Algebraic curves over finite fields

Ruud Pellikaan
Technical University of Eindhoven

Soria Summer School
on Computational Mathematics
July 7, 2008

Content:

Sections 1, 2.1, 2.2 and 2.3 from:
Algebraic geometry codes
by T. Høholdt, J.H. van Lint and R. Pellikaan
in Handbook of Coding Theory, vol 1, pp. 871-961
V.S. Pless and W.C. Huffman eds., Elsevier, Amsterdam 1998.

http://www.win.tue.nl/ ruudp/paper/31.pdf
http://www.win.tue.nl/ ruudp/lectures/slides1-AGC-Soria.pdf

§0 Introduction

Consider a **geometric object** $\mathcal{X}$

with a subset $\mathcal{P}$ consisting of n **points** enumerated by $P_1, \ldots, P_n$.

Suppose there is a **vector space** L over $\mathbb{F}_q$ of
functions on $\mathcal{X}$ with values in $\mathbb{F}_q$.
So $f(P_i) \in \mathbb{F}_q$ for all i and $f \in L$.

Consider the **evaluation map**

$$ev_{\mathcal{P}} : L \longrightarrow \mathbb{F}_q^n$$

defined by $ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n))$.

This evaluation map is linear,
so its image is a **linear code**.

The image and its dual are the objects of study.
The **dimension** and the **minimum distance** of
these codes and their duals will be considered in these lectures.

Decoding algorithms for these codes will be treated in
the other lectures by Tom Høholdt and Mike O'Sullivan.

In this generality not much can be said about the parameters of these codes.

In the following, $\mathcal{X}$ is a subset of the **affine** or **projective space** which is the common set of zeros of some given set of polynomials, called a **variety**.

$P_1, \ldots, P_n$ will be **rational points** of $\mathcal{X}$, that is points that have coordinates in $\mathbb{F}_q$.

The functions will be polynomials or rational functions, that is to say quotients of polynomials.

We call the above codes **algebraic geometry (AG)** codes if some theory of the variety $\mathcal{X}$ gives bounds on the dimension of the vector space L and the minimum distance of the code.

The classical example is given by **Reed-Solomon (RS)** codes.

Here the geometric object $\mathcal{X}$ is the affine line over $\mathbb{F}_q$,
the points are n distinct elements of $\mathbb{F}_q$ and

L is the vector space of polynomials of degree at most $k-1$,
with coefficients in $\mathbb{F}_q$.

This vector space has dimension k.
Such polynomials have at most $k-1$ zeros,
so nonzero codewords have at least $n-k+1$ nonzeros.

Hence this code has parameters $[n, k, n-k+1]$ if $k \leq n$.

The length of a RS code is at most q.

Take as geometric object $\mathbb{A}^m$ the affine space of dimension m over $\mathbb{F}_q$,

for the set $\mathcal{P}$ all the q^m points of this affine space,

and as vector space all polynomials of degree at most r.

Then we get the **Reed-Muller (RM)** codes
of order r in m variables over $\mathbb{F}_q$.

Every variety has a **dimension**.
A variety of dimension one is called an **algebraic curve**.

Let $\mathcal{X}$ be an algebraic curve over $\mathbb{F}_q$ and
$\mathcal{P}$ a set of n distinct points of $\mathcal{X}$ that are defined over $\mathbb{F}_q$.

Let L be a vector space of rational functions with
prescribed behavior of their poles and zeros.

Then we get the **geometric Goppa** codes.

The parameters of these codes are determined
by the theorem of **Riemann-Roch**.

They satisfy the following bound

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

where g is an invariant of the curve called its **genus**

The best codes are obtained for curves of genus zero.

They are in fact extended generalized RS codes.
These codes have length at most $q + 1$.

Therefore they cannot give **asymptotically good sequences** of codes.

The length n of RM codes is not bounded,
but k/n or d/n tends to zero if $n \to \infty$.

The **information rate** $R = k/n$ and

the **relative minimum distance** $\delta = d/n$ of

geometric Goppa codes satisfy the following inequality

$$R + \delta \geq 1 - \frac{g-1}{n}.$$

For good geometric Goppa codes we need
curves of **low genus** with **many rational points**.

By studying the number of rational points on
modular curves over finite fields

It was shown that there exist asymptotically good sequences
of geometric Goppa codes satisfying the

Tsfasman-Vladuţ-Zink (TVZ) bound

$$R + \delta \geq 1 - \frac{1}{\sqrt{q} - 1} \quad \text{when } q \text{ is a square.}$$

This bound is better than the **Gilbert-Varshamov (GV)** bound when $q \geq 49$.

It was the first time that the GV bound could be improved.

§1 Algebraic curves

A **field** is denoted by $\mathbb{F}$ and its **algebraic closure** by $\bar{\mathbb{F}}$.

The **finite field** with $q = p^m$ elements, with p a prime is denoted by $\mathbb{F}_q$.

Let $\mathbb{F}$ be a field. The **prime field** of $\mathbb{F}$ is the smallest field contained in $\mathbb{F}$.
This is $\mathbb{Q}$ the field of rational numbers, or $\mathbb{F}_p$ with p prime.
Then the **characteristic** of $\mathbb{F}$ is 0 or p, respectively.

Let $\mathcal{X}/\mathbb{F}$ be a **variety** $\mathcal{X}$ over a field $\mathbb{F}$

As a **set** $\mathcal{X}$ consists of points defined over $\bar{\mathbb{F}}$ with a **topology** of closed subsets

$\mathcal{X}(\mathbb{F})$ are the $\mathbb{F}$-**rational points** or points **defined over** $\mathbb{F}$

$\mathbb{F}[\mathcal{X}]$ **coordinate ring** or **regular functions** on $\mathcal{X}$

$\mathbb{F}(\mathcal{X})$ **function field** or **rational functions** on $\mathcal{X}$

$\mathbb{A}^n/\mathbb{F}$ is the n-dimensional **affine space** over $\mathbb{F}$

coordinates $(x_1, x_2, \ldots, x_n)$

$\mathbb{A}^n(\mathbb{F}) = \mathbb{F}^n$ is the n-dimensional affine space over $\mathbb{F}$

The closed sets are the algebraic sets.

$\mathbb{F}[\mathbb{A}^n] = \mathbb{F}[X_1, X_2, \ldots, X_n]$ is the coordinate ring of polynomials

$\mathbb{F}(\mathbb{A}^n) = \mathbb{F}(X_1, X_2, \ldots, X_n)$ is the function field of rational functions

Variables: $X_1, X_2, \ldots, X_n$

Monomial: $X^i = X_1^{i_1} \cdots X_n^{i_n}$

Polynomial: $F(X_1, X_2, \ldots, X_n) = \sum_i f_i X^i$

Coefficients: f_i in $\mathbb{F}$

$\mathbb{F}[X_1, X_2, \ldots, X_n]$ is the **ring of all polynomials**

in the variables $X_1, X_2, \ldots, X_n$ with coefficients in $\mathbb{F}$

Let $F_1, \ldots, F_m \in \mathbb{F}[X_1, X_2, \ldots, X_n]$.
Define the **set of zeros** of $F_1, \ldots, F_m$ by

$$V(F_1, \ldots, F_m) = \{ \mathbf{x} \in \bar{\mathbb{F}}^n \mid F_i(\mathbf{x}) = 0 \text{ for all } i \}.$$

Let I be an ideal in $\mathbb{F}[X_1, X_2, \ldots, X_n]$. Define the **zero set** of I by

$$V(I) := \{ \mathbf{x} \in \bar{\mathbb{F}}^n \mid F(\mathbf{x}) = 0 \text{ for all } F \in I \}.$$

Let $I = \langle F_1, \ldots, F_m \rangle$ be the ideal generated by $F_1, \ldots, F_m$

Then $V(F_1, \ldots, F_m) = V(I)$.

Let V be a subset of $\bar{\mathbb{F}}^n$.

Define the **vanishing ideal** of V by

$$I(V) := \{ F \in \mathbb{F}[X_1, X_2, \ldots, X_n] \mid F(\mathbf{x}) = 0 \text{ for all } \mathbf{x} \in V \}$$

Then $I(V)$ is a **radical** ideal,

this means that:

$$F^n \in I(V),\ n \in \mathbb{N}_0 \ \Rightarrow \ F \in I(V).$$

Let I be an ideal. Define the **radical** of I by

$$\text{rad}(I) = \{F \mid F^n \in I \text{ for some } n \in \mathbb{N}_0\}.$$

Hilbert's Nullstellensatz.

$$I(V(I)) = \text{rad}(I)$$

If I is a radical ideal, then it consists of **all** the polynomials that vanish on $V(I)$.

An **algebraic set** in $\mathbb{A}^n$ is a subset of the form $V(I)$.

The algebraic sets form the **closed sets** of the **Zarisky topology**, since

$$V(\{0\}) = \bar{\mathbb{F}}^n, \;\; V(\langle 1 \rangle) = \emptyset,$$
$$V(I) \cup V(J) = V(I \cap J),$$
$$\cap_{a \in A} V(I_a) = V(\textstyle\sum_{a \in A} I_a).$$

The complement of a closed set is called **open**.

An algebraic set is called **irreducible** if it cannot be written as the union of two proper algebraic subsets.

Every algebraic set is the finite union of irreducible **components**

An ideal I is called **prime** if

$$FG \in I \quad \Rightarrow \quad F \in I \text{ or } G \in I.$$

If I is a radical ideal, then
$V(I)$ is irreducible if and only if I is a prime ideal.

Example Let

$$F(X,Y) = X^2 - Y^2 \text{ and } I = \langle F \rangle.$$

The corresponding algebraic set in $\mathbb{A}^2$
is the union of two lines with equations:

$$Y = X \text{ and } Y = -X.$$

and each of these lines is an irreducible algebraic set in the plane .

Example

Suppose that -1 is not a square in $\mathbb{F}$.

Let

$$F(X,Y) = X^2 + Y^2 \text{ and } I = \langle F \rangle.$$

Then I is a prime ideal and $V(I)$ is irreducible.

But I is not prime in $\bar{\mathbb{F}}[X,Y]$ and $V(I)$ is reducible over $\bar{\mathbb{F}}$.

An algebraic set is **absolutely irreducible** if it is irreducible over $\bar{\mathbb{F}}$.

An **affine variety** is an absolutely irreducible algebraic set.

Example Let

$$F(X,Y) = X^2 + Y^2 + Z^2 - 1 \text{ and } I = \langle F \rangle.$$

The corresponding algebraic set in $\mathbb{A}^3$
is the is the affine variety consisting
of all $(x, y, z) \in \bar{\mathbb{F}}^3$ such that

$$x^2 + y^2 + z^2 = 1.$$

Let $\mathcal{X} = V(I)$ be an affine variety in $\mathbb{A}^n$.

Then the **coordinate ring** of $\mathcal{X}$ is defined by

$$\mathbb{F}[\mathcal{X}] := \mathbb{F}[X_1, X_2, \ldots, X_n]/I$$

Two polynomials that differ by an element of I will have the same value in each point of $\mathcal{X}$.

We adopt the following convention:

capital letters $X_1, \ldots, X_n$, Y and Z denote variables.

Polynomials are denoted by F, G and H

and their **cosets** modulo the ideal I

are denoted by **small** letters f, g and h.

Let I be a prime ideal of an affine variety $\mathcal{X} = V(I)$.

Then the coordinate ring $\mathbb{F}[\mathcal{X}]$ is an **integral domain**,

that means:

$$\text{if } fg = 0 \text{ , then } \quad f = 0 \text{ or } g = 0.$$

The **quotient field** or **the field of fractions** of the ring $\mathbb{F}[\mathcal{X}]$

is defined by

$$\mathbb{F}(\mathcal{X}) := \left\{ \frac{f}{g} \mid f, g \in \mathbb{F}[\mathcal{X}], g \neq 0 \right\}$$

and it is called the **function field** of $\mathcal{X}$.

The elements of $\mathbb{F}(\mathcal{X})$ are called **rational functions**.

The **dimension** of the variety $\mathcal{X}$ is defined equivalently by

1) **transcendence degree** of $\mathbb{F}(\mathcal{X})$ over $\mathbb{F}$.

2) the maximal d such that there is a chain of proper inclusions of subvarieties

$$\mathcal{X}_0 \subset \mathcal{X}_1 \subset \cdots \subset \mathcal{X}_d$$

$\mathcal{X}$ is called an **algebraic curve** if this dimension is 1.

So points and the curve itself are the only subvarieties of a curve.

Example Consider the **parabola** $\mathcal{X}$ in $\mathbb{A}^2/\mathbb{F}$ with equation

$$Y^2 = X.$$

The coordinate ring $\mathbb{F}[\mathcal{X}]$ consists of all expressions of the form

$$A + By,$$

where A and B are in $\mathbb{F}[x]$ and y satisfies $y^2 = x$.

The function field $\mathbb{F}(\mathcal{X})$ is an algebraic extension of $\mathbb{F}(x)$ of degree 2, by the element y.

In **projective** space $\mathbb{P}^n$ we have **homogeneous coordinates**.

A point

$$(x_0 : x_1 : \cdots : x_n)$$

in $\mathbb{P}^n$ is the line in $\mathbb{A}^{n+1}$ through the origin and $(x_0, x_1, \ldots, x_n) \neq 0$.

So

$$(x_0 : x_1 : \cdots : x_n) = (y_0 : y_1 : \cdots : y_n)$$

if and only if

$$(x_0, x_1, \ldots, x_n) = \lambda(y_0, y_1, \ldots, y_n)$$

for some $\lambda \in \mathbb{F}^*$.

A polynomial F of the form

$$F(X_0, X_1 \ldots, X_n) = \sum_{i_0+i_1+\cdots+i_n=d} f_i X_0^{i_0} X_1^{i_1} \cdots X_n^{i_n}$$

is called **homogeneous** of degree d. Then

$$F(\lambda x_0, \lambda x_1, \ldots, \lambda x_n) = \lambda^d F(x_0, x_1, \ldots, x_n)$$

Hence it makes sense to consider the **zero set** in $\mathbb{P}^n$
of homogeneous polynomials.

Let I be an ideal in $\mathbb{F}[X_0, X_1, \ldots, X_n]$ generated by homogeneous polynomials.

Define the **zero set** of I in $\mathbb{P}^n$ by

$$V(I) :=$$

$$\{ (x_0 : x_1 : \cdots : x_n) \mid \mathbf{x} \in \bar{\mathbb{F}}^{n+1}, \mathbf{x} \neq 0, F(\mathbf{x}) = 0, F \text{ homogeneous in } I \}.$$

For rational functions to have a meaning one takes only

those quotients F/G for which the numerator F and

the denominator G are homogeneous polynomials of the **same degree**.

If $G(\mathbf{x}) \neq 0$, then

$$\frac{F(\lambda \mathbf{x})}{G(\lambda \mathbf{x})} = \frac{\lambda^d F(\mathbf{x})}{\lambda^d G(\mathbf{x})} = \frac{F(\mathbf{x})}{G(\mathbf{x})}.$$

So the value of F/G is well defined at all point $\mathbf{x}$ of $\mathbb{P}^n$ such that $G(\mathbf{x}) \neq 0$.

A **projective variety** $\mathcal{X}$ is the zero set in $\mathbb{P}^n$
of a homogeneous prime ideal I in $\mathbb{F}[X_0, X_1, \ldots, X_n]$.

Consider the **subring** $R(\mathcal{X})$ of $\mathbb{F}(X_0, X_1, \ldots, X_n)$
consisting of the fractions F/G, where F and G are
homogeneous polynomials of the same degree and $G \notin I$.

Then $R(\mathcal{X})$ has a unique **maximal ideal** $M(\mathcal{X})$
consisting of all those F/G with $F \in I$.

Define the **function field**

$$\mathbb{F}(\mathcal{X}) := R(\mathcal{X})/M(\mathcal{X}).$$

Let $\mathcal{X}$ be a projective variety. Let P be a point on $\mathcal{X}$.

Then a **rational function** ϕ on $\mathcal{X}$ is called
regular at the point P if one can find F and G,
homogeneous polynomials of the same degree,
such that $G(P) \neq 0$ and ϕ is the coset of F/G.

The functions that are regular at every point of the set U
form a ring, denoted by $\mathbb{F}[U]$.

Example Consider the variety $\mathcal{X}$ in $\mathbb{P}^2$ defined by

$$XZ - Y^2 = 0.$$

The function x/y is equal to y/z on the curve, hence it is regular in the point $P = (0 : 0 : 1)$.

The function

$$\frac{2xz + z^2}{y^2 + z^2}$$

is regular in P. By replacing y^2 by xz, we see that

$$\frac{2xz + z^2}{y^2 + z^2} = \frac{2x + z}{x + z}.$$

and therefore it is also regular at $Q = (1 : 0 : 0)$.

Let $\mathcal{X}$ be a projective variety.
Then the only regular functions on $\mathcal{X}$ are constant.

Let U be an affine open subset of $\mathcal{X}$.
Then the coordinate ring $\mathbb{F}[U]$ coincides
with the ring of regular functions on U.

So there is no ambiguity in the notation $\mathbb{F}[U]$.

The **local ring**

$$\mathcal{O}_P \text{ or } \mathcal{O}_P(\mathcal{X})$$

of $P \in \mathcal{X}$ is
the set of all rational functions that are regular at P.

This is indeed a "local ring", since
it has the **unique maximal ideal**,

$$\mathcal{M}_P = \{\, \phi \in \mathcal{O}_P \mid \phi(P) = 0 \,\}.$$

Embedding of an affine variety in a projective variety.

Associate with $F \in \mathbb{F}[X_1, \ldots, X_n]$ the homogeneous polynomial F^* defined by

$$F^*(X_0, X_1, \ldots, X_n) := X_0^d F(X_1/X_0, \ldots, X_n/X_0),$$

where d is the degree of F.

Let $\mathcal{X}$ be an affine variety in $\mathbb{A}^n$
defined by the prime ideal I.

Let I^* be the ideal generated by $\{F^* | F \in I\}$.

Then I^* is a homogeneous prime ideal
defining the projective variety $\mathcal{X}^*$ in $\mathbb{P}^n$.

Let

$$\mathcal{X}_0^* = \{ (x_0 : x_1 : \cdots : x_n) \in \mathcal{X}^* \mid x_0 \neq 0 \}.$$

Then $\mathcal{X}$ is isomorphic with $\mathcal{X}_0^*$
under the map

$$(x_1, \ldots, x_n) \mapsto (1 : x_1 : \cdots : x_n).$$

The points $(x_0 : x_1 : \cdots : x_n) \in \mathcal{X}^*$ such that $x_0 = 0$
are called the **points at infinity** of $\mathcal{X}$.

The isomorphism of function fields

$$\mathbb{F}(\mathcal{X}) \cong \mathbb{F}(\mathcal{X}^*)$$

is given by the map

$$\frac{f}{g} \mapsto \frac{x_0^m f^*}{g^*},$$

where $m = \deg(g) - \deg(f)$.

For any point P of a projective variety $\mathcal{X}$ and

any hyperplane $\mathcal{H}$ not containing P

the complement

$$\mathcal{X} \setminus \mathcal{H}$$

is an affine variety containing P.

Let

$$F = \sum a_{ij} X^i Y^j.$$

The **partial derivative** F_X of F **with respect to** X is defined by

$$F_X = \sum i a_{ij} X^{i-1} Y^j$$

and F_Y is defined similarly.

Let $\mathcal{X}$ be the affine plane curve defined by $F(X, Y) = 0$.

Let $P \in \mathcal{X}$. If

$$F_X(P) = F_Y(P) = 0,$$

then P is called **singular**, otherwise **simple** or **nonsingular**

A curve is called **nonsingular** or **smooth**
if all its points are nonsingular.

Let $P = (a, b)$ be a nonsingular point on $\mathcal{X}$.
The **tangent line** T_P at P is defined by

$$F_X(a, b)(X - a) + F_Y(a, b)(Y - b) = 0.$$

The definitions for a projective plane curve are similar.

Let a projective plane curve be defined by
the homogeneous equation $F = 0$.

Let $P \in \mathcal{X}$. If at least one of the derivatives

$$F_X, \ F_Y, \text{ or } F_Z$$

is not zero in P, then P is called a simple or nonsingular.

Let $P = (a : b : c)$ be a nonsingular point.
Then the **tangent line** at P has equation

$$F_X(P)X + F_Y(P)Y + F_Z(P)Z = 0.$$

The **Fermat curve** $\mathcal{F}_m$
is the projective plane curve with defining equation

$$F := X^m + Y^m + Z^m = 0.$$

The partial derivatives of F are

$$mX^{m-1},\ mY^{m-1},\ \text{and}\ mZ^{m-1}.$$

This curve is nonsingular if and only if
m is relatively prime to the characteristic.

Let $q = r^2$. The **Hermitian curve** $\mathcal{H}_r$ over $\mathbb{F}_q$ is defined by the affine equation

$$U^{r+1} + V^{r+1} + 1 = 0.$$

The corresponding homogeneous equation is

$$U^{r+1} + V^{r+1} + W^{r+1} = 0.$$

Hence it has $r + 1$ points at infinity.
It is the Fermat curve $\mathcal{F}_m$ over $\mathbb{F}_q$ with $m = r + 1$.

The conjugate of $a \in \mathbb{F}_q$ over $\mathbb{F}_r$ with $q = r^2$ is obtained by

$$\bar{a} = a^r.$$

So the equation

$$U^{r+1} + V^{r+1} + W^{r+1} = 0.$$

can be rewritten as

$$U\bar{U} + V\bar{V} + W\bar{W} = 0.$$

Like a Hermitian form over the complex numbers.

Choose an element $b \in \mathbb{F}_q$ such that

$$b^{r+1} = -1.$$

There are exactly $r + 1$ of these, since $q = r^2$.

Let $P = (1 : b : 0)$. Then P is a point of the Hermitian curve.
The tangent line at P has equation

$$U + b^r V = 0.$$

Multiplying the equation $U + b^r V = 0$ with b gives

$$V = bU.$$

Substituting $V = bU$ in the defining equation gives that

$$W^{r+1} = 0.$$

So P is the only intersection point of
the Hermitian curve with the tangent line at P.

New homogeneous coordinates are chosen such that this tangent line becomes the line at infinity.

Let $X_1 = W$, $Y_1 = U$ and $Z_1 = bU - V$.
Then the curve has homogeneous equation

$$X_1^{r+1} = b^r Y_1^r Z_1 + bY_1 Z_1^r - Z_1^{r+1}$$

in the coordinates X_1, Y_1 and Z_1.
Choose an element $a \in \mathbb{F}_q$ such that

$$a^r + a = -1.$$

There are r of these.
Let $X = X_1$, $Y = bY_1 + aZ_1$ and $Z = Z_1$.

Then the curve has homogeneous equation

$$X^{r+1} = Y^r Z + Y Z^r$$

with respect to X, Y and Z.
Hence the Hermitian curve has affine equation

$$X^{r+1} = Y^r + Y$$

with respect to X and Y.

This last equation has $(0 : 1 : 0)$ as the only point at infinity.

The **Klein curve** has homogeneous equation

$$X^3Y + Y^3Z + Z^3X = 0.$$

More generally define the curve $\mathcal{K}_m$
by the equation

$$X^mY + Y^mZ + Z^mX = 0.$$

The partial derivatives are

$$mX^{m-1}Y + Z^m,\ mY^{m-1}Z + X^m \text{ and } mZ^{m-1}X + Y^m.$$

Let $m^2 - m + 1$ be relatively prime to the characteristic.

Let $(x : y : z) \in \mathcal{K}_m$ be a singular point.

If m is divisible by the characteristic, then

$$x^m = y^m = z^m = 0.$$

So $x = y = z = 0$, a contradiction.

If m is relatively prime to the characteristic, then

$$x^m y = -m y^m z = m^2 z^m x.$$

So

$$(m^2 - m + 1) z^m x = x^m y + y^m z + z^m x = 0.$$

Therefore $z = 0$ or $x = 0$, since
$m^2 - m + 1$ is relatively prime to the characteristic.

But $z = 0$ implies

$$x^m = -my^{m-1}z = 0.$$

Furthermore

$$y^m = -mz^{m-1}x.$$

So $x = y = z = 0$, which is a contradiction.
Similarly $x = 0$ leads to a contradiction.

Hence $\mathcal{K}_m$ with equation

$$X^m Y + Y^m Z + Z^m X = 0.$$

is nonsingular if

$$\gcd(m^2 - m + 1, p) = 1.$$

where p is the characteristic.

Show that the converse is also true.

§2 Local parameters and discrete valuations

Let $\mathcal{X}$ be a smooth curve in $\mathbb{A}^2$ defined by the equation $F = 0$.

Let $P = (a, b) \in \mathcal{X}$. The maximal ideal $\mathcal{M}_P$ is generated by $x - a$ and $y - b$.

$$d_P F = F_X(P)(x - a) + F_Y(P)(y - b) = 0.$$

Hence the $\mathbb{F}$-vector space

$$\mathcal{M}_P / \mathcal{M}_P^2$$

has dimension 1 and therefore $\mathcal{M}_P$ has **one generator**.

Hence $\mathcal{M}_P$ of $\mathcal{O}_P$ is a **principal ideal**.

Let $g \in \mathbb{F}[\mathcal{X}]$ be the coset of a polynomial G.

Then g is a generator of $\mathcal{M}_P$ if and only if

$d_P G$ is not a constant multiple of $d_P F$.

Let t be a generating element of $\mathcal{M}_P$.
Then t is called a **local parameter** or **uniformizing parameter**.

Every element $z \in \mathcal{O}_P$ has a unique expression

$$z = ut^m,$$

where u is a unit and $m \in \mathbb{N}_0$.

If $m > 0$, then P is a **zero** of multiplicity m.

We write

$$m = \text{ord}_P(z) = v_P(z).$$

Convention $v_P(0) = \infty > n$ for all $n \in \mathbb{N}_0$.

Theorem The map

$$v_P : \mathcal{O}_P \to \mathbb{N}_0 \cup \{\infty\}$$

is a **discrete valuation**, that is
the map is surjective and satisfies:

(i) $v_p(f) = \infty$ if and only if $f = 0$,
(ii) $v_P(\lambda f) = v_P(f)$ for all nonzero $\lambda \in \mathbb{F}$,
(iii) $v_P(f+g) \geq \min\{v_P(f), v_P(g)\}$
and equality holds when $v_P(f) \neq v_P(g)$,
(iv) $v_P(fg) = v_P(f) + v_P(g)$.
(v) If $v_P(f) = v_P(g)$,
then there exists a nonzero $\lambda \in \mathbb{F}$
such that $v_P(f - \lambda g) > v_P(g)$.

Extend the function v_P to $\mathbb{F}(\mathcal{X})$ by defining

$$v_P(f/g) = v_P(f) - v_P(g).$$

If $v_P(z) = m > 0$, then z has a **zero** of order m in P.

If $v_P(z) = -m < 0$, then z has a **pole** of order m in P.

If $z \in \mathbb{F}(\mathcal{X})$ with $v_P(z) = m$, then we can write

$$z = at^m + z',$$

where $a \in \mathbb{F}$, $a \neq 0$ and $v_P(z') > m$.

In this way, one can show that z has a **(formal) Laurent series**

$$z = \sum_{i \geq m} a_i t^i,$$

where $a_i \in \mathbb{F}$ for all i and $a_m \neq 0$.

Example Let $\mathbb{P}^1$ be the projective line.

A local parameter in the point $P = (1 : 0)$ is

$$x_1/x_0.$$

The rational function

$$\frac{x_0^2 - x_1^2}{x_1^2}$$

has a pole of order 2 at P.

If $\mathbb{F}$ does not have characteristic 2, then $(1 : 1)$ and $(-1 : 1)$ are zeros with multiplicity 1.

Example Let the characteristic of $\mathbb{F}$ be unequal to 2.

Let $\mathcal{X}$ be in $\mathbb{A}^2$ with equation

$$X^2 + Y^2 = 1.$$

Let $P = (1, 0)$. Let $z = 1 - x$.

This function is 0 in P, so it is in $\mathcal{M}_P$.

We claim that z has order 2.

Observe that y is a local parameter in P,
because the line

$$Y = 0$$

is not equal to the tangent line

$$X = 1$$

in P. Furthermore, on $\mathcal{X}$ we have

$$1 - x = y^2/(1 + x)$$

and the function

$$1/(1 + x)$$

is a unit in $\mathcal{O}_P$.

Example Let $\mathcal{X}$ be the plane curve with equation

$$X^3 + Y^3 + Z^3 = 0$$

over the field $\mathbb{F}_2$. Then $Q = (0 : 1 : 1) \in \mathcal{X}$.

Take $t = x/z$ as local parameter at Q.

The expression $x/(y + z)$ does not make sense at Q.

On $\mathcal{X}$ we have

$$\frac{x}{y+z} = \frac{x(y^2+yz+z^2)}{y^3+z^3} = t^{-2} \cdot \frac{y^2+yz+z^2}{z^2},$$

where the second factor on the right is regular and not 0 in Q.

Hence f has a pole of order 2 in Q.

Exercise
$y/(y+z)$ has a pole of order 3 in Q.

Let $\mathcal{X}$ be a curve defined over $\mathbb{F}_q$,
the defining equations have coefficients in $\mathbb{F}_q$.

Then points on $\mathcal{X}$ with all their coordinates in $\mathbb{F}_q$
are called $\mathbb{F}_q$-**rational points**.

The set of all $\mathbb{F}_q$-**rational points** of $\mathcal{X}$ is denoted by:

$$\mathcal{X}(\mathbb{F}_q).$$

Example Consider the Klein quartic with equation

$$X^3Y + Y^3Z + Z^3X = 0$$

over the algebraic closure of $\mathbb{F}_2$.

Over $\mathbb{F}_2$ the rational points are

$$(1:0:0),\ (0:1:0),\ \text{and}\ (0:0:1).$$

Let

$$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\},$$

where

$$\alpha^2 = 1 + \alpha.$$

Over $\mathbb{F}_4$, there are two more points:

$$(1 : \alpha : 1 + \alpha) \text{ and } (1 : 1 + \alpha : \alpha).$$

Exercise
Compute the number of rational points
of the Klein quartic over $\mathbb{F}_8$.

Define $\mathbb{F}_8$ as $\mathbb{F}_2(\xi)$, where

$$\xi^3 = \xi + 1.$$

If a rational point has a coordinate 0,
it must be one of the points over $\mathbb{F}_2$.

If

$$xyz \neq 0,$$

we can take $z = 1$ by symmetry.

If

$$y = \xi^i,\ 0 \leq i \leq 6,$$

then write $x = \xi^{3i}\eta$.

Substitution in the equation gives

$$\eta^3 + \eta + 1 = 0,$$

that is, η is one of the elements

$$\xi,\ \xi^2 \text{ or } \xi^4.$$

So we find a total of

$$3 + 7 * 3 = 24$$

rational points over $\mathbb{F}_8$.

Example Consider the Hermitian curve $\mathcal{H}_2$.

$$X^3 + Y^3 + Z^3 = 0$$

over $\mathbb{F}_4$.

Since a third power of an element of $\mathbb{F}_4$ is 0 or 1,
all the rational points have one coordinate 0.

Take one of the others to be 1, and the third one any nonzero element of $\mathbb{F}_4$.

So we find nine (projective) points.

Exercise Let $q = r^2$.

Consider the Hermitian curve with affine equation

$$X^{r+1} = Y^r + Y$$

Show that it has $r^3 + 1$ points over $\mathbb{F}_q$.

§3 Bézout's theorem

A polynomial of degree m in one variable,
with coefficients in a field has at most m zeros.

If the field is algebraically closed
and if the zeros are counted with **multiplicities**,
then the number of zeros is equal to m.

Bézout's theorem is a generalization of these facts
to polynomials in several variables.

The **degree** of a projective plane curve is
the degree of the defining polynomial.
It is the maximal number of points in the intersection with a line,
not containing a component of the curve.

Consider the intersection of irreducible
nonsingular projective curves $\mathcal{X}$ and $\mathcal{Y}$ of degrees l and m.

Let $G = 0$ be the defining equation of $\mathcal{Y}$.

Let P be a point of $\mathcal{X}$.
Let H be a homogeneous linear form such that $H(P) \neq 0$.
Let h be the class of H modulo the ideal defining $\mathcal{X}$.

Then the **intersection multiplicity**

$$I(P; \mathcal{X}, \mathcal{Y})$$

of $\mathcal{X}$ and $\mathcal{Y}$ at P is defined by $v_P(g/h^m)$.

This definition of the intersection multiplicity does not depend on the choice of H, since h/h' is a unit in $\mathcal{O}_P$ for any other choice of a linear form H' that is not zero in P.

If P is also a point of $\mathcal{Y}$, then

$$I(P; \mathcal{X}, \mathcal{Y}) = I(P; \mathcal{Y}, \mathcal{X}).$$

Bézout's Theorem

Let $\mathcal{X}$ and $\mathcal{Y}$ be two plane curves that have no component in common.
Then $\mathcal{X}$ and $\mathcal{Y}$ intersect in exactly lm points
(counted with multiplicities).

Corollary

The intersection of two projective plane curves is not empty.

Corollary

A nonsingular projective plane curve is irreducible.

Exercise
a) Proof this corollary.
b) Give an example of a nonsingular affine plane curve that is reducible.

Proof

If $F = GH$ is a factorization of F with factors of positive degree, we get

$$F_X = G_X H + G H_X$$

by the product or Leibniz rule for the partial derivative.

So

$$F_X \in (G, H),$$

and similarly for the other two partial derivatives. Hence

$$(F_X, F_Y, F_Z, F) \subseteq (G, H).$$

The zero sets satisfy

$$V(G, H) \subseteq V(F_X, F_Y, F_Z, F).$$

Now $V(G, H)$ is the intersection of the curves with equations $G = 0$ and $H = 0$, and this not empty by the above Corollary.

Therefore the curve has a singular point.

Notice that the assumption that the curve
is a **projective** plane curve is essential.

The equation $X^2Y - X = 0$ defines a nonsingular affine plane curve,
but is clearly reducible.

However if $F = 0$ is an affine plane curve and the homogenization F^*
defines a nonsingular projective curve, then F is irreducible.

The affine curve with equation $X^2Y - X = 0$ has the points
$(1 : 0 : 0)$ and $(0 : 1 : 0)$at infinity,
and $(0 : 1 : 0)$ is a singular point.

Let

$$V_l = \{F \in \mathbb{F}_q[X,Y] \mid \deg(F) \leq l\},$$

the vector space of bivariate polynomials of degree at most l and coefficients in $\mathbb{F}_q$.

Consider an element G of degree m in $\mathbb{F}_q[X,Y]$ such that the homogeneous form G^* defines a nonsingular curve.

Then G is irreducible in $\bar{\mathbb{F}}[X,Y]$, where $\bar{\mathbb{F}}$ is the algebraic closure of $\mathbb{F}_q$.

Let $P_1, P_2, \ldots, P_n$ be rational points on the plane curve defined by the equation $G = 0$, So

$$P_i = (a_i, b_i) \in \mathbb{F}_q^2 \text{ and } G(P_i) = 0 \text{ for } 1 \leq i \leq n.$$

Define the code C by

$$C = \{(F(P_1), F(P_2), \ldots, F(P_n)) \mid F \in \mathbb{F}_q[X, Y], \deg(F) \leq l\}.$$

Theorem Let $n > lm$.

Denote the **minimum distance** of this code by d and its **dimension** by k.

Then

$$d \geq n - lm,$$

and

$$k = \begin{cases} \binom{l+2}{2} & \text{if } l < m, \\ lm + 1 - \binom{m-1}{2} & \text{if } l \geq m. \end{cases}$$

Proof

The monomials of the form $X^\alpha Y^\beta$ with $\alpha + \beta \leq l$ form a basis of V_l.

Hence V_l has dimension $\binom{l+2}{2}$.

Let $F \in V_l$.
If G is a factor of F, then the codeword in C corresponding to F is zero.

Conversely, if this codeword is zero, then the curves with equations $F = 0$ and $G = 0$ have degree $l' \leq l$ and m respectively, and they have the n points $P_1, P_2, \ldots, P_n$ in their intersection.

Bézout's theorem and the assumption $lm < n$ imply that F and G have a common factor.

Since G is irreducible, F must be divisible by G.
Hence the functions $F \in V_l$ that yield the zero codeword form the subspace GV_{l-m}.

This implies that if $l < m$, then $k = \binom{l+2}{2}$,
and if $l \geq m$, then

$$k = \binom{l+2}{2} - \binom{l-m+2}{2} = lm + 1 - \binom{m-1}{2}.$$

The same argument with Bézout's theorem shows that

a nonzero codeword has at most lm coordinates equal to 0,

that is to say, it has weight at least $n - lm$.

Hence

$$d \geq n - lm.$$

Remark

Let $F_1, \ldots, F_k$ is a basis for V_l modulo GV_{l-m}. Then

$$(F_i(P_j) \mid 1 \leq i \leq k, 1 \leq j \leq n)$$

is a **generator matrix** of C.

So it is a **parity check matrix** for the dual of C.
The minimum distance $d^\perp$ of $C^\perp$ is equal to
the minimal number of dependent columns of this matrix.

Hence for all $t < d^\perp$ and every subset $\mathcal{Q}$ of $\mathcal{P} = \{P_1, \ldots, P_n\}$
consisting of t distinct points,
the corresponding $k \times t$ submatrix has maximal rank t.

Let $L_l = V_l/GV_{l-m}$.

Then the map that evaluates polynomials
at the points of $\mathcal{Q}$ induces a surjective map

$$L_l \longrightarrow \mathbb{F}_q^t.$$

Denote the kernel by $L_l(\mathcal{Q})$,
it is the space of all functions $F \in V_l$
that are zero at the points of $\mathcal{Q}$ modulo GV_{l-m}.
So

$$\dim(L_l(\mathcal{Q})) = k - t \text{ if } t < d^{\perp}.$$

Conversely, the dimension of $L_l(\mathcal{Q})$ is at least $k - t$ for all t-subsets $\mathcal{Q}$ of $\mathcal{P}$.

But in order to get a bound for $d^\perp$, we have to know that $\dim(L_l(\mathcal{Q})) = k - t$ for all $t < d^\perp$.

The theory developed so far is not sufficient to get such a bound.

The theorem of **Riemann-Roch** gives an answer to this question.

Notice that the following inequality holds

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

where $g = (m-1)(m-2)/2$.

We will see that g is the **genus**.

Later g is also the **number of gaps** of
the **Weierstrass semigroup** of a point.