Algebraic geometry over a field of positive characteristic

Luca Giuzzi[*]

Lectures given by Prof. J.W.P. Hirschfeld

Abstract

Curves over finite fields not only are interesting structures in themselves, but they are also remarkable for their application to coding theory and to the study of the geometry of arcs in a finite plane. In this note, the basic properties of curves and the number of their points are recounted.

Keywords: Algebraic geometry, Finite fields
MSC (2000): 51E22, 11G20, 94B05

Preface

These notes were inspired by the lectures given by Prof. J.W.P. Hirschfeld at the "Summer school Giuseppe Tallini on finite geometry" held in S.Felice del Benaco (Brescia) in July 1998. The following topics are discussed:

1. Fundamental definitions;
2. When is a projective algebraic set empty?
3. Plane curves;
4. The Riemann–Roch theorem;
5. Applications to coding theory;
6. The number of rational points and the Hasse–Weil theorem;
7. Equality in the Hasse–Weil bound;
8. The Stöhr–Voloch theorem.

Acknowledgements: The author wishes to thank Prof. J.W.P. Hirschfeld for his constant advice and support in the realisation of these notes.

[*] work supported by an I.N.D.A.M studentship

1 Fundamental definitions

1.1 Algebraic definitions

Let R be a commutative ring.

(1) An *ideal* $I \subseteq R$ is a subring of R such that, for any $F \in R$,

$$FI := \{FG : F \in I\} \subseteq I.$$

(2) An ideal I of R is *principal* if there exists an element $F \in I$ such that

$$I = \langle F \rangle = \{FG : G \in R\}.$$

(3) An ideal I is *prime* if $FG \in I$ implies

$$F \in I \text{ or } G \in I.$$

(4) An ideal I is *maximal* if there exist no ideal J of R such that $J \neq R$, $J \neq I$ and

$$I \subset J.$$

(5) Any maximal ideal is prime.

(6) An ideal I is *homogeneous* if it is *generated* by homogeneous polynomials.

(7) A ring R is an *integral domain* if, for any $F, G \in R$,

$$FG = 0 \Rightarrow F = 0 \text{ or } G = 0.$$

(8) The residue class ring of R by a prime ideal is an integral domain.

(9) The residue class ring of R by a maximal ideal is a field.

(10) A ring with only one maximal ideal is a *local ring*.

1.2 Geometric definitions

Some books on algebraic geometry and number theory that may be consulted are Fulton [2], Ireland and Rosen [7], Joly [8], Koblitz [9], Pretzel [12], Schmidt [13], Seidenberg [15], Stichtenoth [17], Thomas [19], van Lint and van der Geer [20], Walker [21].

Let K be an arbitrary field. For most purposes here, K is assumed to be either the finite field $\mathbf{F}_q$ of q elements or its algebraic closure $\overline{\mathbf{F}}_q$.

(1) An *Affine* $n-$*space over* K is

$$AG(n, K) = \mathbf{A}^n(K) = \{x = (x_1, x_2, \ldots, x_n) : x_i \in K \text{ all } i\}.$$

(2) Given $x^* = (x_0, x_1, \ldots, x_n), y^* = (y_0, y_1, \ldots, y_n)$ in $\mathbf{A}^{n+1}(K)\backslash\{(0,\ldots,0)\}$, let $x^* \sim y^*$ if there exists $\lambda \in K\backslash\{0\}$ with $y_i = \lambda x_i$ for all i; write the equivalence class of x^* as $\mathbf{P}(x^*)$. Then, the *projective* $n-$*space over* K is

$$PG(n, K) = \mathbf{P}^n(K) = \{\mathbf{P}(x^*) : x^* \in \mathbf{A}^{n+1}(K)\backslash\{(0,\ldots,0)\}\}.$$

(3) Let $R_n = K[X_1, \ldots, X_n]$ and $\overline{R}_n = K[X_0, X_1, \ldots, X_n]$. For F in R_n, define F^* in $\overline{R}_n$ as

$$F^*(X_0, X_1, \ldots, X_n) = (X_0)^{\deg F} F(X_1/X_0, \ldots, X_n/X_0).$$

We call the mapping which associates F^* to F *homogenisation*.

(4) A subset $\mathcal{V}$ of $AG(n, K)$ is an (*affine*) *algebraic set* if there exists $S \subset R_n$ such that

$$\mathcal{V} = \{x \in AG(n, K) : F(x) = 0 \text{ for all } F \text{ in } S\}.$$

Similarly, a subset $\mathcal{V}$ of $PG(n, K)$ is a (*projective*) *algebraic set* if there exists $S \subset \overline{R}_n$, with all elements homogeneous, such that

$$\mathcal{V} = \{\mathbf{P}(x^*) \in PG(n, K) : F(x^*) = 0 \text{ for all } F \text{ in } S\}.$$

(5) Given an affine algebraic set $\mathcal{V}$ in $AG(n, K)$, the *ideal of* $\mathcal{V}$ is the set of polynomials

$$I(\mathcal{V}) = \{F \in R_n : F(x) = 0 \text{ for all } x \text{ in } \mathcal{V}\}.$$

An affine algebraic set $\mathcal{V}$ is *irreducible* if there do not exist proper algebraic sets $\mathcal{V}_1, \mathcal{V}_2$ with $\mathcal{V} = \mathcal{V}_1 \cup \mathcal{V}_2$. Equivalently, $\mathcal{V}$ is irreducible if and only if its ideal $I(\mathcal{V})$ is *prime*. The pair consisting of an irreducible algebraic set $\mathcal{V}$ in $AG(n, K)$ and its ideal $I(\mathcal{V})$ is an *affine variety*. The *ideal* $I(\mathcal{V})$ of a projective algebraic set $\mathcal{V}$ in $PG(n, K)$, is the ideal of $\overline{R}_n$ generated by all homogeneous polynomials F such that $F(x^*) = 0$ for all $\mathbf{P}(x^*)$ in $\mathcal{V}$. Irreducibility is defined as in the affine case, that is an algebraic set $\mathcal{V}$ in $PG(n, K)$ is irreducible if and only if $\mathcal{V}$ is a homogeneous prime ideal in $\overline{R}_n$. Analogously to the affine case, a *projective variety* consists of an irreducible algebraic set in $PG(n, K)$ together with its (homogeneous) ideal.

(6) The *coordinate ring* of an affine variety $\mathcal{V}$ in $AG(n, K)$ is the residue class ring

$$\Gamma(\mathcal{V}) = R_n/I(\mathcal{V}).$$

The *homogeneous coordinate ring* of a projective variety $\mathcal{V}$ in $PG(n, K)$ is

$$\Gamma_h(\mathcal{V}) = \overline{R}_n/I(\mathcal{V}).$$

Observe that all these rings are integral domains.

(7) The *function field* $K(\mathcal{V})$ of an affine variety $\mathcal{V}$ is the quotient field of its coordinate ring $\Gamma(\mathcal{V})$; that is,

$$\begin{aligned} K(\mathcal{V}) &= \{f/g : f, g \in \Gamma(\mathcal{V}) \text{ with } g \neq 0\} \\ &= \{F/G : F, G \in R_n \text{ with } G(x) \neq 0 \text{ for all } x \in \mathcal{V}\}. \end{aligned}$$

Note that $F/G = F'/G'$ in $K(\mathcal{V})$ if and only if $FG' - F'G = 0$ in $\Gamma(\mathcal{V})$.

In the projective case, an element f in $\Gamma_h(\mathcal{V})$ has *degree d* if d is the smallest degree for which there exists a homogeneous polynomial F such that $f = F + \Gamma_h(\mathcal{V})$. The *function field* $K(\mathcal{V})$ of a projective variety $\mathcal{V}$ is defined as

$$\begin{aligned} K(\mathcal{V}) &= \{f/g : f, g \in \Gamma_h(\mathcal{V}) \text{ of the same degree with } g \neq 0\} \\ &= \{F/G : F, G \in \overline{R}_n \text{ of the same degree with } G(x^*) \neq 0 \text{ for all } \mathbf{P}(x^*) \in \mathcal{V}\}. \end{aligned}$$

Both in the affine and in the projective case, the *dimension* of $\mathcal{V}$ is the transcendence degree of $K(\mathcal{V})/K$. Hence, the dimension of $\mathcal{V}$ is r if r is the smallest integer such that $K(\mathcal{V})$ is a finite algebraic extension of the field $K(t_1, \ldots, t_r)$, where $t_1, \ldots, t_r$ are independent transcendental elements over K. If $r = 1$, then $\mathcal{V}$ is a *curve.*

The dimension of $\mathcal{V}$ may also be defined as the length minus one of the longest chain of irreducible algebraic varieties $\mathcal{V}_0 \subset \ldots \subset \mathcal{V}_r = \mathcal{V}$ contained in $\mathcal{V}$. The two definitions are equivalent.

(8) Given a point x of the affine variety $\mathcal{V}$, the *local ring at x* is

$$\mathcal{O}_x(\mathcal{V}) = \{f/g : f, g \in \Gamma(\mathcal{V}) \text{ with } g(x) \neq 0\};$$

the unique maximal ideal of $\mathcal{O}_x(\mathcal{V})$ is

$$M_x(\mathcal{V}) = \{f/g : f, g \in \Gamma(\mathcal{V}) \text{ with } f(x) = 0, g(x) \neq 0\}.$$

The local ring consists of all the elements of the function field of the variety which are defined at the point x; the maximal ideal at x provides a representation of the point x itself in the function field.

By natural embeddings,

$$K \subset \Gamma(\mathcal{V}) \subset \mathcal{O}_x(\mathcal{V}) \subset K(\mathcal{V}).$$

(9) For $K = \mathbf{F}_q$, write $AG(n, K) = AG(n, q)$ and $PG(n, K) = PG(n, q)$. Given $F_1, \ldots, F_r$ in R_n, with $x = (x_1, \ldots, x_n)$ and $x^* = (x_0, x_1, \ldots, x_n)$ let

$$\begin{aligned} \mathbf{V}(F_1, \ldots, F_r) &= \{x \in AG(n, q) : F_1(x) = \ldots = F_r(x) = 0\}, \\ \mathbf{V}^*(F_1^*, \ldots, F_r^*) &= \{\mathbf{P}(x^*) \in PG(n, q) : F_1^*(x^*) = \ldots = F_r^*(x^*) = 0\}. \end{aligned}$$

Note that $\mathbf{V}$ and $\mathbf{V}^*$ are algebraic sets.

2 When is a projective algebraic set empty?

Consider the following quadrics in $PG(3, q)$:

$$\begin{aligned}\mathcal{V}_1 &= \mathbf{V}(f(X_0, X_1) + \lambda g(X_2, X_3)),\\ \mathcal{V}_2 &= \mathbf{V}(f(X_0, X_1) + \mu g(X_2, X_3)),\end{aligned}$$

with $\lambda \neq \mu$ and f, g binary quadratic forms irreducible over $\mathbf{F}_q$. Then, $\mathcal{V}_1 \cap \mathcal{V}_2 = \varnothing$, since any common points $\mathbf{P}(x_0, x_1, x_2, x_3)$ of the two quadrics must satisfy $f(x_0, x_1) = g(x_2, x_3) = 0$; it makes no difference whether f and g are distinct or not. Note that the sum of the degrees of the quadrics is greater than the dimension of the space. The generalisation of this observation is the Chevalley–Warning theorem for affine algebraic sets [13, Chapter 4], which was given in its projective version by Segre [14].

The idea is that an algebraic set can be empty if and only if the degree of the polynomials which define it is high enough, when compared with the dimension of the ambient space.

Theorem 2.1. *Let $d_1, \ldots, d_r$ be positive integers with $d_1 + \ldots + d_r = d$.*

(a) (i) *There exist $F_1, \ldots, F_r$ in R_n of degrees $d_1, \ldots, d_r$ with $\mathbf{V}(F_1, \ldots, F_r) = \varnothing$ if and only if $d > n$.*

(ii) *There exist $F_1, \ldots, F_r$ in R_n of degrees $d_1, \ldots, d_r$ with $\mathbf{V}^*(F_1^*, \ldots, F_r^*) = \varnothing$ if and only if $d > n$.*

(b) *When $d \leq n$, then, for any $F_1, \ldots, F_r$ in R_n with $N = |\mathbf{V}(F_1, \ldots, F_r)|$ and $N^* = |\mathbf{V}^*(F_1^*, \ldots, F_r^*)|$,*

(i) $N \geq q^{n-d}$;

(ii) $N \equiv 0 \pmod{p}$; *(Warning)*

(iii) $N^* \geq 1 + q + q^2 + \ldots q^{n-d}$;

(iv) $N^* \equiv 1 \pmod{p}$.

Let $f : \mathbf{F}_q \to \mathbf{F}_q$ be any function. Then, Lagrange's Interpolation Formula expresses f as a polynomial, which will be written using the same notation:

$$\begin{aligned} f(X) &= \sum_{t \in \mathbf{F}_q} -f(t)\,\frac{X^q - X}{X - t} && (2.1)\\ &= \sum_{t \in \mathbf{F}_q} f(t)[1 - (X - t)^{q-1}]. && (2.2)\end{aligned}$$

To prove the theorem, this formula will have to be generalised. Consider $F \in R_n$:

$$F(X_1, \ldots, X_n) = \sum a_{i_1, \ldots, i_n} {X_1}^{i_1} \ldots {X_n}^{i_n}. \qquad (2.3)$$

In any finite field $\mathbf{F}_q$, the relation

$$x^q - x = 0$$

holds. There exists a unique $\hat{F} \in R_n$ of degree $q-1$ in each X_i equivalent to F:

$$\begin{aligned} \hat{F}(X_1, \ldots, X_n) &= \sum_{i_1=0}^{q-1} \cdots \sum_{i_n=0}^{q-1} \hat{a}_{i_1,\ldots,i_n} {X_1}^{q-1-i_1} \ldots {X_n}^{q-1-i_n}, & (2.4) \\ \hat{F}(X_1, \ldots, X_n) &\equiv F(X_1, \ldots, X_n) \text{ mod } ({X_1}^q - X_1, \ldots, {X_n}^q - X_n). & (2.5) \end{aligned}$$

Observe that the values of $\hat{F}$ over $\mathbf{F}_q$ are exactly the same as the ones of F, even if the two polynomials cannot be identified. In particular given any F, the forms of $\hat{F}$ over $\mathbf{F}_q$ and $\mathbf{F}_{q^i}$ are different. So, for all $(c_1, \ldots, c_n) \in (\mathbf{F}_q)^n$,

$$\hat{F}(c_1, \ldots, c_n) = F(c_1, \ldots, c_n). \tag{2.6}$$

Let

$$\chi_{c_1,\ldots,c_n}(X_1, \ldots, X_n) = \prod_{i=1}^{n} [1 - (X_i - c_i)^{q-1}]; \tag{2.7}$$

be the *characteristic function* of the set $\{c_1, \ldots, c_n\}$; thus,

$$\chi_{c_1,\ldots,c_n}(x_1, \ldots, x_n) = \begin{cases} 1 & \text{if } (x_1, \ldots, x_n) = (c_1, \ldots, c_n), \\ 0 & \text{if } (x_1, \ldots, x_n) \neq (c_1, \ldots, c_n). \end{cases} \tag{2.8}$$

Hence, $\hat{F}$ can be given explicitly as follows:

$$\hat{F}(X_1, \ldots, X_n) = \sum_{AG(n,q)} F(c_1, \ldots, c_n) \chi_{c_1,\ldots,c_n}(X_1, \ldots, X_n); \tag{2.9}$$

this provides the “generalised Lagrange’s Interpolation Formula”.

Comparing the coefficients of $X_1^{q-1} \ldots X_n^{q-1}$ on both sides of (2.9) shows that

$$\hat{a}_{0,\ldots,0} = (-1)^n \sum_{AG(n,q)} F(c_1, \ldots, c_n). \tag{2.10}$$

Lemma 2.2. *Let d be an integer with* $0 \leq d \leq q-1$. *Then,*

$$\sum_{t \in \mathbf{F}_q} t^d = \begin{cases} 0 & \text{if } d \neq q-1, \\ -1 & \text{if } d = q-1. \end{cases}$$

Proof:

If $d = 0$,

$$\sum_{x \in \mathbf{F}_q} x^d = \sum_{x \in \mathbf{F}_q} 1 = q = 0.$$

When $0 < d < q-1$, let us take z to be a generator of the cyclic group $\mathbf{F}_q^*$; then, $z^d \neq 1$. On the other hand, as x runs over $\mathbf{F}_q$, also zx runs over all the elements of $\mathbf{F}_q$; thus,

$$\sum_{x \in \mathbf{F}_q} x^u = \sum_{x \in \mathbf{F}_q} (zx)^u = z^u \sum_{x \in \mathbf{F}_q} x^u$$

is possible if and only if the sum is zero.

If $d = q-1$,

$$\sum_{x \in \mathbf{F}_q} x^d = 0 + \sum_{x \in \mathbf{F}_q^\star} x^{q-1} = \sum_{x \in \mathbf{F}_q^\star} 1 = q-1 = -1.$$

□

Lemma 2.3. *Let F in R_n have degree $d < n(q-1)$. Then,*

$$\sum_{x \in AG(n,q)} F(x) = 0.$$

Proof: By linearity, it suffices to consider the case in which F is a monomial. If $F(x) = X_1^{d_1} X_2^{d_2} \ldots X_n^{d_n}$, then

$$\sum_{x \in AG(n,q)} F(x) = \prod_{i=1}^{n} \left(\sum_{x_i \in \mathbf{F}_q} x_i^{u_i} \right).$$

Since $d_1 + \ldots + d_n < n(q-1)$, there is a d_j with $nd_j \leq d \leq n(q-1)$. So, by the previous lemma,

$$\sum_{x_j \in \mathbf{F}_q} x_j^{d_j} = 0,$$

and the result follows. □

Proof of parts (ii) and (iv) of Theorem 2.1

With $X = (X_1, \ldots, X_n)$, let

$$G(X) = \prod_{i=1}^{r} \left[1 - F_i(X)^{q-1} \right].$$

Then, G has degree $d(q-1) < n(q-1)$. So, by Lemma 2.3, $\sum_{x \in AG(n,q)} G(x) = 0$. On the other hand, $F_i(x)^{q-1} = 1$ for any $x \in AG(n,q)$, unless $F_i(x) = 0$. Hence, $G(x) = 0$ unless x is a common zero of $F_1, \ldots, F_r$, in which case $G(x) = 1$. Therefore,

$$0 = \sum_{x \in AG(n,q)} G(x) = N,$$

whence $N \equiv 0 \pmod p$.

The projective version follows now readily. Let $N' = |\mathbf{V}(F_1^*, \ldots, F_r^*)|$; that is, N' counts the number of zeros in $AG(n+1,q)$ of $\mathbf{V}(F_1^*, \ldots, F_r^*)$. Then, $N^* = (N'-1)/(q-1)$. As $N' \equiv 0 \pmod p$, so $N^* \equiv 1 \pmod p$. □

For a proof of the following improvement to the theorem, especially relevant when d is small compared to n, see [1, 8].

Theorem 2.4. *With the hypotheses of Theorem 2.1, let $d < n$ and let e be an integer with $e < n/d$. Then, $N \equiv 0 \pmod{q^e}$.*

3 Plane curves

Our attention will be mostly restricted to plane curves. First, some precise definitions are required. Let F in $\mathbf{F}_q[X,Y,Z]$ be homogeneous. As in §1, let

$$\mathbf{V}(F)=\{\mathbf{P}(x,y,z)\in PG(2,q):F(x,y,z)=0\}.$$

Then, the *curve defined by* F is

$$\mathcal{V}=(q,\mathbf{V}(F),(F))=\mathbf{V}(F);$$

sometimes this curve may simply be referred to as F. The elements of $\mathbf{V}(F)$ are the *rational points* of $\mathcal{V}$ and (F) is the ideal generated by F in $\mathbf{F}_q\,[X,Y,Z]$. The polynomial F defines a curve; however, in order to understand the geometry of this curve, the knowledge of zeros of F over $\mathbf{F}_q$ and over any extension of $\mathbf{F}_q$ is required: in fact, the zeros over $\mathbf{F}_q$ are not always sufficient to recover F. Let $\overline{\mathbf{F}}_q$ be the algebraic closure of $\mathbf{F}_q$and write as $PG(2,q^i)$ the projective plane over $\mathbf{F}_{q^i}$. An $\mathbf{F}_{q^i}$*-rational point* of $\mathcal{V}$ is a point $\mathbf{P}(x,y,z)$ in $PG(2,q^i)$ such that $F(x,y,z)=0$. Thus, an $\mathbf{F}_q$-rational point of $\mathcal{V}$ is a rational point of $\mathcal{V}$. A *point* of $\mathcal{V}$ is simply an $\mathbf{F}_{q^i}$-rational point for some positive integer i. Also, let

$$\overline{\mathbf{V}}(F)=\{\mathbf{P}(x,y,z)\in PG(2,\overline{\mathbf{F}}_q):F(x,y,z)=0\}.$$

Hence, a point of $\mathcal{V}$ is just a point which is rational over the algebraic closure of $\mathbf{F}_q$, that is a point of $\overline{\mathbf{V}}(F)$.

A *point of degree* i of $\mathcal{V}$ is a point that is $\mathbf{F}_{q^i}$-rational but not $\mathbf{F}_{q^j}$-rational for $j<i$. A *closed point of degree* i of $\mathcal{V}$ is a set $\{P,P^q,\ldots,P^{q^{i-1}}\}$, where P is a point of degree i.

A *divisor* D on $\mathcal{V}$ is an element of the free group generated by the closed points of $\mathcal{V}$; in other words, D is a formal sum:

$$D=\sum_{P\in\overline{\mathbf{V}}(F)}n_PP,$$

where $n_P\in\mathbf{Z}$ and $n_P=0$ for all but a finite number of P. We say that $D=\sum n_PP$ is an $\mathbf{F}_q$*-divisor* if, when $P\in$ Supp(D) and P is of degree i, then $P'\in$ Supp(D) and $n_{P'}=n_P$, for all P' in the closed point $\{P,P^q,\ldots,P^{q^{i-1}}\}$. The $\mathbf{F}_q$-divisors form the subgroup $\mathrm{Div}_{\mathbf{F}_q}(\mathcal{V})$ of $\mathrm{Div}(\mathcal{V})$.

The *support* of D is

$$\text{Supp}(D)=\{P:n_P\neq 0\}.$$

The *degree* of D is $\deg D=\sum n_P$. The divisors on $\mathcal{V}$ form a free Abelian group $\mathrm{Div}(\mathcal{V})$.

A divisor D is *effective* if $n_P\geq 0$ for all $P\in\mathrm{Supp}(D)$. This allows the introduction of a partial order on the divisor group: we say that

$$D\geq D'$$

if and only if $D-D'$ is effective.

Something has now to be said about singular points.

A *singular point* of $\mathcal{V}$ is a point $\mathbf{P} = \mathbf{P}(x, y, z)$ such that every line through it intersects $\mathcal{V}$ twice in $\mathbf{P}$. That implies that $\mathbf{P}(x, y, z)$ has to satisfy

$$\frac{\partial F}{\partial X} = \frac{\partial F}{\partial Y} = \frac{\partial F}{\partial Z} = 0 \text{ at } (x, y, z).$$

Note that a singular point does not have to be in $\mathbf{V}(F)$, but may be in $\overline{\mathbf{V}}(F)$. For example, consider q to be odd and let $\nu^2 = -1$. Then, with

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

the curve $\mathcal{V}$ has the two singular points $\mathbf{P}(\nu, 1, 0)$ and $\mathbf{P}(-\nu, 1, 0)$, which are rational when $q \equiv 1(\text{mod}4)$ but not when $q \equiv -1(\text{mod}4)$.

Let now F be absolutely irreducible. Also, take $U_2 = \mathbf{P}(0, 0, 1)$ and write

$$F(X, Y, 1) = F_s + F_{s+1} + \ldots + F_m,$$

where $F_s \neq 0$ and each F_i is homogeneous in X and Y of degree i. Then, U_2 has *multiplicity* s on $\mathcal{V}$; it is singular if $s > 1$ and an *ordinary* singular point if F_s has no repeated factors. The factors of F_s are the *tangents* to $\mathcal{V}$ at U_2. To find the properties of any other singular point, it is possible to transform it to U_2 by a translation. The multiplicity of P on $\mathcal{V}$ is denoted by $m_P(\mathcal{V})$.

A line through P is said to be a *tangent* to $\mathcal{V}$ if it meets the curve with multiplicity $k > m_P(\mathcal{V})$.

We say that a double point P is a *node* if there are exactly two tangents passing through it; for example, consider the origin for the curve

$$F = Y^2 - X^2 - X^3$$

defined over the reals.

A *cusp* is a double point at which there is only one tangent; the origin for

$$F = Y^2 - X^3$$

provides an example.

An *isolated double point* is a double point at which the tangents lie in a quadratic extension of the field, and thus are not visible. As an example we can consider the real curve

$$F = Y^2 + X^2 - X^3.$$

Clearly, there are no isolated double points over algebraically closed fields.

In fact, there are two numbers that need to be distinguished for a (plane) curve $\mathcal{V}$. Let N_1^* be the number of rational points on a non-singular model, and let $R = |\mathbf{V}(F)|$. In the case that $q = 2$ and

$$F = (X^2 + XY + Y^2)Z + X^3,$$

$R = 4,\ N_1^* = 3$. Here, $\mathbf{V}(F) = \{\mathbf{P}(0, 0, 1), \mathbf{P}(1, 1, 1), \mathbf{P}(1, 0, 1), \mathbf{P}(0, 1, 0)\}$, but $\mathbf{P}(0, 0, 1)$ is an isolated double point; that is, the tangents in it lie over $\mathbf{F}_4$; thus, the point is not visible on a non-singular model.

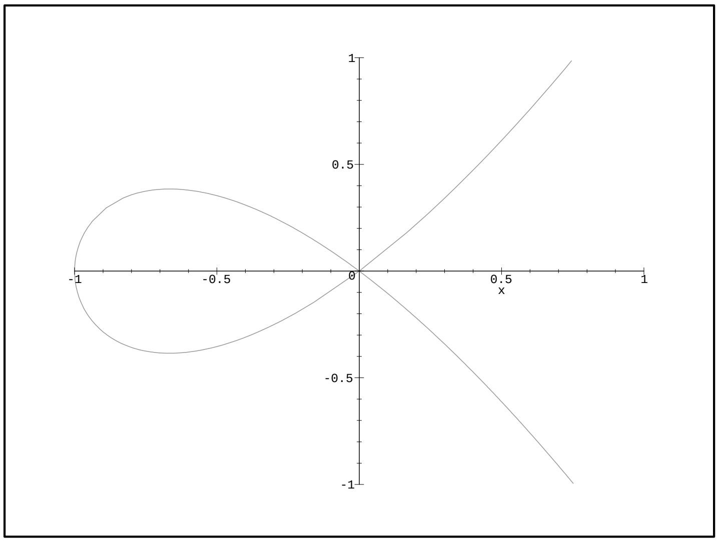

Figure 1: Node

The number N_1^* is generalised to N_i^*, which is the number of $\mathbf{F}_{q^i}$-rational points on a non-singular model of $\mathcal{V}$.

The same definitions applies also to affine curves.

As an example, consider the affine Fermat cubic given by

$$f = X^3 + Y^3 + 1 :$$

(a) over $\mathbf{F}_2$ there are two rational points $(0, 1)$ and $(1, 0)$; hence, $N_1 = 2$;

(b) over $\mathbf{F}_4 := \{0, 1, \omega, \omega^2\}$ there are six rational points:

$$(0,1), \quad (0,\omega), \quad (0,\omega^2),$$

$$(1,0), \quad (\omega,0), \quad (\omega^2,0),$$

whence $N_2 = 6$.

Passing to the projective case, we consider $f^* = X^3 + Y^3 + Z^3$ and we get

(a) $N_1^* = 3$;

(b) $N_2^* = 9$.

Once the multiplicity of a point on a curve has been defined, it is possible to introduce the intersection multiplicity of two curves at a point. Here, such number is not shown to exist; however, effective rules for calculating it are given.

Let $\mathcal{V} = \mathbf{V}(F)$ and $\mathcal{W} = \mathbf{V}(G)$. Then, the *intersection multiplicity of $\mathcal{V}$ and $\mathcal{W}$ at P*, denoted by $I(P, \mathcal{V} \cap \mathcal{W})$, has the following properties.

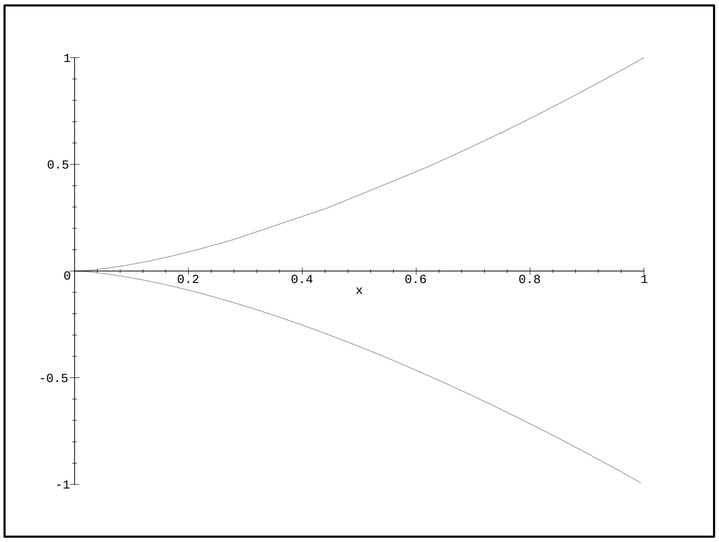

Figure 2: Cusp

I. $I(P, \mathcal{V} \cap \mathcal{W}) = I(P, \mathcal{W} \cap \mathcal{V})$.

II. (a) $I(P, \mathcal{V} \cap \mathcal{W}) = 0$ if $P \notin \overline{\mathbf{V}}(F) \cap \overline{\mathbf{V}}(G)$;

(b) $I(P, \mathcal{V} \cap \mathcal{W}) = \infty$ if $\mathcal{V}$ and $\mathcal{W}$ have a common component through P;

(c) $I(P, \mathcal{V} \cap \mathcal{W}) \in \mathbf{N}$ otherwise.

III. If $\tau \ \in PGL(3, q)$ with $\mathcal{V}\tau = \mathcal{V}', \ \mathcal{W}\tau = \mathcal{W}', \ P\tau = P'$, then $I(P, \mathcal{V} \cap \mathcal{W}) = I(P', \mathcal{V}' \cap \mathcal{W}')$.

IV. $I(P, \mathcal{V} \cap \mathcal{W}) \geq m_P(\mathcal{V}) m_P(\mathcal{W})$, with equality if and only if $\mathcal{V}$ and $\mathcal{W}$ have no common tangent at P.

V. If $F = \prod F_i^{r_i}, \ G = \prod G_j^{s_j}$, with $F_i, \ G_j$ forms in $\overline{\mathbf{F}}_q[X, Y, Z]$ and $\mathcal{V}_i = \mathbf{V}(F_i), \ \mathcal{W}_j = \mathbf{V}(G_j)$, then

$$I(P, \mathcal{V} \cap \mathcal{W}) = \sum_{i,j} r_i s_j I(P, \mathcal{V}_i \cap \mathcal{W}_j).$$

VI. $I(P, \mathcal{V} \cap \mathcal{W}) = I(P, \mathcal{V} \cap \mathcal{H})$, where $\mathcal{H} = \mathbf{V}(H)$, with $H = G + EF$ and E is a form in $\overline{\mathbf{F}}_q[X, Y, Z]$ such that $\deg E = \deg G - \deg F \geq 0$.

VII. (Bézout's theorem) Over an algebraically closed field, if $\mathcal{V}$ of degree m and $\mathcal{W}$ of degree n have no common component, then

$$\sum_P I(P, \mathcal{V} \cap \mathcal{W}) = mn.$$

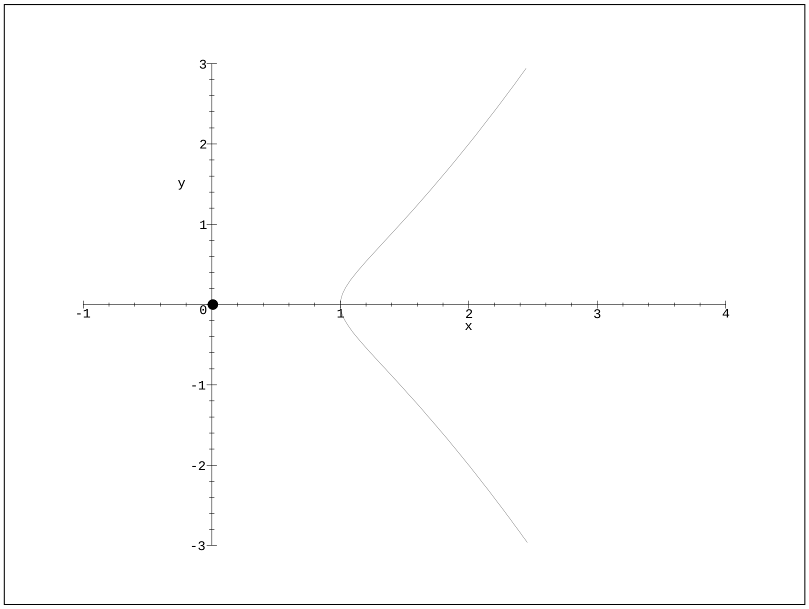

Figure 3: Isolated double point

The *intersection divisor* of $\mathcal{V}$ and $\mathcal{W}$ is the formal sum

$$\mathcal{V}.\mathcal{W} = \sum_P I(P, \mathcal{V} \cap \mathcal{W})P;$$

then, we can write Property VII as

$$\deg(\mathcal{V}.\mathcal{W}) = mn.$$

In order to calculate $I(P, \mathcal{V} \cap \mathcal{W})$, property III is used with $P' = U_2$, and then V and VI are applied till IV can provide a final answer.

As an example consider

$$F = YZ - X^2 \qquad\qquad G = YZ^2 - X^3.$$

By VI, the intersection multiplicity of F and G at any point is the same as that of $G - XF = YZ^2 - XYZ = YZ(Z - X)$ and F. There are no common components through F and G. By V, we can consider the intersections of F with the three components of G, thus

$$F.Y = 2(0,0,1), \qquad F.Z = 2(0,1,0), \qquad F.(Z - X) = (0,1,0) + (1,1,1),$$

whence

$$F.G = 2(0,0,1) + 3(0,1,0) + (1,1,1)$$

and $\deg(F.G) = 6$.

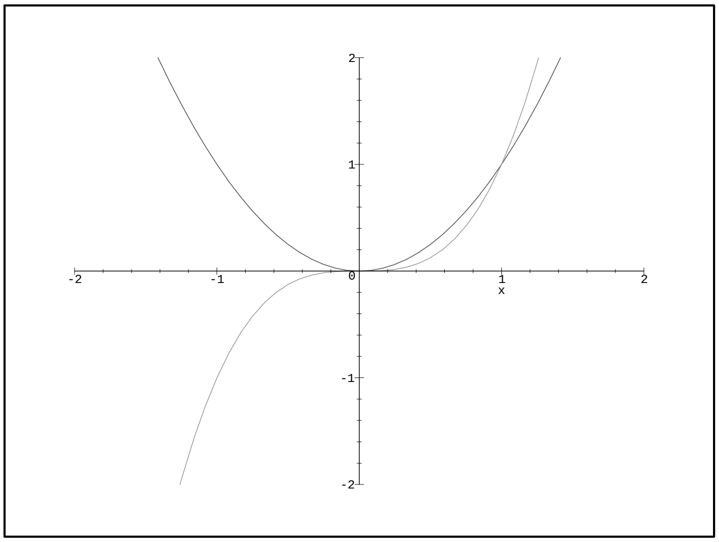

Figure 4: F and G

3.1 Mappings

A *regular* (or *polynomial*) map between two curves F and G is a function $f : F \to G$ defined by two elements f_1, f_2 of the coordinate ring of F such that

$$(x, y) \in \mathbf{V}(F) \to (f_1(x, y), f_2(x, y)) \in \mathbf{V}(G).$$

We say that $\phi \in K(F)$ is *defined* at a point $(x, y) \in F$ if there exist $f, g \in \Gamma(F)$ with $g(x, y) \neq 0$ and

$$\phi(x, y) = \frac{f(x, y)}{g(x, y)}.$$

A *rational map* $\phi : F \to G$ is a pair $\phi_1, \phi_2 \in K(F)$ such that, *if* ϕ_1, ϕ_2 are defined at $(x, y) \in \mathbf{V}(F)$, then $(\phi_1(x, y), \phi_2(x, y)) \in \mathbf{V}(G)$.

An *isomorphism* is a regular map with an inverse regular map.

A *birational isomorphism* is a rational map with an inverse rational map.

The following results show the relationship between algebraic and geometric structures.

Theorem 3.1. *The curve F is isomorphic to G if and only if*

$$\Gamma(F) \simeq \Gamma(G).$$

Theorem 3.2. *The curve F is birationally isomorphic to G if and only if*

$$K(F) \simeq K(G).$$

Example 3.3. Let $F = X$, $G = Y - X^3$ and define $f(0,t) = (t, t^3)$. Then,

$$\Gamma(F) = K[X,Y]/(X) \simeq K[Y]$$

and

$$\Gamma(G) = K[X,Y]/(Y - X^3) \simeq K[X].$$

The inverse of f is $f^{-1}(x,y) = (0,x)$ — clearly this is regular, as well as f is. It follows that

$$\Gamma(F) \simeq \Gamma(G)$$

and the two curves are isomorphic.

Consider now $F = X$ and $G = Y^2 - X^3$ and let $f(0,t) = (t^2, t^3)$. The function f is clearly regular, but the inverse $f^{-1}(x,y) = (0, y/x)$ is *not* at the point $(0,0)$.

On the other hand, $\Gamma(F) = K[Y]$ and $\Gamma(G) = K[X,Y]/(Y^2 - X^3)$, whence

$$K(F) \simeq K(Y).$$

We can also verify that

$$K(G) \simeq K(Y/X) \simeq K(Y) \simeq K(F),$$

whence we obtain that F and G are birationally isomorphic even if not isomorphic.

The *Zarisky topology* in $PG(2,K)$ is defined as the topology whose **closed sets** are intersection of curves. Using this definition it is possible state the following result.

Theorem 3.4. *If $\phi : PG(2,K) \to PG(2,K)$ is an isomorphism on an open set, then ϕ it is a birational isomorphism of $PG(2,K)$.*

A point P of $\mathbf{V}(F)$ with multiplicity m is an *ordinary singular point* if $m \geq 2$ and the tangents at P are all distinct.

For example the singular point $(0,0)$ is ordinary for $F = Y^2 - X^2 - X^3$ in odd characteristic, but it is not ordinary for the curve $F = Y^2 - X^3$.

Nodes are ordinary singular points, cusps are not.

Theorem 3.5. *Let $\mathcal{V}$ be a curve in $PG(2,K)$. Then, there exists a birational isomorphism ϕ of $PG(2,K)$ such that $\phi(\mathcal{V})$ has only ordinary singular points.*

In fact, there exists an algorithm for constructing this birational map: it is based on the use of projectivities and of the standard quadratic transformation

$$(x,y,z) \to (yz, zx, xy).$$

Let $\mathcal{V}$ be a curve with ordinary singular points $P_1, \ldots, P_t$ of multiplicities $s_1, \ldots, s_t$. The *genus* of $\mathcal{V}$ is the number

$$g = g(\mathcal{V}) = \tfrac{1}{2}(m-1)(m-2) - \textstyle\sum_{i=1}^{t} \tfrac{1}{2} s_i(s_i - 1).$$

A curve $\mathcal{V}$ can be transformed into a curve $\mathcal{X}$, not necessarily plane, with no singular points at all. Such a curve $\mathcal{X}$ is a *non-singular model* of $\mathcal{V}$; any two such models are birationally isomorphic.

Example 3.6. Let $\mathcal{V} = \{\mathbf{P}(1, t, t^2, t^3) \in PG(3, K) : t \in K\} \cup \{\mathbf{P}(0, 0, 0, 1)\}$ be the *twisted cubic*. Then there are three types of chords:

(1) tangent;

(2) bisecant;

(3) 0-secant (that is, a bisecant with two non-rational contact points).

Through every point $P \in PG(3, K) \setminus \mathcal{V}$ there is exactly one chord. We say that the point P is of type i if there is a chord of type i through it. Then, the projection of $\mathcal{V}$ through P is a plane cubic with:

(a) a cusp if P is of type (1);

(b) a node if P is of type (2);

(c) an isolated double point if P is of type (3).

Let $\mathcal{V} = \mathbf{V}(F)$ be a curve in $PG(2, K)$. The points of a non–singular model $\mathcal{X}$ of $\mathcal{V}$ are the *places* of $\mathcal{V}$. We say that a place Q is *centred* at P if $\phi(Q) = P$, where $\phi : \mathcal{X} \to \mathcal{V}$.

Any function $\phi \in K(\mathcal{X})$ can be expanded at a simple point P as a formal power series

$$\phi(t) = \sum_{i=r}^{\infty} a_i t^i.$$

The integer r is called the *order* of ϕ at P and it is denoted by the symbol ord$_P(\phi)$. A formal approach to this can be found in [15], pag. 82.

It is always possible to associate a divisor to ϕ. Roughly speaking, if $\phi = f/g$ then

$$\text{div}(\phi) = (\phi) = \mathcal{X}.f - \mathcal{X}.g = \sum v_P(\phi)P,$$

and the valuation $v_P(\phi)$ coincides with ord$_P(\phi)$ as defined above. This divisor may be written as the difference of two effective divisors: $(\phi)_0 - (\phi)_\infty$. In this expression, $(\phi)_0$ is called *divisor of zeros* and $(\phi)_\infty$ is the *divisor of poles* of ϕ. A divisor D such that there exists $\phi \in K(\mathcal{X})$ with $D = (\phi)$ is *principal*. All principal divisors have degree 0, but the converse is not true. The quotient group between the group of all the divisors of degree 0 and the group of all principal divisors is denoted by the symbol $C(\mathcal{X})$. This group plays an important role in the study of the arithmetic and geometric properties of the curve $\mathcal{X}$. In fact, over an algebraically closed field, $C(\mathcal{X})$ is usually denoted by Jac$(\mathcal{X})$ and has the structure of an algebraic variety with an Abelian group law. This variety is called the *Jacobian variety* of $\mathcal{X}$.

Given a curve, we may ask ourselves how many effective $\mathbf{F}_q$-divisors of a prescribed degree i there are. Let M_i be this number.

As an example, consider again the Fermat cubic over $\mathbf{F}_2$. This curve has only $P_0 = (0, 1, 1)$, $P_1 = (1, 0, 1)$ and $P_2 = (1, 1, 0)$ as $\mathbf{F}_2$-rational points; let also:

$$Q_0 = (0, 1, \omega), \qquad Q_0^2 = (0, 1, \omega^2),$$

$$Q_1 = (1, 0, \omega), \qquad Q_1^2 = (1, 0, \omega^2),$$
$$Q_2 = (1, \omega, 0), \qquad Q_2^2 = (1, \omega^2, 0),$$

where $\mathbf{F}_4 = \{0, 1, \omega, \omega^2\}$. Then, we have the following:

- Degree 1: P_0, P_1, P_2, hence $M_1 = 3$;
- Degree 2: $2P_0$, $P_0 + P_1$, etc. and $Q_0 + Q_0^2$, $Q_1 + Q_1^2$, etc. for a total of $M_2 = 9$;
- Degree 3: With similar arguments we get $M_3 = 21$;
- Degree r: we can prove $M_r = 3(2^r - 1)$.

In order to carry out our project more algebraic tools are needed; in fact, the geometry of curves is governed by the properties of local rings.

Theorem 3.7. *Let R be a local ring that is not a field. Then, the following are equivalent:*

(i) *the unique maximal ideal M in R is principal;*

(ii) *there exists $t \in R$ such that if $z \in R \backslash \{0\}$ then $z = ut^n$ for a unique unit u and unique non-negative integer n.*

Such a ring R is a *discrete valuation ring* (DVR); the element t is a *uniformising parameter*.

Suppose, in this situation, that K is a subring of R isomorphic to R/M.

Theorem 3.8.

(i) *For any $z \in R$, there is a unique λ in K such that $z - \lambda \in M$.*

(ii) *For any $n \geq 0$, there are unique $\lambda_0, \lambda_1, \ldots, \lambda_n$ in K and $z_n \in R$ such that*

$$z = \lambda_0 + \lambda_1 t + \ldots + \lambda_n t^n + z_n t^{n+1}.$$

Theorem 3.9.

(i) *The point P on a curve $\mathcal{V}$ is simple if and only if $\mathcal{O}_P(\mathcal{V})$ is a DVR.*

(ii) *In this case, the image $\overline{L}$ in $\Gamma(\mathcal{V})$ of a line $L = aX + bY + c$ that is not a tangent to $\mathcal{V}$ at P is a uniformising parameter for $\mathcal{O}_P(\mathcal{V})$.*

The set of all places P of a curve $\mathcal{V}$ corresponds bijectively to the set of all the maximal ideals M_P of the DVR's of the curve.

In this more abstract setting, the valuation $v_P(\phi)$ of a function $\phi \in \mathcal{O}_P(\mathcal{V})$ at a place corresponding to the ideal M_P can be defined to be the integer n such that $\phi = uL^n$ where u is an unit in $\mathcal{O}_P(\mathcal{V})$.

In order to find $n = v_P(\phi)$ for P in $(\phi)_0$, we write

$$\phi = uL^n;$$

to determine $n = v_P(\phi)$ for P in $(\phi)_\infty$, we write

$$\frac{1}{\phi} = uL^n.$$

Example 3.10. Let us consider the Fermat cubic over the field $\mathbf{F}_2$ and label the set of its $\mathbf{F}_4$-rational points as follows:

$$\begin{array}{ccccccccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & \omega & \omega^2 \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 & 0 & 0 & 0 \\ P_0 & P_1 & P_2 & P_3 & P_4 & P_5 & P_6 & P_7 & P_8 \end{array}.$$

Let $\phi_1 = \frac{X}{Y+Z}$ and $\phi_2 = \frac{Y}{Y+Z}$. Then,

$$\text{div}(\phi_1) = P_1 + P_2 - 2P_0,$$

$$\text{div}(\phi_2) = P_3 + P_4 + P_5 - 3P_0.$$

This shows a remarkable property of divisors of functions; in fact,

(1) $\deg \text{div}(\phi) = 0$;

(2) there is an equivalence relation on $\text{Div}_{\mathbf{F}_q}(\mathcal{X})$ that is given by

$$D' \equiv D \iff D' = D + \text{div}(\phi)$$

for some $\phi \in \mathbf{F}_q(\mathcal{X})$.

Example 3.11.

$$\begin{array}{ccccc} (Y+Z).F & \equiv & Y.F & \equiv & X.F \\ 3P_0 & \equiv & P_3 + P_4 + P_5 & \equiv & P_0 + P_1 + P_2 \end{array}$$

Theorem 3.12. *Let P be a point on the irreducible curve $\mathcal{V}$ with local ring $\mathcal{O}_P$ and maximal ideal M_P. Then, the multiplicity m_P of P on $\mathcal{V}$ is*

$$m_P = \dim_K \left({M_P}^n / {M_P}^{n+1} \right)$$

for all sufficiently large n.

4 The Riemann–Roch theorem

The aim of this theorem is to count the number of rational functions with poles in a given divisor $D = \sum n_P P$. For any divisor D, define $L(D)$ as

$$L(D) = \{\phi \in K(\mathcal{X}) : v_P(\phi) \geq -n_P\};$$

that is, $\phi \in L(D)$ if and only if div$(\phi) + D$ is effective. Clearly, $L(D)$ is a vector space over the field K. We want to compute its dimension $l(D) := \dim L(D)$. This is the same as asking for the maximal number of linearly independent curves cutting out divisors equivalent to D.

Theorem 4.1 (Riemann).

(i) *Given an irreducible curve $\mathcal{X}$, there exists a constant $g \geq 0$ such that, for any divisor D,*

$$l(D) \geq \deg D + 1 - g.$$

The smallest such g is the genus *of $\mathcal{X}$.*

(ii) *There exists an integer N such that, when* $\deg D > N$*,*

$$l(D) = \deg D + 1 - g.$$

(iii) *The genus g is a birational invariant.*

The Riemann–Roch theorem extends part (i) of Theorem 4.1 by giving explicitly the difference between the two sides of the inequality. See [11], chapter 2 for the details.

Example 4.2. Consider as usual the Fermat cubic F over $\mathbf{F}_4$ and let $D = 3P_0$. Then, $\phi_1, \phi_2 \in L(D)$ and $g = 1$; it follows that $l(D) = l(3P_0) = 3 + 1 - 1 = 3$, whence

$$L(3P_0) = \langle 1, \phi_1, \phi_2 \rangle.$$

Let D be a divisor and let $f_0, \ldots, f_r \in L(D)$ be linearly independent. Then the set of effective divisors

$$D_\lambda = \text{div}(\sum \lambda_i f_i) + D$$

as $\lambda_0, \ldots, \lambda_r$ vary in $\overline{\mathbf{F}}_q$ is a *linear series* g^r_n of *degree* n and *dimension* r. The series is *complete* if $L(D) = \langle f_0, \ldots, f_r \rangle$; this is equivalent to say that there is no g^s_n with $s > r$ and $g^r_n \subset g^s_n$.

A *parameter space* for g^r_n is a $PG(r, q)$ given by the bijection

$$D_\lambda \to (\lambda_0, \ldots, \lambda_r).$$

Another way of viewing this is to define

$$f_0 = 1, \qquad f_i = \frac{F_i}{F_0} \text{ for } i \geq 1$$

for suitable polynomials $F_0, \ldots, F_r$. Then,

$$D_\lambda = \mathcal{X}.(\lambda_0 F_0 + \ldots + \lambda_r F_r);$$

that is, the series is *cut out* by the family of curves $\lambda_0 F_0 + \ldots + \lambda_r F_r$.

In Example 4.2, the lines of the plane are a linear combination of $Y + Z$, X and Y and cut out a complete linear series g_3^2 on F.

For a g_n^r, we have $l(D) - 1 = r$, whence we can restate part (ii) of the theorem as follows: given a complete linear series g_n^r with $n > N$,

$$r = n - g.$$

5 Applications to coding theory

It is possible to introduce the following distance function on any vector space V: *for all* x, y *in* V*, let*

$$d(x, y) := |\{i : x_i \neq y_i\}|.$$

This distance is called the *Hamming distance* on V.

An $[n, k, d]_q$-linear code C is a k-dimensional linear subspace of $(\mathbf{F}_q)^n$ such that for all $x, y \in C$ with $x \neq y$ we have

$$d(x, y) \geq d.$$

The parameters are as follows:

n is the *length* of C;

k is the *dimension* of C;

d is the *minimum distance* of C.

The elements of C are called *words*. The *weight* of a word is defined to be the number

$$w(x) = d(x, 0) = |\{i : x_i \neq 0\}|.$$

For a linear code, the minimum distance is

$$d(C) = \min_{x,y \in C x \neq y} d(x, y) = \min_{x \in C x \neq 0} w(x).$$

Clearly, not all the parameters are independent.

Theorem 5.1 (Singleton). *For a linear* $[n, k, d]_q$ *code,*

$$d \leq n - k + 1$$

We say that a code is e*-error correcting* if the minimum distance d between its words satisfies

$$d \geq 2e + 1.$$

A code is an *MDS code* (Maximum Distance Separable code) if the Singleton bound is attained, that is, $d = n - k + 1$.

Usually a code is good if n is small and both k and d are fairly large.

A *generator matrix* for C is a $k \times n$ matrix whose rows form a basis for C.

Example 5.2. Let

$$P_k := \{f \in \mathbf{F}_q[T] : \deg f < k\} =< 1, T, \ldots, T^{k-1} >;$$

$$\mathbf{F}_q = \{t_1, \ldots, t_q\};$$

$$C = \{(f(t_1), \ldots, f(t_q)) : f \in P_k\}$$

Then, $n = q$ and $\dim C = k$. Since there are at most $k-1$ zeros in any word, there are at least $q - (k-1)$ non–zeros, hence

$$d = q - k + 1 = n - k + 1$$

and the code is MDS. The generator matrix G may be written as

$$G = \left[\begin{array}{ccccc} 1 & 1 & 1 & \ldots & 1 \\ t_1 & t_2 & t_3 & \ldots & t_q \\ t_1^2 & t_2^2 & \ldots & & t_q^2 \\ \vdots & & & & \\ t_1^{k-1} & \ldots & \ldots & \ldots & t_q^{k-1} \end{array} \right].$$

5.1 Construction of an algebraic geometry code

These codes were found by Goppa in 1981. Let

(1) $\mathcal{X}$ be an algebraic curve over $\mathbf{F}_q$ of genus g;

(2) $D = P_1 + \ldots + P_n$ be a divisor, where all the P_i are rational and distinct;

(3) $E = m_1Q_1 + \ldots + m_rQ_r$ be a $\mathbf{F}_q$-divisor where $Q_j \neq P_i$ for all i, j; thus, $\deg E = \sum m_j = m$;

(4) θ be the map

$$\theta : \left\{ \begin{array}{ccc} L(E) & \rightarrow & (\mathbf{F}_q)^n \\ f & \rightarrow & (f(P_1), \ldots, f(P_n)) \end{array} \right.$$

(5) $C = C(D, E) := \text{im}\theta = \{(f(P_1), \ldots, f(P_n)) : f \in L(E)\}$.

Then, C is an $[n,k,d]_q$-code whose parameters satisfy the following conditions.

Theorem 5.3. *If $n > m > 2g-2$, then*

(i) $k = m - g + 1$*;*

(ii) $d \geq n - m$*.*

Corollary 5.4.

$$n - k + 1 - g \leq d \leq n - k + 1$$

Proof:

(i) This is the statement of Riemann's theorem.

(ii) If $f \in L(E)$ and $w(\theta(f)) = d$, then f is zero at $n-d$ points $P_{i_1}, \ldots, P_{i_{n-d}}$ forming a divisor D' where $\deg D' = n - d$ and $D' < D$. Now div$f + E$ is effective and no P_{i_j} occurs in E; hence,

$$\text{div} f + E > D'.$$

If we take the degrees of both sides, we obtain now

$$m > n - d,$$

as required.

By adding (i) and (ii) we get

$$k + d \geq n - g + 1,$$

whence the corollary follows. □

Example 5.5. Let $F = X^3 + Y^3 + Z^3$ be the Fermat cubic over $\mathbf{F}_4$, and, with the notation of before, $E = 3P_0$ and $D = P_1 + \ldots + P_8$. Then, we take as generator matrix

$$\begin{array}{c|cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \frac{X}{Y+Z} & 0 & 0 & 1 & \omega^2 & \omega & 1 & \omega^2 & \omega \\ \frac{Y}{Y+Z} & \omega & \omega^2 & 0 & 0 & 0 & 1 & 1 & 1 \end{array} = G.$$

Hence, $n = 8$, $k = 3$, $5 \leq d \leq 6$. Since row 3 of G is a word of weight 5, it follows that $C(D,E)$ is an $[8,3,5]_4$ code with $e = 2$.

The relevance of algebraic geometry codes is that it is possible to determine good upper and lower bounds on their minimum distance.

6 Number of rational points and Hasse–Weil theorem

Assume $\mathcal{C}$ to be a plane curve of genus g defined over $\mathbf{F}_q$, and let $\mathcal{X}$ be its non-singular model. Also, let

(1) N_i be the number of points of $\mathcal{V}$ that are rational over $\mathbf{F}_{q^i}$;

(2) M_s be the number of effective $\mathbf{F}_q$-divisors on $\mathcal{V}$ of degree s;

(3) B_j be the number of closed points of degree j.

We define the zeta function of $\mathcal{X}$ as

$$\zeta_{\mathcal{X}}(T) = \sum_{\mathrm{Div}_{\mathbf{F}_q}(\mathcal{X})} T^{\deg D} = 1 + \sum_{s=1}^{\infty} M_s T^s.$$

Lemma 6.1.

(i) $N_i = \sum_{j|i} jB_j$.

(ii) $\zeta_{\mathcal{X}}(T) = \prod_{j=1}^{\infty}(1-T^j)^{-B_j} = \exp(\sum_{i=1}^{\infty} N_i T^i/i)$.

Thus, the zeta function encodes information on the number of rational points of $\mathcal{C}$ over any extension of $\mathbf{F}_q$.

Theorem 6.2. (Hasse–Weil)

$$\zeta_{\mathcal{X}}(T) = f(T)/\{(1-T)(1-qT)\},$$

where

(i) $f(T) = (1-\alpha_1 T)\dots(1-\alpha_{2g}T) \in \mathbf{Z}[T]$;

(ii) $\alpha_1, \dots, \alpha_{2g}$ *are complex numbers;*

(iii) $\alpha_j \alpha_{g+j} = q,\ j = 1, \dots, g$;

(iv) $|\alpha_j| = \sqrt{q},\ j = 1, \dots, 2g$.

Corollary 6.3.

(i) $N_i = 1 + q^i - (\alpha_1^i + \dots + \alpha_{2g}^i)$;

(ii) $|N_i - (1+q^i)| \leq 2g\sqrt{q^i}$.

Proof:

(i) This follows by taking logarithms of both sides in the theorem.

(ii) From (i),

$$\begin{aligned}|N_i - (1+q^i)| &= |\alpha_1^i + \ldots + \alpha_{2g}^i| \\ &\leq |\alpha_1^i| + \ldots + |\alpha_{2g}^i| \\ &= 2g\sqrt{q^i}.\end{aligned}$$

□

Example 6.4. Recall that

$$\begin{aligned}\log \frac{f(T)}{(1-T)(1-qT)} &= (c_1T + c_2T^2 + \ldots) \\ &\quad -(c_1T + c_2T^2 + \ldots)/2 + \ldots \\ &\quad +(T + T^2/2 + \ldots \\ &\quad +(qT + q^2T^2/2 + \ldots \\ &= (1+q+c_1)T + (1+q^2+2c_2-c_1^2)T^2/2 + \ldots\end{aligned}$$

Hence, $N_1 = 1+q+c_1$, $N_2 = 1+q^2+2c_2-c_1^2$.
We now consider some special cases:

(1) If $g = 0$, then $\mathcal{X}$ is either a line or a conic.

$$\zeta_{\mathcal{X}}(T) = \frac{1}{(1-T)(1-qT)}.$$

We get $c_1 = 0$, and $N_i = 1+q^i$ for all i.

(2) $F = X^3 + Y^3 + Z^3$ over $\mathbf{F}_2$; then,

$$\zeta_F(T) = \frac{1+c_1T+2T^2}{(1-T)(1-2T)}.$$

Since $N_1 = 3 = 1+2+c_1$, we get $c_1 = 0$; hence,

$$\log \zeta_F(T) = \sum (-1)^{(j-1)}(2T^2)^j/j + \sum T^i/i + \sum (2T)^i/i.$$

This implies that

$$N_h = \begin{cases} 1+2^h & \text{for } h \text{ odd} \\ 1+2^h+2^{1+h/2} & \text{for } h \equiv 2(\text{mod} 4) \\ 1+2^h-2^{1+h/2} & \text{for } h \equiv 0(\text{mod} 4)\end{cases}$$

Corollary 6.5. (i) $|N_1 - (1+q)| \leq 2g\sqrt{q}$;

(ii) $N_1 = 1+q-(\alpha_1 + \ldots + \alpha_{2g})$;

(iii) $N_2 = 1+q^2-(\alpha_1^2 + \ldots + \alpha_{2g}^2)$.

Corollary 6.6. *For a plane non-singular curve of degree d,*

$$|N_1 - (1+q)| \leq (d-1)(d-2)\sqrt{q}.$$

7 Equality in the Hasse–Weil bound

The *Hermitian* curve $\mathcal{U}_{2,q}$ is defined by

$$F = X^{\sqrt{q}+1} + Y^{\sqrt{q}+1} + Z^{\sqrt{q}+1},$$

where q is a square. This gives an example of a curve $\mathcal{V}$ in which the upper bound in Corollary 6.5(i) is achieved. Here, $g = \frac{1}{2}(q - \sqrt{q})$, whence

$$q + 1 + 2g\sqrt{q} = q + 1 + (q - \sqrt{q})\sqrt{q} = q\sqrt{q} + 1 = N_1.$$

Conversely, the curve $\mathcal{U}' = (q^2, \mathbf{V}(F), (F))$, obtained taking the same equation F over $GF(q^2)$ archives the lower bound on the number of its rational points.

A curve $\mathcal{V}$ is *maximal* if $N_1 = q + 1 + 2g\sqrt{q}$. Thus, $\mathcal{U}_{2,q}$ is one example.

Theorem 7.1. *Let $\mathcal{V}$ be a maximal curve. Then, the inverse roots satisfy*

$$\alpha_i = -\sqrt{q}$$

for all i.

Proof: The result follows from Theorem 6.2 (iii) and Corollary 6.5 (ii). □

It can also be seen that the zeta function of a maximal curve $\mathcal{V}$ is

$$\zeta_{\mathcal{V}}(T) = \frac{(1 + \sqrt{q}T)^{2g}}{(1 - T)(1 - qT)};$$

that of the Hermitian curve is

$$\zeta_{\mathcal{U}_2}(T) = \frac{(1 + \sqrt{q}T)^{q-\sqrt{q}}}{(1 - T)(1 - qT)}.$$

In fact, the Hasse–Weil theorem provides a good bound when q is large compared to the genus g, but it is not so good when g is large compared to q.

Write $N_q(g) := \max N_1$, where N_1 is computed for non–singular curves of genus g over $\mathbf{F}_q$ and define

$$A_q := \lim \sum_{g \to \infty} \frac{N_q(g)}{g}.$$

From the Hasse–Weil theorem it follows that $A_q \leq \lfloor 2\sqrt{q} \rfloor$. However, this can be improved.

Theorem 7.2 (Drinfeld-Vlăduţ). *The parameter A_q satisfies*

$$A_q \leq \sqrt{q} - 1$$

with equality for q square.

8 The Stöhr–Voloch theorem

In this section we summarise some background material concerning Weierstrass points and Frobenius orders from Stöhr and Voloch [18].

Let us start by considering what happens in the case of the lines. The *order sequence* of a non-singular curve F with respect to the lines at a point P is given by the three numbers

$$\min I(P, l_i \cap F),$$

$i = 1, 2, 3$, where

(1) l_1 is an arbitrary line of $PG(2, q)$;

(2) l_2 contains P;

(3) l_3 is the tangent T_P.

For example, for the Hermitian curve $\mathcal{U}_{2,q}$ the order sequence is

(i) $(0, 1, \sqrt{q})$ if P is not rational;

(ii) $(0, 1, \sqrt{q} + 1)$ if P is rational.

In order to count the number of points of a plane curve F, we can consider a family of curves in the plane meeting F and apply some technique in order to count the intersections of members of this family with the given curve.

For a general curve F, a *point of inflexion* is a simple point P of F such that if T_P is the tangent at P to F, then $I(P, T_P \cap F) \geq 3$.

The Hasse–Weil theorem keeps track only of the singularities of F that turn up in the computation of the genus; the Stöhr-Voloch theory considers inflexions with respect to a given family of curves.

The essential idea is as follows: consider the action induced by the morphism

$$\phi : (x, y, z) \to (x^q, y^q, z^q)$$

over $\mathbf{F}_q$ and let $G(X, Y) = F(X, Y, 1)$. The curve F is fixed by ϕ, and so are all its $\mathbf{F}_q$-rational points. Thus, we have that the set of all the $\mathbf{F}_q$-rational points of F is contained in

$$\{P \in \mathcal{V}(F) : \phi(P) = P\}.$$

Write $G_X := \frac{\partial G}{\partial X}$ and $G_Y := \frac{\partial G}{\partial Y}$; then, the tangent at a point $P = (x_0, y_0)$ of F can be written as

$$T_p = G_X(x_0, y_0)(X - x_0) + G_Y(x_0, y_0)(Y - y_0).$$

The following inclusion holds:

$$\{P \in F : \phi(P) = P\} \subseteq \{P \in F : \phi(P) \in T_P\}.$$

Now let $H = (X^q - X)G_X + (Y^q - Y)G_Y$, in order to be able to write

$$\phi(P) \in T_P \iff H(x_0, y_0) = 0,$$

and consider how the curves H and G intersect:

$$\begin{array}{rcl} H_X & = & (qX^{q-1} - 1)G_X + (X^q - x)G_{XX} + (Y^q - Y)G_{YX} \\ & = & -G_X + (X^q - X)G_{XX} + (Y^q - Y)G_{YX} \\ H_Y & = & -G_Y + (X^q - X)G_{XY} + (Y^q - Y)G_{YY}. \end{array}$$

Hence, at a simple rational point $P = (x_0, y_0)$ of F,

$$H_X = -G_X, \qquad\qquad H_Y = -G_Y;$$

that is, at P the curves G and H have a common tangent. If we now let $n = \deg F = \deg G$ and N_1 is the number of rational points of F, by Bezout's theorem we obtain that, when G is not a component of H,

$$(n + q - 1)n = \deg H \deg G = \sum I(Q, H \cap G) \geq 2N_1,$$

whence $N_1 \leq \frac{1}{2}n(n + q - 1)$.

Suppose now that G divides H; that is, $H = 0$ identically, when it is considered as a function on the points of G. Then,

$$(X^q - X)\frac{G_X}{G_Y} + Y^q - Y = 0,$$

and

$$\frac{d^2Y}{dX^2} = \frac{1}{G_Y^2}[G_{XX}G_Y^2 - 2G_{XY}G_XG_Y + G_{YY}G_X^2] = 0.$$

Thus, it is possible to state the following theorem.

Theorem 8.1. *If $\frac{d^2Y}{dX^2} \neq 0$, that is, not all points of F are inflexions, and q is odd, then $N_1 \leq \frac{1}{2}n(n + q - 1)$.*

The case in which all the points of a curve are inflexions can actually happen.

For example, take a field $\mathbf{F}_q$ with q square and let $U = X^{\sqrt{q}+1} + Y^{\sqrt{q}+1} + Z^{\sqrt{q}+1}$ be the Hermitian curve. Let also $P = (x_0, y_0, z_0) \in U$ and let T_0 be the tangent at P_0 to U. Take $P = (x, y, z) \in T_0 \cap U$. Then, we have the following:

$$\begin{array}{lcr} P_0 \in U: & x_0^{\sqrt{q}+1} + y_0^{\sqrt{q}+1} + z_0^{\sqrt{q}+1} = 0, & (1) \\ & x_0^{\sqrt{q}+q} + y_0^{\sqrt{q}+q} + z_0^{\sqrt{q}+q} = 0; & (2) \\ P \in T_0: & x_0^{\sqrt{q}}x + y_0^{\sqrt{q}}y + z_0^{\sqrt{q}}y = 0; & (3) \\ P \in U: & x^{\sqrt{q}+1} + y^{\sqrt{q}+1} + z^{\sqrt{q}+1} = 0. & (4) \end{array}.$$

Hence, substituting z from (3) in (4),

$$(y_0x - x_0y)^{\sqrt{q}}(y_0^qx - x_0^qy) = 0. \qquad (5)$$

Then, we obtain

(i) if $(x, y) = (x_0, y_0)$, from (3), $z = z_0$;

(ii) if $(x, y) = (x_0^q, y_0^q)$, then $z = z_0^q$.

This can be summed up by writing

$$T_0.U = \sqrt{q}P_0 + P_0^q;$$

that is, T_0 meets U once in P_0^q and $\sqrt{q}$ times in P_0; if P_0 is $\mathbf{F}_q$-rational, then the number of times T_0 meets the curve at P_0 is $\sqrt{q} + 1$; otherwise it is $\sqrt{q}$.

As a consequence, we have that every point of U (either rational or not) is an inflexion. Note that this case cannot happen over the complex field, where an Hermitian curve has only 9 inflexions (but in this case we are not counting the rational points anyhow!!).

Example 8.2. Let us consider a curve of genus $g = 3$. Such a curve is birationally isomorphic to a non-singular plane quartic.

We have the following table

q	3	5	7	9	11	13	17	19
$q + 1 + 3[2\sqrt{q}]$	13	18	23	28	30	35	42	44
$2(q + 3)$	12	16	20	24	28	32	40	44
$N_q(3)$	10	16	20	28	28	32	40	44
				$*$				

The case marked by $*$ is the one corresponding to the Hermitian curve.

Now we want to generalise this construction.

For a plane curve F whose generic point P is not an inflexion, the order sequence for lines is $(0, 1, 2)$. Consider the family of conics in the plane and define an order sequence

$$(\epsilon_0, \epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4, \epsilon_5).$$

in the same way as before By considering degenerate conics, the sequence turns out necessarily to have the form

$$(0, 1, 2, 3, 4, \epsilon_5).$$

The very same construction can be seen in a slightly more abstract and general way: let α be the embedding

$$\alpha : \left\{ \begin{array}{ccc} F & \rightarrow & PG(5, q) \\ (x, y, z) & \rightarrow & (x^2, y^2, z^2, yz, zx, xy) \end{array} \right.$$

This map sends a curve of $PG(2, q)$ to a curve of $PG(5, q)$ and transforms the conic of equation

$$\lambda_0 x^2 + \lambda_1 y^2 + \lambda_2 z^2 + \lambda_3 yz + \lambda_4 zx + \lambda_5 xy = 0$$

into a curve that lies in the hyperplane

$$\lambda_0 X_0 + \lambda_1 X_1 + \ldots + \lambda_5 X_5 = 0.$$

If F has degree n, then the lines of $PG(3,q)$ form a linear system of projective dimension 2 and cut out a linear series g_n^2. The conics form a linear system in $PG(5,q)$ of dimension 5, thus cutting out a linear series g_{2n}^5 — the natural space where to consider the curve and the order series is hence $PG(5,q)$.

In general a system of dimension m cuts out a g_d^m and has order sequence

$$(\epsilon_0, \epsilon_1, \ldots, \epsilon_m),$$

where the ϵ_i are the intersection numbers of the families of hyperplanes in $PG(m,q)$ with a suitable embedding of the curve. On the other hand, if D is an element of the linear series g_d^m and $(1, \frac{f_1}{f_0}, \ldots, \frac{f_m}{f_0})$ is a basis for $L(D)$, then the embedding α of F in $PG(m,q)$ is simply given by $(f_0, \ldots, f_m)$.

In this more general setting the role of the tangent line to the curve has to be replaced by the *osculating hyperplane*.

In order to compute the *osculating hyperplane* to a curve in a projective space over a field with finite characteristic it is necessary to use a derivative that “keeps track of the characteristic”. This is accomplished by the *Hasse derivative* D_t. It is defined as follows:

$$D_t t^j = j t^{j-1},$$

but

$$D_t^{(2)} t^j = \frac{1}{2} j(j-1) t^{j-2},$$

and, likewise,

$$D_t^{(r)} t^j = \begin{pmatrix} j \\ r \end{pmatrix} t^{j-r}.$$

Then, the equation of the osculating hyperplane H_Q at a point $Q = \alpha(P)$ is

$$\begin{vmatrix} X_0 & \ldots & \ldots & X_m \\ D_t^{(j_0)} f_0 & \ldots & \ldots & D_t^{(j_0)} f_m \\ \vdots & & & \\ D_t^{(j_{m-1})} f_0 & \ldots & \ldots & D_t^{(j_{m-1})} f_m \end{vmatrix} = 0,$$

where $(j_0, \ldots, j_m)$ is the order sequence for P.

Example 8.3 (the twisted cubic). The cubic is parametrised as follows:

$$(f_0, f_1, f_2, f_3) = (1, t, t^2, t^3)$$

and

$$(j_0, j_1, j_2, j_3) = (0, 1, 2, 3).$$

Hence

$$H_q = \begin{vmatrix} X_0 & X_1 & X_2 & X_3 \\ 1 & t & t^2 & t^3 \\ 0 & 1 & 2t & 3t^2 \\ 0 & 0 & 1 & 3t \end{vmatrix} = t^3X_0 - 3t^2X_1 + 3tX_2 - X_3.$$

We have always $I(Q, H_Q \cap \alpha(F)) = j_m$. The point Q is a *Weierstrass point* if the order sequence is not the trivial one, that is:

$$(j_0, \ldots, j_m) \neq (0, 1, \ldots, m).$$

A curve without Weierstrass points is said to be *classical*. Weierstrass points play here the same role as inflexions in the plane.

As before, we now count the cardinality of the set

$$\{Q \in \alpha(F) : \phi(Q) \in H_Q\}$$

which contains all the rational points.

Let us define

$$W_{(\nu_0,\ldots,\nu_{m-1})} = \begin{vmatrix} X_0 & \ldots & \ldots & X_m \\ D_t^{(\nu_0)} f_0 & \ldots & \ldots & D_t^{(\nu_0)} f_m \\ \vdots & & & \\ D_t^{(\nu_{m-1})} f_0 & \ldots & \ldots & D_t^{(\nu_{m-1})} f_m \end{vmatrix},$$

where the numbers $(\nu_0, \ldots, \nu_{m-1}) \subseteq (\epsilon_0, \ldots, \epsilon_m)$ are as small as possible for the rows of W to be linearly independent. The sequence $(\nu_0, \ldots, \nu_{m-1})$ is called the *Frobenius order sequence*.

Theorem 8.4. *If $\mathcal{X}$ is a projective, non-singular algebraic curve of genus g defined over $\mathbf{F}_q$ with N_1 rational points and g_d^m is a linear series on $\mathcal{X}$ with no fixed points and Frobenius order sequence $(\nu_0, \ldots, \nu_{m-1})$, then*

$$N_1 \leq \frac{1}{m}\{(2g-2)(\nu_0 + \ldots + \nu_{m-1}) + (q+m)d\}.$$

Example 8.5.

(1) If we consider the Hermitian curve, we have $g = \sqrt{q}(\sqrt{q}-1)$ and the Frobenius order sequence is $(\nu_0, \nu_1) = (0, \sqrt{q})$, whence

$$N_1 \leq \frac{1}{2}\{\sqrt{q}(2q - 2\sqrt{q} - 2) + (q+2)(\sqrt{q}+1)\} = q\sqrt{q} + 1.$$

(2) If $g_d^m = g_n^2$, then

$$N_1 \leq \frac{1}{2}\{(2g-2)\nu_1 + n(q+2)\},$$

with $\nu_1 \in \{1, 2, p^v\}$. If not every point is an inflexion and $p > 2$, then $\nu_1 = 1$ and

$$N_1 \leq \frac{1}{2}n(n-3+q+2) = \frac{1}{2}n(n+q-1).$$

(3) If $g^m_d = g^5_{2n}$, then

$$N_1 \leq \frac{1}{5}\{(2g-2)(\nu_1+\nu_2+\nu_3+\nu_4)+2n(q+5)\}.$$

If $\mathcal{X}$ is classical for g^5_{2n}, then $\nu_i = i$ and

$$N_1 \leq \frac{2}{5}n\{5(n-2)+q\}.$$

Some values of $N_q(g)$ for $q = p^h$ are known:

$$N_q(0) = q+1;$$

$$N_q(1) = \begin{cases} q+[2\sqrt{q}] & \text{if } h \text{ is odd, } h \geq 3 \text{ and } p \mid [2\sqrt{q}], \\ q+1+[2\sqrt{q}] & \text{otherwise.} \end{cases}$$

In fact, $q = 128$ is the smallest q for which the first possibility holds when $g = 1$.

A prime power $q = p^h$ is *special* if h is odd and one of the following holds:

(a) $p \mid [2\sqrt{q}]$;

(b) $q = n^2+1$;

(c) $q = n^2+n+1$;

(d) $q = n^2+n+2$.

Let $\{M\} := M - \lfloor M \rfloor$. Then, if q is special,

$$N_q(2) = \begin{cases} q+2[2\sqrt{q}] & \text{if } \{2\sqrt{q}\} > \frac{1}{2}(\sqrt{5}-1), \\ q-1+2[2\sqrt{q}] & \text{otherwise.} \end{cases}$$

If q is not special,

$$N_q(2) = \begin{cases} 2q+2 & \text{if } q = 4, 9, \\ q+1+2[2\sqrt{q}] & \text{otherwise.} \end{cases}$$

For $q \leq 128$ the only special q with $\{2\sqrt{q}\} > \frac{1}{2}(\sqrt{5}-1)$ are 2,8,128.

References

[1] J. Ax, Zeroes of polynomials over finite fields, *Amer. J. Math.* **86** (1964), 255–261.

[2] W. Fulton, *Algebraic curves*, Benjamin, 226 pp., 1969.

[3] J.W.P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Oxford University Press, Oxford, 316 + x pp., 1985.

[4] J.W.P. Hirschfeld, *Projective Geometries Over Finite Fields, Second Edition*, Oxford University Press, Oxford, 555 + xiv pp., 1998.

[5] J.W.P. Hirschfeld, Codes on curves and their geometry. *Rend. Circ. Mat. Palermo Suppl.* **51** (1998), 123–137.

[6] J.W.P. Hirschfeld and J.A. Thas, *General Galois Geometries*, Oxford University Press, Oxford, 407 + xiii pp., 1991.

[7] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, *Second Edition*, Springer-Verlag, Berlin, 388 + xiv pp., 1990.

[8] J.-R. Joly, Equations et variétés algébriques sur un corps fini, *Enseignement Math.* **19** (1973), 1–117.

[9] N. Koblitz, *p-adic Numbers*, *p-adic Analysis*, *and Zeta-Functions, Second Edition*, Springer-Verlag, Berlin, 150 + xii pp., 1984.

[10] D. B. Leep and C. C. Yeomans, The number of points on a singular curve over a finite field, *Arch. Math.* **63** (1994), 420–426.

[11] C. Moreno, *Algebraic curves over finite fields*, Cambridge University Press, Cambridge, 246 + ix pp., 1991.

[12] O. Pretzel, *Codes and Algebraic Curves*, Oxford University Press, Oxford, 192 + xii pp., 1998.

[13] W. M. Schmidt, *Equations over Finite Fields*, *an Elementary Approach*, *Lecture Notes in Math.* **536**, Springer, Berlin, 267 pp., 1976.

[14] B. Segre, Geometry and algebra in Galois spaces, *Abh. Math. Sem. Univ. Hamburg* **25** (1962), 129–139.

[15] A. Seidenberg, *Elements of the Theory of Algebraic Curves*, Addison Wesley, Reading, Mass., 216 + viii pp., 1969.

[16] J.-P. Serre, Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, *C.R. Acad. Sci. Paris Sér. I* **296** (1983), 397–402.

[17] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 260 + x pp., 1991.

[18] K.O. Stöhr and J.F. Voloch, Weierstrass points and curves over finite fields, *Proc. London Math. Soc.* **52** (1986), 1–19.

[19] A. D. Thomas, *Zeta-Functions*: *an Introduction to Algebraic Geometry*, Pitman, London, 1977, 230 pp.

[20] J. H. van Lint and G. van der Geer, *Introduction to Coding Theory and Algebraic Geometry*, Birkhäuser, Basel, 1988, 83 pp.

[21] R. J. Walker, *Algebraic Curves*, Princeton University Press, Princeton, 201 + x pp., 1950 (Dover, New York, 1962).

LUCA GIUZZI, DIPARTIMENTO DI MATEMATICA, FACOLTÀ DI INGEGNERIA, UNIVERSITÀ DEGLI STUDI DI BRESCIA, VIA VALOTTI 9, 25133 BRESCIA (ITALY)

E–mail address: `giuzzi@dmf.unicatt.it`
URL: `http://www.dmf.unicatt.it/˜giuzzi/`

JAMES W.P. HIRSCHFELD, SCHOOL OF MATHEMATICAL SCIENCES, UNIVERSITY OF SUSSEX, BRIGHTON BN1 9QH (UNITED KINGDOM)

E–mail address: `jwph@sussex.ac.uk`
URL: `http://www.maths.susx.ac.uk/Staff/JWPH/`

FIRST PRINTED: OCTOBER 1998 — REVISED VERSION: JULY 2002