,2],Serre[5,2,#]&]

{{0,0,0,8,3},{0,0,1,5,5},{0,0,1,6,5},{0,0,1,8,6},
{0,0,1,9,6},{0,0,1,10,6},{0,0,2,2,7},{0,0,2,3,7},
{0,0,2,5,8},{0,0,2,6,8},{0,0,2,7,8},{0,0,2,8,8},
{0,0,2,8,9},{0,0,2,9,9},{0,0,2,10,10},{0,0,3,1,9},
{0,0,3,3,10},{0,0,3,4,10},{0,0,3,5,10},{0,0,3,6,11},
{0,0,3,7,11},{0,0,3,8,12},{0,0,4,4,12},{0,0,4,5,14},
{0,0,4,6,14},{0,0,4,7,15}}
```

The above list contains the sequences of number of places a_d of degree d

$$\{a_1, a_2, a_3, a_4, a_5\}$$

for the candidate L-polynomials of the genus-5 DS-curves for $\mathbb{F}_{2^2}/\mathbb{F}_2$ with

$$a_1 = N_1 = 0 = N_2 = a_2$$

if any.

Bibliography

[1] A. S. Bamunoba (2014). *Arithmetic of Carlitz polynomials*. Ph.D. thesis, Stellenbosch: Stellenbosch University.

[2] W. Barth, et al. (2015). *Compact complex surfaces*, vol. 4. Springer Science & Business Media.

[3] A. Beauville & B. Arnaud (1996). *Complex algebraic surfaces*. No. 34. Cambridge University Press.

[4] A. M. Bigatti (2020). 'Computations with Algebraic Surfaces'. *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7340950/* .

[5] E. Bombieri (1974). 'Counting points on curves over finite fields'. In *Séminaire Bourbaki vol. 1972/73 Exposés 418–435*, pp. 234–241. Springer.

[6] E. Bombieri & D. Mumford (1976). 'Enriques' classification of surfaces in char. p, III'. *Inventiones mathematicae* **35**(1):197–232.

[7] L. Carlitz (1938). 'A class of polynomials'. *Transactions of the American Mathematical Society* **43**(2):167–182.

[8] L. Carlitz et al. (1935). 'On certain functions connected with polynomials in a Galois field'. *Duke Mathematical Journal* **1**(2):137–168.

[9] K. Conrad (2021). 'Expository papers. Carlitz extensions'. *https://kconrad.math.uconn.edu/blurbs/* .

[10] P. Deligne (1974). 'La conjecture de Weil. I'. *Publications Mathématiques de l'IHES* **43**:273–307.

[11] P. Deligne (1980). 'Weil's conjecture. II'. *Publications Mathématiques of the Institute of Higher Scientific Studies IHES* **52**(1):137–252.

[12] P. Deligne & G. Lusztig (1976). 'Representations of reductive groups over finite fields'. *Annals of Mathematics* **103**(1):103–161.

[13] T. S. Developers (2020). 'SageMath, the Sage Mathematics Software System (Version 9.1)'. *https://www.sagemath.org* .

[14] B. Dwork (1960). 'On the rationality of the zeta function of an algebraic variety'. *American Journal of Mathematics* **82**(3):631–648.

[15] A. Emch (1916). 'Federigo Enriques, Vorlesungen über projektive Geometrie'. *Bulletin of the American Mathematical Society* **22**(5):251–251.

[16] M. Gebhardt (2002). 'Constructing function fields with many rational places via the Carlitz module'. *Manuscripta mathematica* **107**(1):89–99.

[17] J. González (1998). 'On the p-rank of an abelian variety and its endomorphism algebra'. *Publicacions Matemàtiques* **42**:119–130.

[18] A. Grothendieck (1963). 'Elements of algebraic geometry: III. Cohomological study of coherent sheaves, Second part'. *IHES mathematical publications* **17**:5–91.

[19] D. Harvey (2015). 'Computing zeta functions of arithmetic schemes'. *Proceedings of the London Mathematical Society* **111**(6):1379–1401.

[20] E. W. Howe (1995). 'Principally polarized ordinary abelian varieties over finite fields'. *Transactions of the American Mathematical Society* **347**(7):2361–2401.

[21] E. W. Howe & K. E. Lauter (2003). 'Improved upper bounds for the number of points on curves over finite fields'. *Annales de l'Institut Fourier* **53**(6):1677–1737.

[22] E. W. Howe & K. E. Lauter (2012). 'New methods for bounding the number of points on curves over finite fields'. In *Geometry and Arithmetic*, pp. 173–212. European Mathematical Society.

[23] D. Huybrechts (2016). *Lectures on K3 surfaces*, vol. 158. Cambridge University Press.

[24] K. S. Kedlaya (2004). 'Computing zeta functions via p-adic cohomology'. In *International Algorithmic Number Theory Symposium*, pp. 1–17.

[25] K. S. Kedlaya & A. V. Sutherland (2016). 'A census of zeta functions of quartic K3 surfaces over F2'. *LMS Journal of Computation and Mathematics* **19**(A):1–11.

[26] S. Lang (1974). 'Higher dimensional diophantine problems'. *Bulletin of the American Mathematical Society* **80**(5):779–787.

[27] D. Maisner, et al. (2002). 'Abelian surfaces over finite fields as Jacobians'. *Experimental Mathematics* **11**(3):321–337.

[28] B. Mazur (2018). 'The unity and breadth of Mathematics – From Diophantus to today'. *Background notes for the 2018 Paul Bernays Lectures. Private communication*.

[29] B. Mazur, et al. (2018). 'Diophantine stability'. *American Journal of Mathematics* **140**(3):571–616.

[30] D. Mumford, et al. (2015). 'Enriques' classification of surfaces in char p: (I)'. In *Global Analysis*, pp. 325–340. Princeton University Press.

[31] H. Niederreiter & C. Xing (2001). *Rational Points on Curves over Finite Fields (Theory and Applications)*, vol. 285. London Mathematical Society. Cambridge University Press.

[32] M. Rosen (2002). *Number Theory in Function Fields*, vol. 210. Springer Science & Business Media.

[33] S. Y. Rybakov (2005). 'Zeta functions of conic bundles and Del Pezzo surfaces of degree 4 over finite fields'. *Moscow Mathematical Journal* **5**(4):919–926.

[34] S. Y. Rybakov (2008). 'Zeta functions of bielliptic surfaces over finite fields'. *Mathematical Notes* **83**(1):246–256.

[35] J.-P. Serre (1963). 'Zeta and L functions'. In *Arithmetical Algebraic Geometry, Proc. Conf. held at Purdue Univ. (Harper and Row, New York)*, pp. 82–92.

[36] J.-P. Serre (2020). *Rational Points on Curves Over Finite Fields*, vol. 18. Société Mathématique de France.

[37] A. V. Sutherland (2020). 'html home page'. *https://math.mit.edu/drew/* .

[38] L. Taelman (2016). 'K3 surfaces over finite fields with given L-function'. *Algebra & Number Theory* **10**(5):1133–1146.

[39] J. Tate (1971). 'Isogeny classes of abelian varieties over a finite field (after T. Honda)'. *Bourbaki seminar* **1968/69**(Exhibits 347-363):95–110.

[40] G. van der Geer, et al. (2009). 'Tables of Curves with Many Points'. *http://www.manypoints.org* .

[41] A. Weil (1948). *Variéties abéliennes et courbes algébriques*, vol. 1064. Actualités scientifiques et industrielles. Paris, Hermann.

[42] X. Xarles (2020a). 'A census of all genus 4 curves over the field with 2 elements'. *https://github.com/XavierXarles/Censusforgenus4curvesoverF2* .

[43] X. Xarles (2020b). 'A census of all genus 4 curves over the field with 2 elements'. *arXiv preprint arXiv:2007.07822* .

[44] O. Zariski (2006). *An Introduction to the Theory of Algebraic Surfaces*, vol. 83. Lecture Notes in Mathematics. Springer.