Basic Algebraic Geometry Codes

E. Martínez-Moro

Department of Applied Mathematics
University of Valladolid, Spain

edgar@maf.uva.es
http://www.singacom.uva.es/~edgar/

International School and Conference in Coding Theory
CIMAT, Guanajuato, 2008-11-28
Outline

1. History
2. Affine space, projective space
3. Some classical codes
   - Generalized Reed-Solomon codes
   - Classical Goppa codes
   - Generalized Reed-Muller codes
4. Algebraic curves
   - Examples of curves
   - Degree of a point and intersection multiplicity
   - Bézout and Plücker
5. Algebraic Geometry codes
   - Rational functions
   - The vector space $L(D)$
   - Evaluation. Riemann-Roch. Geometric Reed Solomon codes
   - Generalized Reed-Solomon codes are AG codes
   - Differentials and Geometric Goppa Codes
6. Gilbert-Varshamov bound
   - Goppa codes meet GV bound
   - AG codes exceed GV bound
Main references


History


... algebraic curves ↔ algebraic function fields

Høholdt, van Lint, Pellikaan (1998) Algebraic geometry codes, in Handbook of Coding Theory, Elsevier, 871-961. Weight functions...

**History**


...  

... algebraic curves $\leftrightarrow$ algebraic function fields

**Høholdt, van Lint, Pellikaan (1998)** Algebraic geometry codes, in Handbook of Coding Theory, Elsevier, 871-961. Weight functions...

**Martínez, Munuera, Ruano Eds. (2008)** Advances in Algebraic Geometry Codes. World Scientific.

... 


... algebraic curves $\leftrightarrow$ algebraic function fields

Høholdt, van Lint, Pellikaan (1998) Algebraic geometry codes, in Handbook of Coding Theory, Elsevier, 871-961. Weight functions...

History

- ... 
- ... algebraic curves ↔ algebraic function fields
  - **Høholdt, van Lint, Pellikaan (1998)** Algebraic geometry codes, in Handbook of Coding Theory, Elsevier, 871-961. **Weight functions**
  - **Martínez, Munuera, Ruano Eds. (2008)** Advances in Algebraic Geometry Codes. World Scientific.
History


... 

... algebraic curves $\leftrightarrow$ algebraic function fields

Høholdt, van Lint, Pellikaan (1998) Algebraic geometry codes, in Handbook of Coding Theory, Elsevier, 871-961. Weight functions...

Affine space, projective space

Algebraic Geometry codes are defined w.r.t. curves in the affine and projective space. Let \( F \) be a field, the \( n \)-dimensional affine space \( \mathbb{A}^n(F) \) over \( F \) is just the vector space \( F^n \)

\[
\mathbb{A}^n(F) = \{ (x_1, x_2, \ldots, x_n) \mid x_i \in F \}.
\]

Let \( x, x' \) be two elements in \( F^{n+1} \setminus \{0\} \), they are equivalent \( x \equiv x' \) if there is a \( \lambda \in F \) such that \( x = \lambda x' \). The \( n \)-dimensional projective space \( \mathbb{P}^n(F) \) over \( F \) is

\[
\mathbb{P}^n(F) = F^{n+1} / \equiv.
\]
Algebraic Geometry codes are defined w.r.t. curves in the affine and projective space. Let \( \mathbb{F} \) be a field, the \( n \)-dimensional affine space \( \mathbb{A}^n(\mathbb{F}) \) over \( \mathbb{F} \) is just the vector space \( \mathbb{F}^n \)

\[
\mathbb{A}^n(\mathbb{F}) = \{ (x_1, x_2, \ldots, x_n) | x_i \in \mathbb{F} \}.
\]

Let \( x, x' \) be two elements in \( \mathbb{F}^{n+1} \setminus \{0\} \), they are equivalent \( x \equiv x' \) if there is a \( \lambda \in \mathbb{F} \) such that \( x = \lambda x' \). The \( n \)-dimensional projective space \( \mathbb{P}^n(\mathbb{F}) \) over \( \mathbb{F} \) is

\[
\mathbb{P}^n(\mathbb{F}) = \mathbb{F}^{n+1} / \equiv.
\]
The equivalence class (projective point) containing \( x = (x_1, x_2, \ldots, x_{n+1}) \) will be denoted by \( x = (x_1 : x_2 : \ldots : x_{n+1}) \) (homogeneous coordinates). Thus projective points are 1 dimensional subspaces of \( \mathbb{A}^{n+1}(\mathbb{F}) \).

If \( P \in \mathbb{P}^n(\mathbb{F}) \) and \( P = (x_1 : x_2 : \ldots : x_{n+1} = 0) \) then it is called point at infinity, those points not at infinity are called affine points and each of them can be uniquely represented as \( P = (x_1 : x_2 : \ldots : x_{n+1} = 1) \).

Any point at infinity can be uniquely represented as with a 1 at its right-most non-zero position \( P = (x_1 : x_2 : \ldots : x_i = 1 : 0 : \ldots : 0) \).
Affine space, projective space

Projective points

The equivalence class (projective point) containing \( x = (x_1, x_2, \ldots, x_{n+1}) \) will be denoted by \( x = (x_1 : x_2 : \ldots : x_{n+1}) \) (homogeneous coordinates). Thus projective points are 1 dimensional subspaces of \( \mathbb{A}^{n+1}(\mathbb{F}) \).

If \( P \in \mathbb{P}^n(\mathbb{F}) \) and \( P = (x_1 : x_2 : \ldots : x_{n+1} = 0) \) then it is called point at infinity, those points not at infinity are called affine points and each of them can be uniquely represented as \( P = (x_1 : x_2 : \ldots : x_{n+1} = 1) \).

Any point at infinity can be uniquely represented as with a 1 at its right-most non-zero position \( P = (x_1 : x_2 : \ldots : x_i = 1 : 0 : \ldots : 0) \).
Affine space, projective space

Projective points

The equivalence class (projective point) containing \( x = (x_1, x_2, \ldots, x_{n+1}) \) will be denoted by \( x = (x_1 : x_2 : \ldots : x_{n+1}) \) (homogeneous coordinates). Thus projective points are 1 dimensional subspaces of \( \mathbb{A}^{n+1}(\mathbb{F}) \).

If \( P \in \mathbb{P}^n(\mathbb{F}) \) and \( P = (x_1 : x_2 : \ldots : x_{n+1} = 0) \) then it is called point at infinity, those points not at infinity are called affine points and each of them can be uniquely represented as \( P = (x_1 : x_2 : \ldots : x_{n+1} = 1) \).

Any point at infinity can be uniquely represented as with a 1 at its right-most non-zero position \( P = (x_1 : x_2 : \ldots : x_i = 1 : 0 : \ldots : 0) \).
Exercise

Let $F = F_q$, prove that

- $\mathbb{P}^n(F)$ contains $\sum_{i=0}^{n} q^i$ points.
- $\mathbb{P}^n(F)$ contains $\sum_{i=0}^{n-1} q^i$ points at infinity.

Note: Please, try even the trivial exercises.
Exercise

Let $\mathbb{F} = \mathbb{F}_q$, prove that

- $\mathbb{P}^n(\mathbb{F})$ contains $\sum_{i=0}^{n} q^i$ points.
- $\mathbb{P}^n(\mathbb{F})$ contains $\sum_{i=0}^{n-1} q^i$ points at infinity.

Note: Please, try even the trivial exercises.
Let \( \mathbb{F}[x_1, x_2, \ldots, x_n] \) be the set of polynomials with coefficients from \( \mathbb{F} \). A polynomial \( f \in \mathbb{F}[x_1, x_2, \ldots, x_n] \) is homogeneous of degree \( d \) if every term of \( f \) is of degree \( d \).

If \( f \in \mathbb{F}[x_1, x_2, \ldots, x_n] \) is not homogeneous and \( f \) has maximum degree \( d \) we can homogenize it adding a variable as follows

\[
f^H(x_1, x_2, \ldots, x_n, x_{n+1}) = x_{n+1}^d f \left( \frac{x_1}{x_{n+1}}, \frac{x_2}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}} \right).
\]
Affine space, projective space

Homogenization

Let \( \mathbb{F}[x_1, x_2, \ldots, x_n] \) be the set of polynomials with coefficients from \( \mathbb{F} \). A polynomial \( f \in \mathbb{F}[x_1, x_2, \ldots, x_n] \) is homogeneous of degree \( d \) if every term of \( f \) is of degree \( d \).

If \( f \in \mathbb{F}[x_1, x_2, \ldots, x_n] \) is not homogeneous and \( f \) has maximum degree \( d \) we can homogenize it adding a variable as follows

\[
f^H(x_1, x_2, \ldots, x_n, x_{n+1}) = x_{n+1}^d f \left( \frac{x_1}{x_{n+1}}, \frac{x_2}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}} \right).
\]
Affine space, projective space
Homogenization

Clearly \( f^H(x_1, x_2, \ldots, x_n, 1) = f(x_1, x_2, \ldots, x_n) \). Moreover, if we start with and homogeneous polynomial 
\( g(x_1, x_2, \ldots, x_n, x_{n+1}) \) of degree \( d \),

\[ g(x_1, x_2, \ldots, x_n, 1) = f(x_1, x_2, \ldots, x_n), \]

then \( f \) has degree \( k \leq d \) and 
\( g = x_{n+1}^{d-k} f^H. \)

Thus there is a one-to-one correspondence between polynomials in \( n \) variables of degree \( d \) or less and homogeneous polynomials of degree \( d \) in \( n + 1 \) variables.
Affine space, projective space
Homogenization

Clearly \( f^H(x_1, x_2, \ldots, x_n, 1) = f(x_1, x_2, \ldots, x_n) \). Moreover, if we start with and homogeneous polynomial \( g(x_1, x_2, \ldots, x_n, x_{n+1}) \) of degree \( d \),

\[
g(x_1, x_2, \ldots, x_n, 1) = f(x_1, x_2, \ldots, x_n),
\]

then \( f \) has degree \( k \leq d \) and \( g = x_{n+1}^{d-k} f^H \).

Thus there is a one-to-one correspondence between polynomials in \( n \) variables of degree \( d \) or less and homogeneous polynomials of degree \( d \) in \( n + 1 \) variables.
Affine space, projective space

Homogenization

Theorem

Let $g(x_1, x_2, \ldots, x_n, x_{n+1})$ be an homogeneous polynomial of degree $d$ over $\mathbb{F}$.

1. If $\alpha \in \mathbb{F}$ then $g(\alpha x_1, \alpha x_2, \ldots, \alpha x_n, \alpha x_{n+1}) = \alpha^d g(x_1, x_2, \ldots, x_n, x_{n+1})$.

2. $f(x_1, \ldots, x_n) = 0$ if and only if $f^H(x_1, \ldots, x_n, 1) = 0$.

3. If $(x_1 : x_2 : \ldots : x_{n+1}) = (x'_1 : x'_2 : \ldots : x'_{n+1})$ then $g(x_1, \ldots, x_n, x_{n+1}) = 0$ iff $g(x'_1, \ldots, x'_n, x'_{n+1}) = 0$. 

AG codes

E. Martínez-Moro

History

$A^n(\mathbb{F}), P^n(\mathbb{F})$

Classical codes

Generalized RS

Goppa

Reed-Muller

Curves

Examples

Degree & multiplicity

Bézout and Plücker

AG codes

Rational functions

$L(D)$

Evaluation

GRS are AG

Differentials and dual

GV bound

Goppa meet

AG exceed
Theorem above implies that the zeros of $f$ in $\mathbb{A}^n(\mathbb{F})$ correspond precisely to affine points in $\mathbb{P}^n(\mathbb{F})$ that are zeros of $f^H$ and the concept of a point of $\mathbb{P}^n(\mathbb{F})$ being a zero of a homogeneous polynomial is well defined.
Some classical codes
Generalized Reed-Solomon codes

For $k \geq 0$ let $\mathcal{P}_k \subset \mathbb{F}_q[x]$ be the set of all polynomials of degree less than $k$. Let $\alpha$ be a primitive $n$-th root of unity in $\mathbb{F}_q$ ($n = q - 1$), then the code

$$
\mathcal{C} = \{(f(1), f(\alpha), \ldots, f(\alpha^{q-2})) \mid f \in \mathcal{P}_k\}
$$

is the narrow-sense $[n, k, n - k + 1]$ RS code over $\mathbb{F}_q$.

RS codes are BCH codes

$\mathcal{C}$ can be extended to a $[n + 1, k, n - k + 2]$ code given by

$$
\hat{\mathcal{C}} = \{(f(1), f(\alpha), \ldots, f(\alpha^{q-2}), f(0)) \mid f \in \mathcal{P}_k\}
$$
Some classical codes
Generalized Reed-Solomon codes

For \( k \geq 0 \) let \( \mathcal{P}_k \subset \mathbb{F}_q[x] \) be the set of all polynomials of degree less than \( k \). Let \( \alpha \) be a primitive \( n \)-th root of unity in \( \mathbb{F}_q \) (\( n = q - 1 \)), then the code

\[
C = \{(f(1), f(\alpha), \ldots, f(\alpha^{q-2})) \mid f \in \mathcal{P}_k\}
\]

is the narrow-sense \([n, k, n - k + 1]\) RS code over \( \mathbb{F}_q \).

RS codes are BCH codes

\( C \) can be extended to a \([n+1, k, n - k + 2]\) code given by

\[
\hat{C} = \{(f(1), f(\alpha), \ldots, f(\alpha^{q-2}), f(0)) \mid f \in \mathcal{P}_k\}
\]
Some classical codes
Generalized Reed-Solomon codes

For $k \geq 0$ let $\mathcal{P}_k \subset \mathbb{F}_q[x]$ be the set of all polynomials of degree less than $k$. Let $\alpha$ be a primitive $n$-th root of unity in $\mathbb{F}_q$ ($n = q - 1$), then the code

$$\mathcal{C} = \{(f(1), f(\alpha), \ldots, f(\alpha^{q-2})) \mid f \in \mathcal{P}_k\}$$

(1)

is the narrow-sense $[n, k, n - k + 1]$ RS code over $\mathbb{F}_q$.

RS codes are BCH codes

$\mathcal{C}$ can be extended to a $[n + 1, k, n - k + 2]$ code given by

$$\hat{\mathcal{C}} = \{(f(1), f(\alpha), \ldots, f(\alpha^{q-2}), f(0)) \mid f \in \mathcal{P}_k\}$$

(2)
Some classical codes
Generalized Reed-Solomon codes

Exercise

Show that if \( f \in \mathcal{P}_k \) with \( k < q \) then
\[
\sum_{\beta \in \mathbb{F}_q} f(\beta) = 0.
\]

Clue: \( q > 2 \sum_{\beta \in \mathbb{F}_q} \beta = 0. \)

Thus \( \hat{C} \) results from adding an overall parity check to a RS code and the minimum weight increases.
Some classical codes
Generalized Reed-Solomon codes

Exercise

Show that if $f \in \mathcal{P}_k$ with $k < q$ then

$$\sum_{\beta \in \mathbb{F}_q} f(\beta) = 0.$$ 

Clue: $q > 2 \sum_{\beta \in \mathbb{F}_q} \beta = 0$.

Thus $\hat{C}$ results from adding an overall parity check to a RS code and the minimum weight increases.
Some classical codes
Generalized Reed-Solomon codes

Let $n$ be an integer $1 \leq n \leq q$, and $\gamma = (\gamma_0, \ldots, \gamma_{n-1})$ a $n$-tuple of distinct elements of $\mathbb{F}_q$, and $\mathbf{v} = (v_0, \ldots, v_{n-1})$ a $n$-tuple of non-zero elements of $\mathbb{F}_q^*$. Let $k$ be an integer $1 \leq k \leq n$, then

$$GRS_k(\gamma, \mathbf{v}) = \{(v_0 f(\gamma_0), \ldots, v_{n-1} f(\gamma_{n-1})) \mid f \in \mathcal{P}_k\}$$

are the Generalized Reed-Solomon codes over $\mathbb{F}_q$.

GRS codes are $[n, k, n-k+1]$ MDS codes.

Note that both, the narrow sense RS code and the extended RS code can be seen as Generalized Reed-Solomon codes.
Some classical codes
Generalized Reed-Solomon codes

Let $n$ be an integer $1 \leq n \leq q$, and $\gamma = (\gamma_0, \ldots, \gamma_{n-1})$ a $n$-tuple of distinct elements of $\mathbb{F}_q$, and $\mathbf{v} = (v_0, \ldots, v_{n-1})$ a $n$-tuple of non-zero elements of $\mathbb{F}_q^*$. Let $k$ be an integer $1 \leq k \leq n$, then

$$G\text{RS}_k(\gamma, \mathbf{v}) = \{(v_0 f(\gamma_0), \ldots, v_{n-1} f(\gamma_{n-1})) \mid f \in \mathcal{P}_k\} \quad (3)$$

are the Generalized Reed-Solomon codes over $\mathbb{F}_q$.

GRS codes are $[n, k, n - k + 1]$ MDS codes

Note that both, the narrow sense RS code and the extended RS code can be seen as Generalized Reed-Solomon codes.
Let $n$ be an integer $1 \leq n \leq q$, and $\gamma = (\gamma_0, \ldots, \gamma_{n-1})$ a $n$-tuple of distinct elements of $\mathbb{F}_q$, and $\mathbf{v} = (v_0, \ldots, v_{n-1})$ a $n$-tuple of non-zero elements of $\mathbb{F}_q^*$. Let $k$ be an integer $1 \leq k \leq n$, then

$$GRS_k(\gamma, \mathbf{v}) = \{(v_0 f(\gamma_0), \ldots, v_{n-1} f(\gamma_{n-1})) \mid f \in \mathcal{P}_k\} \quad (3)$$

are the Generalized Reed-Solomon codes over $\mathbb{F}_q$.

GRS codes are $[n, k, n - k + 1]$ MDS codes

Note that both, the narrow sense RS code and the extended RS code can be seen as Generalized Reed-Solomon codes.
Some classical codes
Generalized Reed-Solomon codes

Since there is a one-to-one correspondence between $\mathcal{L}_{k-1}$ the homogeneous polynomials in two variables of degree $k-1$ and the non-zero polynomials of $\mathcal{P}_k$, let $P_i = (\gamma_i : 1) \in \mathbb{P}^1(\mathbb{F}_q)$, we can redefine the code $\mathcal{GRS}_k(\gamma, v)$ as follows

$$\{(v_0g(P_0), \ldots, v_{n-1}g(P_{n-1})) \mid g \in \mathcal{L}_{k-1}\}.$$  (4)
Some classical codes
Goppa codes and BCH codes

Let \( t = \text{ord}_q(n) \) and \( \beta \) a primitive \( n \)-th root of unity in \( \mathbb{F}_{q^t} \). Choose \( \delta > 1 \) and let \( C \) the narrow sense BCH code of length \( n \) and designed distance \( \delta \), i.e.

\[
c(x) \in \mathbb{F}[x]/(x^n - 1) \text{ is in } C \iff c(\beta^j) = 0, \quad 1 \leq j \leq \delta - 1.
\]

Note that

\[
(x^n - 1) \sum_{i=0}^{n-1} \frac{c_i}{x - \beta^{-i}} = \sum_{i=0}^{n-1} c_i \sum_{l=0}^{n-1} x^l (\beta^{-i})^{n-1-l} = \sum_{l=0}^{n-1} x^l \sum_{i=0}^{n-1} c_i (\beta^{l+1})^i. \tag{5}
\]
Let $t = \text{ord}_q(n)$ and $\beta$ a primitive $n$-th root of unity in $\mathbb{F}_{q^t}$. Choose $\delta > 1$ and let $C$ the narrow sense BCH code of length $n$ and designed distance $\delta$, i.e.

$$c(x) \in \mathbb{F}[x]/(x^n - 1)$$

is in $C \iff c(\beta^j) = 0, \quad 1 \leq j \leq \delta - 1.$

Note that

$$\left(x^n - 1\right) \sum_{i=0}^{n-1} \frac{c_i}{x - \beta^{-i}} = \sum_{i=0}^{n-1} c_i \sum_{l=0}^{n-1} x^l (\beta^{-i})^{n-1-l}$$

$$= \sum_{l=0}^{n-1} x^l \sum_{i=0}^{n-1} c_i (\beta^{l+1})^i. \quad (5)$$
Some classical codes
Goppa codes and BCH codes

Let \( t = \text{ord}_q(n) \) and \( \beta \) a primitive \( n \)-th root of unity in \( \mathbb{F}_{q^t} \).
Choose \( \delta > 1 \) and let \( C \) the narrow sense BCH code of length \( n \) and designed distance \( \delta \), i.e.

\[ c(x) \in \mathbb{F}[x]/(x^n - 1) \text{ is in } C \iff c(\beta^j) = 0, \quad 1 \leq j \leq \delta - 1. \]

Note that

\[
(x^n - 1) \sum_{i=0}^{n-1} \frac{c_i}{x - \beta^{-i}} = \sum_{i=0}^{n-1} c_i \sum_{l=0}^{n-1} x^l (\beta^{-i})^{n-1-l} = \sum_{l=0}^{n-1} x^l \sum_{i=0}^{n-1} c_i (\beta^l+1)^i.
\]
Let \( t = \text{ord}_q(n) \) and \( \beta \) a primitive \( n \)-th root of unity in \( \mathbb{F}_{q^t} \). Choose \( \delta > 1 \) and let \( C \) the narrow sense BCH code of length \( n \) and designed distance \( \delta \), i.e.

\[
\text{c}(x) \in \mathbb{F}[x]/(x^n - 1) \text{ is in } C \iff \text{c}(\beta^j) = 0, \quad 1 \leq j \leq \delta - 1.
\]

Note that

\[
(x^n - 1) \sum_{i=0}^{n-1} \frac{c_i}{x - \beta^{-i}} = \sum_{i=0}^{n-1} c_i \sum_{l=0}^{n-1} x^l (\beta^{-i})^{n-1-l} = \sum_{l=0}^{n-1} x^l \sum_{i=0}^{n-1} c_i (\beta^l + 1)^i.
\]
Because \( c(\beta^l) = 0, \quad 1 \leq l \leq \delta - 2 \), LHS in (5) is a polynomial with lowest degree term at least \( \delta - 1 \), thus RHS can be written as \( p(x)x^{\delta - 1} \) with \( p(x) \in \mathbb{F}_{q^t}[x] \).

\[
\begin{align*}
  c(x) \in C & \iff \sum_{i=0}^{n-1} \frac{c_i}{x - \beta^{-i}} = \frac{p(x)x^{\delta - 1}}{x^n - 1} \\
  & \iff \sum_{i=0}^{n-1} \frac{c_i}{x - \beta^{-i}} \equiv 0 \mod x^{\delta - 1}. \quad (6)
\end{align*}
\]

This equivalence means that if the LHS is written as a rational function \( \frac{a(x)}{b(x)} \) then the numerator \( a(x) \) will be a multiple of \( x^{\delta - 1} \) (\( b(x) = x^n - 1 \)).
Because \( c(\beta^l) = 0, \ 1 \leq l \leq \delta - 2 \), LHS in (5) is a polynomial with lowest degree term at least \( \delta - 1 \), thus RHS can be written as \( p(x)x^{\delta - 1} \) with \( p(x) \in \mathbb{F}_q[t][x] \).

\[
c(x) \in C \iff \sum_{i=0}^{n-1} \frac{c_i}{x - \beta^{-i}} = \frac{p(x)x^{\delta - 1}}{x^n - 1}
\]

\[
\iff \sum_{i=0}^{n-1} \frac{c_i}{x - \beta^{-i}} \equiv 0 \mod x^{\delta - 1}.
\] (6)

This equivalence means that if the LHS is written as a rational function \( \frac{a(x)}{b(x)} \), then the numerator \( a(x) \) will be a multiple of \( x^{\delta - 1} \) (\( b(x) = x^n - 1 \)).
Some classical codes
Goppa codes and BCH codes

Because $c(\beta^l) = 0$, $1 \leq l \leq \delta - 2$, LHS in (5) is a polynomial with lowest degree term at least $\delta - 1$, thus RHS can be written as $p(x)x^{\delta-1}$ with $p(x) \in \mathbb{F}_q[t][x]$.

\[ c(x) \in C \iff \sum_{i=0}^{n-1} \frac{c_i}{x - \beta^{-i}} = \frac{p(x)x^{\delta-1}}{x^n - 1} \]

\[ \iff \sum_{i=0}^{n-1} \frac{c_i}{x - \beta^{-i}} \equiv 0 \mod x^{\delta-1}. \]

This equivalence means that if the LHS is written as a rational function $\frac{a(x)}{b(x)}$ then the numerator $a(x)$ will be a multiple of $x^{\delta-1}$ ($b(x) = x^n - 1$).
Some classical codes
Goppa codes and BCH codes

Because $c(\beta^l) = 0$, $1 \leq l \leq \delta - 2$, LHS in (5) is a polynomial with lowest degree term at least $\delta - 1$, thus RHS can be written as $p(x)x^{\delta - 1}$ with $p(x) \in \mathbb{F}_{q^t}[x]$.

$$
c(x) \in C \iff \sum_{i=0}^{n-1} \frac{c_i}{x - \beta^{-i}} = \frac{p(x)x^{\delta - 1}}{x^n - 1}
\iff \sum_{i=0}^{n-1} \frac{c_i}{x - \beta^{-i}} \equiv 0 \mod x^{\delta - 1}. \quad (6)
$$

This equivalence means that if the LHS is written as a rational function $\frac{a(x)}{b(x)}$ then the numerator $a(x)$ will be a multiple of $x^{\delta - 1}$ ($b(x) = x^n - 1$).
Because \( c(\beta^l) = 0, \quad 1 \leq l \leq \delta - 2 \), LHS in (5) is a polynomial with lowest degree term at least \( \delta - 1 \), thus RHS can be written as \( p(x)x^{\delta - 1} \) with \( p(x) \in \mathbb{F}_{q^t}[x] \).

\[
\begin{align*}
c(x) \in C \iff & \sum_{i=0}^{n-1} \frac{c_i}{x - \beta^{-i}} = \frac{p(x)x^{\delta - 1}}{x^n - 1} \\
\iff & \sum_{i=0}^{n-1} \frac{c_i}{x - \beta^{-i}} \equiv 0 \mod x^{\delta - 1}.
\end{align*}
\]

This equivalence means that if the LHS is written as a rational function \( \frac{a(x)}{b(x)} \) then the numerator \( a(x) \) will be a multiple of \( x^{\delta - 1} \) \( (b(x) = x^n - 1) \).
Following the discussion above, fix an extension $\mathbb{F}_{q^t}$ of $\mathbb{F}_q$ ($t = \text{ord}_q(n)$ no longer needed). Let

$$L = \{\gamma_0, \gamma_1, \ldots, \gamma_{n-1}\} \subset \mathbb{F}_{q^t}$$

and let $G(x) \in \mathbb{F}_{q^t}[x]$ with $G(\gamma_i) \neq 0$ where $\gamma_i \in L$.

The Goppa code $\Gamma(L, G)$ is the set of vectors $(c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ such that

$$\sum_{i=0}^{n-1} \frac{c_i}{x - \gamma_i} \equiv 0 \mod G(x). \quad (7)$$
Following the discussion above, fix an extension \( \mathbb{F}_{q^t} \) of \( \mathbb{F}_q \) 
\((t = \text{ord}_q(n) \text{ no longer needed}).\) Let

\[
L = \{ \gamma_0, \gamma_1, \ldots, \gamma_{n-1} \} \subset \mathbb{F}_{q^t}
\]

and let \( G(x) \in \mathbb{F}_{q^t}[x] \) with \( G(\gamma_i) \neq 0 \) where \( \gamma_i \in L. \)

The **Goppa code** \( \Gamma(L, G) \) is the set of vectors \( (c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n \) such that

\[
\sum_{i=0}^{n-1} \frac{c_i}{x - \gamma_i} \equiv 0 \mod G(x). \quad (7)
\]
Some classical codes
Goppa codes

This again means that if the LHS is written as a rational function then the numerator is a multiple of \( G(x) \) the Goppa polynomial. Note that \( G(\gamma_i) \neq 0 \) guarantees that \( x - \gamma_i \) is invertible in \( \mathbb{F}_{q^t}[x]/(G(x)) \).
Some classical codes
Goppa codes. Parity check matrix.

Since

$$\frac{1}{x - \gamma_i} \equiv - \frac{1}{G(\gamma_i)} \frac{G(x) - G(\gamma_i)}{x - \gamma_i} \mod G(x) \quad (8)$$

Substituting in eqn. (7) we have \((c_0, \ldots, c_{n-1}) \in \Gamma(L, G)\) iff

$$\sum_{i=0}^{n-1} c_i \frac{G(x) - G(\gamma_i)}{x - \gamma_i} G(\gamma_i)^{-1} \equiv 0 \mod G(x) \quad (9)$$
Some classical codes
Goppa codes. Parity check matrix.

Since

$$\frac{1}{x - \gamma_i} \equiv -\frac{1}{G(\gamma_i)} \frac{G(x) - G(\gamma_i)}{x - \gamma_i} \pmod{G(x)} \quad (8)$$

Substituting in eqn. (7) we have \((c_0, \ldots, c_{n-1}) \in \Gamma(L, G)\) iff

$$\sum_{i=0}^{n-1} c_i \frac{G(x) - G(\gamma_i)}{x - \gamma_i} G(\gamma_i)^{-1} \equiv 0 \pmod{G(x)} \quad (9)$$
Some classical codes
Goppa codes. Parity check matrix.

Suppose \( \deg G(x) = w \) and

\[
G(x) = \sum_{j=0}^{w} g_j x^j, \quad g_j \in \mathbb{F}_{q^t}.
\]

\[
\frac{G(x) - G(\gamma_i)}{x - \gamma_i} G(\gamma_i)^{-1} = G(\gamma_i)^{-1} \sum_{j=0}^{w} g_j \sum_{k=0}^{j-1} x^k \gamma_i^{j-1-k}
\]

\[
= G(\gamma_i)^{-1} \sum_{k=0}^{w} x^k \left( \sum_{j=k+1}^{w} g_j \gamma_i^{j-1-k} \right).
\]

(10)
Suppose $\deg G(x) = w$ and

$$G(x) = \sum_{j=0}^{w} g_j x^j, \quad g_j \in \mathbb{F}_{q^t}.$$ 

Then

$$\frac{G(x) - G(\gamma_i)}{x - \gamma_i} G(\gamma_i)^{-1} = G(\gamma_i)^{-1} \sum_{j=0}^{w} g_j \sum_{k=0}^{j-1} x^k \gamma_i^{j-1-k}$$

$$= G(\gamma_i)^{-1} \sum_{k=0}^{w} x^k \left( \sum_{j=k+1}^{w} g_j \gamma_i^{j-1-k} \right).$$

(10)
Some classical codes
Goppa codes. Parity check matrix.

Suppose deg $G(x) = w$ and

$$G(x) = \sum_{j=0}^{w} g_j x^j, \quad g_j \in \mathbb{F}_{q^t}.$$

$$\frac{G(x) - G(\gamma_i)}{x - \gamma_i} G(\gamma_i)^{-1} = G(\gamma_i)^{-1} \sum_{j=0}^{w} g_j \sum_{k=0}^{j-1} x^k \gamma_i^{j-1-k}$$

$$= G(\gamma_i)^{-1} \sum_{k=0}^{w} x^k \left( \sum_{j=k+1}^{w} g_j \gamma_i^{j-1-k} \right).$$

(10)
Some classical codes
Goppa codes. Parity check matrix.

From (9) setting the coefficients of $x^k$ to 0 in the order $k = w - 1, w - 2, \ldots, 0$ we have that $c \in \Gamma(L, G)$ if $Hc^T = 0$, where $H$ is

$$
\begin{pmatrix}
  h_0 g_w & \cdots & h_{n-1} g_w \\
  h_0 (g_{w-1} + g_w \gamma_0) & \cdots & h_{n-1} (g_{w-1} + g_w \gamma_{n-1}) \\
  \vdots & \vdots & \vdots \\
  h_0 \sum_{j=1}^w g_j \gamma_0^{j-1} & \cdots & h_{n-1} \sum_{j=1}^w g_j \gamma_{n-1}^{j-1}
\end{pmatrix}
$$

(11)

with $h_i = G(\gamma_i)^{-1}$. 
Some classical codes
Goppa codes. Parity check matrix.

\[ H \text{ can be reduced to the matrix } H' \]

\[
\begin{pmatrix}
G(\gamma_0)^{-1} & \ldots & G(\gamma_{n-1})^{-1} \\
G(\gamma_0)^{-1} \gamma_0 & \ldots & G(\gamma_{n-1})^{-1} \gamma_{n-1} \\
\vdots & \vdots & \vdots \\
G(\gamma_0)^{-1} \gamma_0^{w-1} & \ldots & G(\gamma_{n-1})^{-1} \gamma_{n-1}^{w} \\
\end{pmatrix}
\] (12)
Some classical codes
Goppa code as a subfield subcode of a GRS code

Note that the parity check matrix $H'$ is the generator matrix of the $GRS_w(\gamma, v)$ over $\mathbb{F}_{q^t}$ where $v = (G(\gamma_0)^{-1}, \ldots, G(\gamma_{n-1})^{-1})$, i.e. we have that

$$\Gamma(L, G) = GRS_w(\gamma, v)^\perp|_{\mathbb{F}_q}.$$ 

Since $GRS_w(\gamma, v)^\perp$ is also a GRS code then classical Goppa codes are subfield subcodes of GRS codes.
Some classical codes
Goppa code as a subfield subcode of a GRS code

Theorem

The Goppa code $\Gamma(L, G)$ with $\deg(G(x)) = w$ is an $[n, k, d]$ code where $k \geq n - wt$ and $d \geq w + 1$. 
Some classical codes
Goppa code as a subfield subcode of a GRS code

Proof.

The entries of $H'$ are in $\mathbb{F}_{q^t}$. By choosing a base of $\mathbb{F}_{q^t} \mid \mathbb{F}_q$ each element of $\mathbb{F}_{q^t}$ can be represented by a $t \times 1$ column vector, and if we replace each entry in $H'$ by the corresponding vector we get a matrix $H''$ with entries in $\mathbb{F}_q$ such that $H''c^T = 0$, $c \in \Gamma(L, G)$.

The rows of $H''$ may be independent thus $k \geq n - \text{wt}$. If $0 \neq c \in \Gamma(L, G)$ has weight $\leq w$ then when the LHS of (7) is written as a rational function the numerator has degree $\leq w - 1$, but it has to be a multiple of $G(x)$, which contradicts the fact $\deg(G(x)) = w$. 

---
Some classical codes
Goppa code as a subfield subcode of a GRS code

Proof.

The entries of $H'$ are in $\mathbb{F}_{q^t}$. By choosing a base of $\mathbb{F}_{q^t}|\mathbb{F}_q$ each element of $\mathbb{F}_{q^t}$ can be represented by a $t \times 1$ column vector, and if we replace each entry in $H'$ by the corresponding vector we get a matrix $H''$ with entries in $\mathbb{F}_q$ such that $H''c^T = 0$, $c \in \Gamma(L, G)$.

The rows of $H''$ may be independent thus $k \geq n - \text{wt}$. If $0 \neq c \in \Gamma(L, G)$ has weight $\leq w$ then when the LHS of (7) is written as a rational function the numerator has degree $\leq w-1$, but it has to be a multiple of $G(x)$, which contradicts the fact $\deg(G(x)) = w$. 

∪ Up to here the first session (28/11)
Some classical codes
Goppa code as a subfield subcode of a GRS code

Proof.
The entries of $H'$ are in $\mathbb{F}_{q^t}$. By choosing a base of $\mathbb{F}_{q^t} | \mathbb{F}_q$ each element of $\mathbb{F}_{q^t}$ can be represented by a $t \times 1$ column vector, and if we replace each entry in $H'$ by the corresponding vector we get a matrix $H''$ with entries in $\mathbb{F}_q$ such that $H'' \mathbf{c}^T = \mathbf{0}$, $\mathbf{c} \in \Gamma(L, G)$.
The rows of $H''$ may be independent thus $k \geq n - wt$. If $\mathbf{0} \neq \mathbf{c} \in \Gamma(L, G)$ has weight $\leq w$ then when the LHS of (7) is written as a rational function the numerator has degree $\leq w - 1$, but it has to be a multiple of $G(x)$, which contradicts the fact $\deg(G(x)) = w$. 

\[ \square \]
Some classical codes
Goppa code. Another formulation: residues.

Let \( \mathcal{R} \) be the vector space of all the rational functions \( f \) with coefficients in \( \mathbb{F}_{q^t} \) such that

1. \( f = \frac{a(x)}{b(x)} \) where \( a, b \) are relatively prime.

2. The zeros of \( a(x) \) include the zeros of \( G(x) \) with at least the same multiplicity.

3. The only possible poles of \( f \) (i.e. the zeros of \( b(x) \)) are \( \gamma_0, \gamma_1, \ldots, \gamma_{n-1} \) with multiplicity at most one.

\( f \in \mathcal{R} \) has a Laurent series expansion about \( \gamma_i \)

\[
 f = \sum_{j=-1}^{\infty} f_i (x - \gamma_i)^j
\]

where \( f_{-1} \neq 0 \) if \( f \) has a pole at \( \gamma_i \) or \( f_{-1} = 0 \) otherwise.
Some classical codes
Goppa code. Another formulation: residues.

Let $\mathcal{R}$ be the vector space of all the rational functions $f$ with coefficients in $\mathbb{F}_{q^t}$ such that

1. $f = \frac{a(x)}{b(x)}$ where $a, b$ are relatively prime.

2. The zeros of $a(x)$ include the zeros of $G(x)$ with at least the same multiplicity.

3. The only possible poles of $f$ (i.e. the zeros of $b(x)$) are $\gamma_0, \gamma_1, \ldots, \gamma_{n-1}$ with multiplicity at most one.

$f \in \mathcal{R}$ has a Laurent series expansion about $\gamma_i$

$$f = \sum_{j=-1}^{\infty} f_i(x - \gamma_i)^j \quad (13)$$

where $f_{-1} \neq 0$ if $f$ has a pole at $\gamma_i$ or $f_{-1} = 0$ otherwise.
Some classical codes
Goppa code. Another formulation: residues.

The **residue** of \( f(x) \) at \( \gamma_i \) denoted as \( \text{Res}_{\gamma_i} f \) is the coefficient \( f_{-1} \) above. Let

\[
C_{\text{Res}}(G, \gamma) = \{(\text{Res}_{\gamma_0} f, \ldots, \text{Res}_{\gamma_{n-1}} f) \mid f \in \mathcal{R}\}
\]  

(14)

**Exercise**

Show that \( C_{\text{Res}}(G, \gamma)|_{\mathbb{F}_q} = \Gamma(L, G) \).
Some classical codes
Goppa code. Another formulation: residues.

The residue of \( f(x) \) at \( \gamma_i \) denoted as \( \text{Res}_{\gamma_i} f \) is the coefficient \( f_{-1} \) above. Let

\[
C_{\text{Res}}(G, \gamma) = \{(\text{Res}_{\gamma_0} f, \ldots, \text{Res}_{\gamma_{n-1}} f) \mid f \in \mathcal{R}\}
\]  

(14)

Exercise

Show that \( C_{\text{Res}}(G, \gamma)|_{F_q} = \Gamma(L, G) \).
Some classical codes
Generalized Reed-Muller codes

Let $m > 0$, $n = q^m$ and $\{P_1, \ldots, P_n\} = \mathbb{A}^m(F_q)$. Let $0 \leq r \leq m(q - 1)$ and $F_q[x_1, \ldots, x_m]^r$ the set of polynomials of total degree $r$ or less.

The $r$-th order generalized Reed-Muller code of length $n = q^m$ is

$$R_q(r, m) = \{(f(P_1), \ldots, f(P_n)) \mid f \in F_q[x_1, \ldots, x_m]^r\} \quad (15)$$
Let $m > 0$, $n = q^m$ and $\{P_1, \ldots, P_n\} = \mathbb{A}^m(\mathbb{F}_q)$. Let $0 \leq r \leq m(q - 1)$ and $\mathbb{F}_q[x_1, \ldots, x_m]_r$ the set of polynomials of total degree $r$ or less.

The $r$-th order generalized Reed-Muller code of length $n = q^m$ is

$$R_q(r, m) = \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathbb{F}_q[x_1, \ldots, x_m]_r\} \quad (15)$$
Some classical codes
Generalized Reed-Muller codes

Note that since $\beta^q = \beta$ for all $\beta \in \mathbb{F}_q$ if we note $\mathbb{F}_q[x_1, \ldots, x_m]^*_r$ the set of polynomials of total degree $r$ or less with no variable with exponent $q$ or higher we have

$$\mathcal{R}_q(r, m) = \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathbb{F}_q[x_1, \ldots, x_m]^*_r\}$$

(16)

$F_q[x_1, \ldots, x_m]^*_r$ is a vector space with a basis

$$\mathcal{B} = \left\{x_1^{e_1} x_2^{e_2} \cdots x_m^{e_m} \mid 0 \leq e_i < q, \sum_{i=0}^{m} e_i \leq r \right\}$$
Some classical codes
Generalized Reed-Muller codes

Note that since $\beta^q = \beta$ for all $\beta \in \mathbb{F}_q$ if we note $\mathbb{F}_q[x_1, \ldots, x_m]_r^*$ the set of polynomials of total degree $r$ or less with no variable with exponent $q$ or higher we have

$$\mathcal{R}_q(r, m) = \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathbb{F}_q[x_1, \ldots, x_m]_r^*\}$$

(16)

$\mathbb{F}_q[x_1, \ldots, x_m]_r^*$ is a vector space with a basis

$$\mathcal{B} = \left\{x_1^{e_1}x_2^{e_2} \ldots x_m^{e_m} \mid 0 \leq e_i < q, \sum_{i=0}^{m} e_i \leq r\right\}$$
Some classical codes
Generalized Reed-Muller codes

Clearly, the words \( \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{B} \} \) span the code \( \mathcal{R}_q(r, m) \).

**Exercise**

Prove that \( \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{B} \} \) are independent.
An **affine plane curve** $\mathcal{X}$ is the set of affine points $(x, y) \in \mathbb{A}^2(\mathbb{F})$ denoted as $\mathcal{X}_f(\mathbb{F})$ such that $f(x, y) = 0$, $f \in \mathbb{F}[x, y]$.

A **projective plane curve** $\mathcal{X}$ is the set of projective points $(x : y : z) \in \mathbb{P}^2(\mathbb{F})$ denoted (also) as $\mathcal{X}_f(\mathbb{F})$ such that $f(x, y, z) = 0$, $f \in \mathbb{F}[x, y, z]$ an homogeneous polynomial.

If $f \in \mathbb{F}[x, y]$ then $\mathcal{X}_{fH}(\mathbb{F})$ is called the **projective closure of** $\mathcal{X}_f(\mathbb{F})$ (i.e. we add the possible points at infinity).
Algebraic curves

An affine plane curve $\mathcal{X}$ is the set of affine points $(x, y) \in \mathbb{A}^2(\mathbb{F})$ denoted as $\mathcal{X}_f(\mathbb{F})$ such that $f(x, y) = 0$, $f \in \mathbb{F}[x, y]$.

A projective plane curve $X$ is the set of projective points $(x : y : z) \in \mathbb{P}^2(\mathbb{F})$ denoted (also) as $\mathcal{X}_f(\mathbb{F})$ such that $f(x, y, z) = 0$, $f \in \mathbb{F}[x, y, z]$ an homogeneous polynomial.

If $f \in \mathbb{F}[x, y]$ then $\mathcal{X}_{fH}(\mathbb{F})$ is called the projective closure of $\mathcal{X}_f(\mathbb{F})$ (i.e. we add the possible points at infinity).
Algebraic curves

An **affine plane curve** $\mathcal{X}$ is the set of affine points $(x, y) \in \mathbb{A}^2(\mathbb{F})$ denoted as $\mathcal{X}_f(\mathbb{F})$ such that $f(x, y) = 0$, $f \in \mathbb{F}[x, y]$.

A **projective plane curve** $\mathcal{X}$ is the set of projective points $(x : y : z) \in \mathbb{P}^2(\mathbb{F})$ denoted (also) as $\mathcal{X}_f(\mathbb{F})$ such that $f(x, y, z) = 0$, $f \in \mathbb{F}[x, y, z]$ an homogeneous polynomial.

If $f \in \mathbb{F}[x, y]$ then $\mathcal{X}_{fH}(\mathbb{F})$ is called the **projective closure of** $\mathcal{X}_f(\mathbb{F})$ (i.e. we add the possible points at infinity).
Algebraic curves
Smooth curves

If \( f = \sum_{i,j} a_{ij} x^i y^j \in \mathbb{F}[x, y] \) the partial derivative \( f_x \) of \( f \) w.r.t. \( x \) is

\[
f_x = \frac{\partial f}{\partial x} = \sum_{i,j} i a_{ij} x^{i-1} y^j.
\]

The partial derivative \( f_y \) of \( f \) w.r.t. \( y \) is defined analogously.

A point \((x_0, y_0)\) of \( \mathcal{X}_f(\mathbb{F}) \) is singular if \( f_x(x_0, y_0) = f_y(x_0, y_0) = 0 \). A point of \( \mathcal{X}_f(\mathbb{F}) \) is nonsingular or simple if it is not singular.

A curve that has no singular point is called nonsingular, regular or smooth. Analogous definitions hold for projective curves.
Algebraic curves
Smooth curves

If \( f = \sum_{i,j} a_{ij} x^i y^j \in \mathbb{F}[x, y] \) the partial derivative \( f_x \) of \( f \) w.r.t. \( x \) is

\[
f_x = \frac{\partial f}{\partial x} = \sum_{i,j} i a_{ij} x^{i-1} y^j.
\]

The partial derivative \( f_y \) of \( f \) w.r.t. \( y \) is defined analogously.

A point \((x_0, y_0)\) of \( X_f(\mathbb{F}) \) is singular if \( f_x(x_0, y_0) = f_y(x_0, y_0) = 0 \). A point of \( X_f(\mathbb{F}) \) is nonsingular or simple if it is not singular.

A curve that has no singular point is called nonsingular, regular or smooth. Analogous definitions hold for projective curves.
The Fermat curve $F_m(\mathbb{F}_q)$ is a projective plane curve defined by

$$f(x, y, z) = x^m + y^m + z^m = 0.$$

$f_x = mx^{m-1}$, $f_y = my^{m-1}$, $f_z = mz^{m-1}$, thus it has no singular points if $\gcd(m, q) = 1$.

Exercise

- Find the three projective points of $F_3(\mathbb{F}_2)$.
- Find the nine projective points of $F_3(\mathbb{F}_4)$. 
The Fermat curve $\mathcal{F}_m(\mathbb{F}_q)$ is a projective plane curve defined by
\[
f(x, y, z) = x^m + y^m + z^m = 0.
\]

$f_x = mx^{m-1}$, $f_y = my^{m-1}$, $f_z = mz^{m-1}$, thus it has no singular points if $\gcd(m, q) = 1$.

**Exercise**

- Find the three projective points of $\mathcal{F}_3(\mathbb{F}_2)$.
- Find the nine projective points of $\mathcal{F}_3(\mathbb{F}_4)$. 
The Fermat curve $F_m(F_q)$ is a projective plane curve defined by

$$f(x, y, z) = x^m + y^m + z^m = 0.$$  

$f_x = mx^{m-1}$, $f_y = my^{m-1}$, $f_z = mz^{m-1}$, thus it has no singular points if $\gcd(m, q) = 1$.

**Exercise**

- Find the three projective points of $F_3(F_2)$.
- Find the nine projective points of $F_3(F_4)$. 

Algebraic curves
Example 2: Hermitian curve

Let $q = r^2$ where $r$ is a prime power. The Hermitian curve $\mathcal{H}_r(\mathbb{F}_q)$ is a projective plane curve defined by

$$f(x, y, z) = x^{r+1} - y^r z - yz^r = 0.$$ 

Since $r$ is a multiple of the characteristic then $\mathcal{H}_r(\mathbb{F}_q)$ is non-singular.

**Exercise**

- Show that $(0 : 1 : 0)$ is the only point at infinity of $\mathcal{H}_r(\mathbb{F}_q)$.
- Find the eight affine points $(x : y : 1)$ points of $\mathcal{H}_2(\mathbb{F}_4)$. 
Let $q = r^2$ where $r$ is a prime power. The **Hermitian curve** $\mathcal{H}_r(\mathbb{F}_q)$ is a projective plane curve defined by

$$f(x, y, z) = x^{r+1} - y'z - yz' = 0.$$ 

Since $r$ is a multiple of the characteristic then $\mathcal{H}_r(\mathbb{F}_q)$ is non-singular.

**Exercise**

- Show that $(0 : 1 : 0)$ is the only point at infinity of $\mathcal{H}_r(\mathbb{F}_q)$.
- Find the eight affine points $(x : y : 1)$ points of $\mathcal{H}_2(\mathbb{F}_4)$. 
Algebraic curves
Example 2: Hermitian curve

Let \( q = r^2 \) where \( r \) is a prime power. The Hermitian curve \( \mathcal{H}_r(\mathbb{F}_q) \) is a projective plane curve defined by

\[
f(x, y, z) = x^{r+1} - y^r z - yz^r = 0.
\]

Since \( r \) is a multiple of the characteristic then \( \mathcal{H}_r(\mathbb{F}_q) \) is non-singular.

Exercise

- Show that \((0 : 1 : 0)\) is the only point at infinity of \( \mathcal{H}_r(\mathbb{F}_q) \).
- Find the eight affine points \((x : y : 1)\) points of \( \mathcal{H}_2(\mathbb{F}_4) \).
Let \( q = r^2 \) where \( r \) is a prime power. The **Hermitian curve** \( \mathcal{H}_r(\mathbb{F}_q) \) is a projective plane curve defined by

\[
f(x, y, z) = x^{r+1} - y^r z - yz^r = 0.
\]

Since \( r \) is a multiple of the characteristic then \( \mathcal{H}_r(\mathbb{F}_q) \) is non-singular.

**Exercise**

- Show that \((0 : 1 : 0)\) is the only point at infinity of \( \mathcal{H}_r(\mathbb{F}_q) \).
- Find the eight affine points \((x : y : 1)\) points of \( \mathcal{H}_2(\mathbb{F}_4) \).
Algebraic curves

Example 2: Hermitian curve

Theorem

There are $r^3$ affine $(x : y : 1)$ points in $\mathcal{H}_r(\mathbb{F}_q)$. 
Theorem

There are $r^3$ affine $(x : y : 1)$ points in $\mathcal{H}_r(F_q)$.

Proof.

$z = 1$ implies $x^{r+1} = y^r + y = \text{Tr}_2(y)$ where $\text{Tr}_2$ is the trace map from $F_{r^2}$ to $F_r$.

$\text{Tr}_2(y)$ is $F_r$-linear and surjective, so its kernel is a 1-dim. $F_r$-subspace of $F_{r^2}$, thus has $r$ values with $\text{Tr}_2(y)$ that leads to $r$ affine points on $\mathcal{H}_r(F_q)$ of type $(0 : y : 1)$.

(Cont. ...)
Algebraic curves
Example 2: Hermitian curve

**Theorem**

There are $r^3$ affine $(x : y : 1)$ points in $\mathcal{H}_r(\mathbb{F}_q)$.

**Proof.**

If $x \in \mathbb{F}_{r^2}$ then $x^{r+1} \in \mathbb{F}_r$, as $r^2 - 1 = (r + 1)(r - 1)$ and the non zero elements of $\mathbb{F}_r$ in $\mathbb{F}_{r^2}$ are those satisfying $\beta^{r-1} = 1$. When $y$ is one of the $r^2 - r$ elements in $\mathbb{F}_{r^2}$ with $\text{Tr}_2(y) \neq 0$, there are $r+1$ solutions $x \in \mathbb{F}_{r^2}$ of $\text{Tr}_2(y) = x^{r+1}$. Thus there are $(r^2 - r)(r + 1) = r^3 - r$ more affine points on $\mathcal{H}_r(\mathbb{F}_q)$, and the theorem follows.
The **Klein quartic** $\mathcal{K}_4(\mathbb{F}_q)$ is a projective plane curve defined by

$$f(x, y, z) = x^3y + y^3z + z^3x = 0.$$ 

**Exercise**

- Find the three partial derivatives of $f$ and show that if $\text{char}(\mathbb{F}_q) = 3$ then $\mathcal{K}_4(\mathbb{F}_q)$ is non singular.

- If $(x : y : z)$ is a singular point in $\mathcal{K}_4(\mathbb{F}_q)$ show that $x^3y = -3y^3z$, $z^3x = 9y^3z$ and $7y^3z = 0$.

- Show that if $\text{char}(\mathbb{F}_q) \neq 7$ then $\mathcal{K}_4(\mathbb{F}_q)$ is non singular.
Algebraic curves
Example 3: The Klein quartic

The **Klein quartic** $\mathcal{K}_4(\mathbb{F}_q)$ is a projective plane curve defined by

$$f(x, y, z) = x^3y + y^3z + z^3x = 0.$$

**Exercise**

- Find the three partial derivatives of $f$ and show that if $\text{char}(\mathbb{F}_q) = 3$ then $\mathcal{K}_4(\mathbb{F}_q)$ is non singular.

- If $(x : y : z)$ is a singular point in $\mathcal{K}_4(\mathbb{F}_q)$ show that $x^3y = -3y^3z$, $z^3x = 9y^3z$ and $7y^3z = 0$.

- Show that if $\text{char}(\mathbb{F}_q) \neq 7$ then $\mathcal{K}_4(\mathbb{F}_q)$ is non singular.
The degree of a point in a curve depends on the field under consideration. Let $q = p^r$ ($p$ prime) and $m \geq 1$, the map $\sigma_q : \mathbb{F}_q^m \to \mathbb{F}_q^m$ given by $\sigma_q(\alpha) = \alpha^q$ is an automorphism of $\mathbb{F}_q^m$ that fixes $\mathbb{F}_q$ ($\sigma_q = \sigma_p^r$ where $\sigma_p$ is the Frobenius map).

If $P = (x, y)$ or $P = (x : y : z)$ in $\mathbb{A}^2(\mathbb{F}_q^m)$ or $\mathbb{P}^2(\mathbb{F}_q^m)$ denote by $\sigma_q(P) = (\sigma_q(x), \sigma_q(y))$ and $\sigma_q(P) = (\sigma_q(x) : \sigma_q(y) : \sigma_q(z))$ respectively.

**Exercise**

- Show that that $\sigma_q(P)$ is well defined if $P \in \mathbb{P}^2(\mathbb{F}_q)$.
- Show that if $f \in \mathbb{F}_q[x, y]$ (or homogeneous in $\mathbb{F}_q[x, y, z]$) then $f(P) = 0$ implies $f(\sigma_q(P)) = 0$ ($P \in \mathbb{A}^2(\mathbb{F}_q^m)$ or $\mathbb{P}^2(\mathbb{F}_q^m)$ respectively).
Algebraic curves
Degree of a point

The degree of a point in a curve depends on the field under consideration. Let \( q = p^r \) (\( p \) prime) and \( m \geq 1 \), the map \( \sigma_q : \mathbb{F}_q^m \to \mathbb{F}_q^m \) given by \( \sigma_q(\alpha) = \alpha^q \) is an automorphism of \( \mathbb{F}_q^m \) that fixes \( \mathbb{F}_q \) (\( \sigma_q = \sigma_p^r \) where \( \sigma_p \) is the Frobenius map).

If \( P = (x, y) \) or \( P = (x : y : z) \) in \( \mathbb{A}^2(\mathbb{F}_q^m) \) or \( \mathbb{P}^2(\mathbb{F}_q^m) \) denote by \( \sigma_q(P) = (\sigma_q(x), \sigma_q(y)) \) and \( \sigma_q(P) = (\sigma_q(x) : \sigma_q(y) : \sigma_q(z)) \) respectively.

Exercise

- Show that \( \sigma_q(P) \) is well defined if \( P \in \mathbb{P}^2(\mathbb{F}_q) \).
- Show that if \( f \in \mathbb{F}_q[x, y] \) (or homogeneous in \( \mathbb{F}_q[x, y, z] \)) then \( f(P) = 0 \) implies \( f(\sigma_q(P)) = 0 \) \( (P \in \mathbb{A}^2(\mathbb{F}_q^m) \) or \( \mathbb{P}^2(\mathbb{F}_q^m) \) respectively).
Algebraic curves
Degree of a point

The degree of a point in a curve depends on the field under consideration. Let \( q = p^r \) (\( p \) prime) and \( m \geq 1 \), the map \( \sigma_q : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m} \) given by \( \sigma_q(\alpha) = \alpha^q \) is an automorphism of \( \mathbb{F}_{q^m} \) that fixes \( \mathbb{F}_q \) (\( \sigma_q = \sigma_p^r \) where \( \sigma_p \) is the Frobenius map).

If \( P = (x, y) \) or \( P = (x : y : z) \) in \( \mathbb{A}^2(\mathbb{F}_{q^m}) \) or \( \mathbb{P}^2(\mathbb{F}_{q^m}) \) denote by \( \sigma_q(P) = (\sigma_q(x), \sigma_q(y)) \) and \( \sigma_q(P) = (\sigma_q(x) : \sigma_q(y) : \sigma_q(z)) \) respectively.

Exercise

- Show that that \( \sigma_q(P) \) is well defined if \( P \in \mathbb{P}^2(\mathbb{F}_q) \).
- Show that if \( f \in \mathbb{F}_q[x, y] \) (or homogeneous in \( \mathbb{F}_q[x, y, z] \)) then \( f(P) = 0 \) implies \( f(\sigma_q(P)) = 0 \) \( (P \in \mathbb{A}^2(\mathbb{F}_{q^m}) \) or \( \mathbb{P}^2(\mathbb{F}_{q^m}) \) respectively).
From exercise above if \( P \in \mathcal{X}_f(\mathbb{F}_{q^m}) \) then \( \{\sigma_q^i(P) \mid i \geq 0\} \subseteq \mathcal{X}_f(\mathbb{F}_{q^m}) \), and there are at most \( m \) distinct points in the set since \( \sigma_q^m = \text{Id} \).

A point \( P \) on \( \mathcal{X}_f(\mathbb{F}_q) \) of degree \( m \) over \( \mathbb{F}_q \) is a set of \( m \) distinct points \( P = \{P_0, \ldots, P_{m-1}\} \) with \( P_i \in \mathcal{X}_f(\mathbb{F}_{q^m}) \) and \( P_i = \sigma_q^i(P_0) \). We will denote the degree of \( P \) over \( \mathbb{F}_q \) as \( \text{deg}(P) \). Notice that points of degree \( m \) over \( \mathbb{F}_q \) are fixed by \( \sigma_q \) just as the elements of \( \mathbb{F}_q \), that’s why they are considered to be on \( \mathcal{X}_f(\mathbb{F}_q) \).

The points of degree one on \( \mathcal{X}_f(\mathbb{F}_q) \) are called rational points or \( \mathbb{F}_q \)-rational points.
Algebraic curves

Degree of a point

From exercise above if \( P \in \mathcal{X}_f(\mathbb{F}_{q^m}) \) then \( \{\sigma_q^i(P) \mid i \geq 0\} \subseteq \mathcal{X}_f(\mathbb{F}_{q^m}) \), and there are at most \( m \) distinct points in the set since \( \sigma_q^m = \text{Id} \).

A point \( P \) on \( \mathcal{X}_f(\mathbb{F}_q) \) of degree \( m \) over \( \mathbb{F}_q \) is a set of \( m \) distinct points \( P = \{P_0, \ldots, P_{m-1}\} \) with \( P_i \in \mathcal{X}_f(\mathbb{F}_{q^m}) \) and \( P_i = \sigma_q^i(P_0) \). We will denote the degree of \( P \) over \( \mathbb{F}_q \) as \( \text{deg}(P) \). Notice that points of degree \( m \) over \( \mathbb{F}_q \) are fixed by \( \sigma_q \) just as the elements of \( \mathbb{F}_q \), that’s why they are considered to be on \( \mathcal{X}_f(\mathbb{F}_q) \).

The points of degree one on \( \mathcal{X}_f(\mathbb{F}_q) \) are called rational points or \( \mathbb{F}_q \)-rational points.
From exercise above if \( P \in \mathcal{X}_f(\mathbb{F}_{q^m}) \) then \( \{ \sigma_q^i(P) \mid i \geq 0 \} \subseteq \mathcal{X}_f(\mathbb{F}_{q^m}) \), and there are at most \( m \) distinct points in the set since \( \sigma_q^m = \text{Id} \).

A point \( P \) on \( \mathcal{X}_f(\mathbb{F}_q) \) of degree \( m \) over \( \mathbb{F}_q \) is a set of \( m \) distinct points \( P = \{ P_0, \ldots, P_{m-1} \} \) with \( P_i \in \mathcal{X}_f(\mathbb{F}_{q^m}) \) and \( P_i = \sigma_q^i(P_0) \). We will denote the degree of \( P \) over \( \mathbb{F}_q \) as \( \text{deg}(P) \). Notice that points of degree \( m \) over \( \mathbb{F}_q \) are fixed by \( \sigma_q \) just as the elements of \( \mathbb{F}_q \), that’s why they are considered to be on \( \mathcal{X}_f(\mathbb{F}_q) \).

The points of degree one on \( \mathcal{X}_f(\mathbb{F}_q) \) are called rational points or \( \mathbb{F}_q \)-rational points.
Consider the **elliptic curve** defined by

\[ f(x, y, z) = x^3 + xz^2 + z^3 + y^2z + yz^2 \in \mathbb{F}_2[x, y, z]. \]

A point at infinity satisfies \( z = 0 \), thus \( x^3 = 0 \), therefore there is only one point at infinity \( P_\infty = (0 : 1 : 0) \) and is \( \mathbb{F}_2 \)-rational.

When considering the affine points we can assume \( z = 1 \), thus \( x^3 + x + 1 = y^2 + y \). If \( x, y \in \mathbb{F}_2 \) then

\[ x^3 + x + 1 = 1 \neq 0 = y^2 + y \]

thus the only \( \mathbb{F}_2 \)-rational point is \( P_\infty \).
Consider the **elliptic curve** defined by

\[ f(x, y, z) = x^3 + xz^2 + z^3 + y^2z + yz^2 \in \mathbb{F}_2[x, y, z]. \]

A point at infinity satisfies \( z = 0 \), thus \( x^3 = 0 \), therefore there is only one point at infinity \( P_\infty = (0 : 1 : 0) \) and is \( \mathbb{F}_2 \)-rational.

When considering the affine points we can assume \( z = 1 \), thus

\[ x^3 + x + 1 = y^2 + y. \]

If \( x, y \in \mathbb{F}_2 \) then

\[ x^3 + x + 1 = 1 \neq 0 = y^2 + y \]

thus the only \( \mathbb{F}_2 \)-rational point is \( P_\infty \).
Consider the **elliptic curve** defined by

\[ f(x, y, z) = x^3 + xz^2 + z^3 + y^2z + yz^2 \in \mathbb{F}_2[x, y, z]. \]

A point at infinity satisfies \( z = 0 \), thus \( x^3 = 0 \), therefore there is only one point at infinity \( P_\infty = (0 : 1 : 0) \) and is \( \mathbb{F}_2 \)-rational.

When considering the affine points we can assume \( z = 1 \), thus \( x^3 + x + 1 = y^2 + y \). If \( x, y \in \mathbb{F}_2 \) then

\[ x^3 + x + 1 = 1 \neq 0 = y^2 + y \]

thus the only \( \mathbb{F}_2 \)-rational point is \( P_\infty \).
Consider now $x, y \in \mathbb{F}_4$. If $y = 0, 1$ then $0 = y^2 + y$, but $x^3 + x + 1$ has no solution in $\mathbb{F}_4$.

If $y = \omega, \bar{\omega}$ are the roots of $y^2 + y = 1$, thus $x^3 + x = x(x + 1)^2 = 0$. Therefore the points of degree 2 are

$$P_1 = \{(0 : \omega : 1), (0 : \bar{\omega} : 1)\}, \quad P_2 = \{(1 : \omega : 1), (1 : \bar{\omega} : 1)\}$$
Consider now $x, y \in \mathbb{F}_4$. If $y = 0, 1$ then $0 = y^2 + y$, but $x^3 + x + 1$ has no solution in $\mathbb{F}_4$.

If $y = \omega, \bar{\omega}$ are the roots of $y^2 + y = 1$, thus $x^3 + x = x(x + 1)^2 = 0$. Therefore the points of degree 2 are

$$P_1 = \{(0 : \omega : 1), (0 : \bar{\omega} : 1)\}, \quad P_2 = \{(1 : \omega : 1), (1 : \bar{\omega} : 1)\}$$
When defining AG codes we will need to compute the points in the intersection of two curves and the \textbf{multiplicity at the point of intersection}.

We will not define it because the definition is quite technical. Instead of it we will show with the following example how can we compute multiplicity similarly to the way multiplicity of zeros is computed for one variable polynomials.
When defining AG codes we will need to compute the points in the intersection of two curves and the \textbf{multiplicity at the point of intersection}.

We will not define it because the definition is quite technical. Instead of it we will show with the following example how can we compute multiplicity similarly to the way multiplicity of zeros is computed for one variable polynomials.
Consider the elliptic curve defined by

\[ f(x, y, z) = x^3 + xz^2 + z^3 + y^2z + yz^2 \in \mathbb{F}_2[x, y, z]. \]

Intersection with \( x = 0 \):
We have either \( z = 0 \) or \( z = 1 \). In the first case we get \( P_\infty \) and in the latter \( (0 : \omega : 1), (0 : \bar{\omega} : 1) \in \mathbb{P}^2(\mathbb{F}_4) \).

We can see this in two ways:

- The curve and \( x = 0 \) intersect at three degree 1 points in \( \mathbb{P}^2(\mathbb{F}_4) \) with intersection multiplicity 1.
- The curve and \( x = 0 \) intersect at two points in \( \mathbb{P}^2(\mathbb{F}_2) \), one with degree 1 and the second with degree 2, both with with intersection multiplicity 1. (Notice that there are more points of higher degrees.)
Consider the elliptic curve defined by

\[ f(x, y, z) = x^3 + xz^2 + z^3 + y^2z + yz^2 \in \mathbb{F}_2[x, y, z]. \]

**Intersection with \( x = 0 \):**

We have either \( z = 0 \) or \( z = 1 \). In the first case we get \( P_{\infty} \) and in the latter \((0 : \omega : 1), (0 : \bar{\omega} : 1) \in \mathbb{P}^2(\mathbb{F}_4)\).

We can see this in two ways:

- The curve and \( x = 0 \) intersect at three degree 1 points in \( \mathbb{P}^2(\mathbb{F}_4) \) with intersection multiplicity 1.
- The curve and \( x = 0 \) intersect at two points in \( \mathbb{P}^2(\mathbb{F}_2) \), one with degree 1 and the second with degree 2, both with with intersection multiplicity 1. (Notice that there are more points of higher degrees)
Consider the elliptic curve defined by

\[ f(x, y, z) = x^3 + xz^2 + z^3 + y^2z + yz^2 \in \mathbb{F}_2[x, y, z]. \]

**Intersection with** \(x = 0:\)**

We have either \(z = 0\) or \(z = 1\). In the first case we get \(P_{\infty}\) and in the latter \((0 : \omega : 1), (0 : \bar{\omega} : 1) \in \mathbb{P}^2(\mathbb{F}_4)\).

We can see this in two ways:

- The curve and \(x = 0\) intersect at three degree 1 points in \(\mathbb{P}^2(\mathbb{F}_4)\) with intersection multiplicity 1.
- The curve and \(x = 0\) intersect at two points in \(\mathbb{P}^2(\mathbb{F}_2)\), one with degree 1 and the second with degree 2, both with with intersection multiplicity 1. (Notice that there are more points of higher degress)
Consider the elliptic curve defined by

\[ f(x, y, z) = x^3 + xz^2 + z^3 + y^2z + yz^2 \in \mathbb{F}_2[x, y, z]. \]

**Intersection with** \( x = 0 \):

We have either \( z = 0 \) or \( z = 1 \). In the first case we get \( P_\infty \) and in the latter \((0 : \omega : 1), (0 : \bar{\omega} : 1) \in \mathbb{P}^2(\mathbb{F}_4)\).

We can see this in two ways:

- The curve and \( x = 0 \) intersect at three degree 1 points in \( \mathbb{P}^2(\mathbb{F}_4) \) with intersection multiplicity 1.
- The curve and \( x = 0 \) intersect at two points in \( \mathbb{P}^2(\mathbb{F}_2) \), one with degree 1 and the second with degree 2, both with with intersection multiplicity 1. (Notice that there are more points of higher degree.)
Consider the elliptic curve defined by
\[ f(x, y, z) = x^3 + xz^2 + z^3 + y^2z + yz^2 \in \mathbb{F}_{2^r}[x, y, z]. \]

**Intersection with \( x = 0 \):**
We have either \( z = 0 \) or \( z = 1 \). In the first case we get \( P_\infty \) and in the latter \( (0 : \omega : 1), (0 : \bar{\omega} : 1) \in \mathbb{P}^2(\mathbb{F}_4) \).
We can see this in two ways:

- The curve and \( x = 0 \) intersect at three degree 1 points in \( \mathbb{P}^2(\mathbb{F}_4) \) with intersection multiplicity 1.
- The curve and \( x = 0 \) intersect at two points in \( \mathbb{P}^2(\mathbb{F}_2) \), one with degree 1 and the second with degree 2, both with with intersection multiplicity 1. (Notice that there are more points of higher degrees)
Intersection with $x^2 = 0$:
Notice that $x^2 = 0$ is the union of the line $x = 0$ with itself. Thus any point at $x^2 = 0$ and the elliptic curve occurs twice as frequently as it did at $x = 0$. Thus

- The curve and $x^2 = 0$ intersect at three degree 1 points in $\mathbb{P}^2(\mathbb{F}_4)$ with intersection multiplicity 2.
- The curve and $x = 0$ intersect at two points in $\mathbb{P}^2(\mathbb{F}_2)$, one with degree 1 and the second with degree 2, both with with intersection multiplicity 2.
Intersection with $x^2 = 0$:
Notice that $x^2 = 0$ is the union of the line $x = 0$ with itself. Thus any point at $x^2 = 0$ and the elliptic curve occurs twice as frequently as it did at $x = 0$. Thus

- The curve and $x^2 = 0$ intersect at three degree 1 points in $\mathbb{P}^2(\mathbb{F}_4)$ with intersection multiplicity 2.
- The curve and $x = 0$ intersect at two points in $\mathbb{P}^2(\mathbb{F}_2)$, one with degree 1 and the second with degree 2, both with with intersection multiplicity 2.
Intersection with $x^2 = 0$:

Notice that $x^2 = 0$ is the union of the line $x = 0$ with itself. Thus any point at $x^2 = 0$ and the elliptic curve occurs twice as frequently as it did at $x = 0$. Thus

- The curve and $x^2 = 0$ intersect at three degree 1 points in $\mathbb{P}^2(\mathbb{F}_4)$ with intersection multiplicity 2.
- The curve and $x = 0$ intersect at two points in $\mathbb{P}^2(\mathbb{F}_2)$, one with degree 1 and the second with degree 2, both with with intersection multiplicity 2.
Intersection with $x^2 = 0$:

Notice that $x^2 = 0$ is the union of the line $x = 0$ with itself. Thus any point at $x^2 = 0$ and the elliptic curve occurs twice as frequently as it did at $x = 0$. Thus

- The curve and $x^2 = 0$ intersect at three degree 1 points in $\mathbb{P}^2(\mathbb{F}_4)$ with intersection multiplicity 2.
- The curve and $x = 0$ intersect at two points in $\mathbb{P}^2(\mathbb{F}_2)$, one with degree 1 and the second with degree 2, both with with intersection multiplicity 2.
Intersection with $z = 0$:
We have seen that there is only one point $P_\infty$ of the elliptic curve with $z = 0$. $P_\infty$ has degree 1 over any extension field of $\mathbb{F}_2$. When we plug $z = 0$ in the equation of the elliptic curve we get $x^3 = 0$, thus $P_\infty$ occurs with multiplicity 3.

Intersection with $z^2 = 0$:
As in the case $x^2 = 0$ we double the multiplicities obtained above, thus $P_\infty$ occurs on the intersection with multiplicity 6.
Intersection with $z = 0$:
We have seen that there is only one point $P_\infty$ of the elliptic curve with $z = 0$. $P_\infty$ has degree 1 over any extension field of $\mathbb{F}_2$. When we plug $z = 0$ in the equation of the elliptic curve we get $x^3 = 0$, thus $P_\infty$ occurs with multiplicity 3.

Intersection with $z^2 = 0$:
As in the case $x^2 = 0$ we double the multiplicities obtained above, thus $P_\infty$ occurs on the intersection with multiplicity 6.
Intersection with $y = 0$:

$z = 0$ is not possible ($\Rightarrow x = 0$), so $z = 1$ and we have

$$x^3 + x + 1 = 0.$$ 

The solutions to this equation occur in $\mathbb{F}_8$ and give us the points

$$(\alpha : 0 : 1), \quad (\alpha^2 : 0 : 1), \quad (\alpha^4 : 0 : 1) \quad \in \mathbb{P}(\mathbb{F}_8)$$

Therefore over $\mathbb{F}_8$ there are 3 points in the intersection, each of them of degree 1 and multiplicity 1. Over $\mathbb{F}_2$ they combine in a single degree 3 point $P_3$ with intersection multiplicity 1.
Intersection with $y = 0$:

$z = 0$ is not possible ($\implies x = 0$), so $z = 1$ and we have

$$x^3 + x + 1 = 0.$$  

The solutions to this equation occur in $\mathbb{F}_8$ and give us the points

$$(\alpha : 0 : 1), \quad (\alpha^2 : 0 : 1), \quad (\alpha^4 : 0 : 1) \in \mathbb{P}(\mathbb{F}_8).$$

Therefore over $\mathbb{F}_8$ there are 3 points in the intersection, each of them of degree 1 and multiplicity 1. Over $\mathbb{F}_2$ they combine in a single degree 3 point $P_3$ with intersection multiplicity 1.
Intersection with \( y = 0 \):
z = 0 is not possible (\( \Rightarrow x = 0 \)), so \( z = 1 \) and we have
\[
x^3 + x + 1 = 0.
\]
The solutions to this equation occur in \( \mathbb{F}_8 \) and give us the points
\[
(\alpha : 0 : 1), \quad (\alpha^2 : 0 : 1), \quad (\alpha^4 : 0 : 1) \quad \in \mathbb{P}(\mathbb{F}_8)
\]
Therefore over \( \mathbb{F}_8 \) there are 3 points in the intersection, each of them of degree 1 and multiplicity 1. Over \( \mathbb{F}_2 \) they combine in a single degree 3 point \( P_3 \) with intersection multiplicity 1.
We have seen that there is a “type” of uniformity when counting properly the number of points in the intersection of two curves, where properly means take into account both degree and multiplicity. This was stated in the following theorem.

**Theorem (Bézout)**

Let $f, g$ be homogeneous polynomials in $\mathbb{F}[x, y, z]$ of degrees $d_f, d_g$ respectively. Suppose that $f$ and $g$ have no common nonconstant polynomial factors. Then $\mathcal{X}_f$ and $\mathcal{X}_g$ intersect at $d_fd_g$ points counted with multiplicity and degree.
We have seen that there is a “type” of uniformity when counting properly the number of points in the intersection of two curves, where properly means take into account both degree and multiplicity. This was stated in the following theorem

**Theorem (Bézout)**

Let \( f, g \) be homogeneous polynomials in \( \mathbb{F}[x, y, z] \) of degrees \( d_f, d_g \) respectively. Suppose that \( f \) and \( g \) have no common nonconstant polynomial factors. Then \( \mathcal{X}_f \) and \( \mathcal{X}_g \) intersect at \( d_f d_g \) points counted with multiplicity and degree.
A divisor $D$ on $\mathcal{X}$ over $\mathbb{F}$ is a formal sum

$$D = \sum n_P P,$$  \hspace{1cm} (17)

where $n_P$ is an integer and $P$ is a point of arbitrary degree on the curve $\mathcal{X}$, with only a finite number of $n_P$ being nonzero.

The divisor $D$ is effective if $n_P \geq 0$ for all $P$. The support $\text{supp}(D)$ of the divisor $D$ is the set $\{P \mid n_P \neq 0\}$. The degree of the divisor is

$$\deg(D) = \sum n_P \deg(P).$$  \hspace{1cm} (18)
Algebraic curves

Divisors

A divisor $D$ on $\mathcal{X}$ over $\mathbb{F}$ is a formal sum

$$D = \sum n_P P,$$  \hspace{1cm} (17)

where $n_P$ is an integer and $P$ is a point of arbitrary degree on the curve $\mathcal{X}$, with only a finite number of $n_P$ being nonzero.

The divisor $D$ is effective if $n_P \geq 0$ for all $P$. The support $\text{supp}(D)$ of the divisor $D$ is the set $\{P \mid n_P \neq 0\}$. The degree of the divisor is

$$\deg(D) = \sum n_P \deg(P).$$  \hspace{1cm} (18)
If \( \mathcal{X}_1 \) and \( \mathcal{X}_2 \) are two projective curves then their intersection divisor over \( \mathbb{F} \) denoted by \( \mathcal{X}_1 \cap \mathcal{X}_2 = \sum n_P P \) where the summation runs over all the points both in \( \mathcal{X}_1 \) and \( \mathcal{X}_2 \) and \( n_P \) is the multiplicity of the point in the intersection of the curves.

If \( \mathcal{X}_1 \) and \( \mathcal{X}_2 \) are defined by homogeneous polynomials of degrees \( d_f, d_g \) respectively with no common nonconstant polynomial factors then

\[
\deg(\mathcal{X}_1 \cap \mathcal{X}_2) = d_f d_g. \tag{19}
\]
If $\mathcal{X}_1$ and $\mathcal{X}_2$ are two projective curves then their intersection divisor over $\mathbb{F}$ denoted by $\mathcal{X}_1 \cap \mathcal{X}_2 = \sum n_P P$ where the summation runs over all the points both in $\mathcal{X}_1$ and $\mathcal{X}_2$ and $n_P$ is the multiplicity of the point in the intersection of the curves.

If $\mathcal{X}_1$ and $\mathcal{X}_2$ are defined by homogeneous polynomials of degrees $d_f, d_g$ respectively with no common nonconstant polynomial factors then

$$\deg(\mathcal{X}_1 \cap \mathcal{X}_2) = d_f d_g. \quad (19)$$
Consider the **elliptic curve** defined by

\[ f(x, y, z) = x^3 + xz^2 + z^3 + y^2z + yz^2 \in \mathbb{F}_2[x, y, z]. \]

- Intersection with \( x = 0 \): \( P_\infty + P_1 \).
- Intersection with \( x^2 = 0 \): \( 2P_\infty + 2P_1 \).
- Intersection with \( z = 0 \): \( 3P_\infty \).
- Intersection with \( z^2 = 0 \): \( 6P_\infty \).
- Intersection with \( y = 0 \): \( P_3 \).
Consider the **elliptic curve** defined by

\[ f(x, y, z) = x^3 + xz^2 + z^3 + y^2z + yz^2 \in \mathbb{F}_2[x, y, z]. \]

- Intersection with \( x = 0 \): \( P_\infty + P_1 \).
- Intersection with \( x^2 = 0 \): \( 2P_\infty + 2P_1 \).
- Intersection with \( z = 0 \): \( 3P_\infty \).
- Intersection with \( z^2 = 0 \): \( 6P_\infty \).
- Intersection with \( y = 0 \): \( P_3 \).
Consider the **elliptic curve** defined by

\[ f(x, y, z) = x^3 + xz^2 + z^3 + y^2z + yz^2 \in \mathbb{F}_2[x, y, z]. \]

- Intersection with \( x = 0 \): \( P_\infty + P_1 \).
- Intersection with \( x^2 = 0 \): \( 2P_\infty + 2P_1 \).
- Intersection with \( z = 0 \): \( 3P_\infty \).
- Intersection with \( z^2 = 0 \): \( 6P_\infty \).
- Intersection with \( y = 0 \): \( P_3 \).
Consider the **elliptic curve** defined by

\[ f(x, y, z) = x^3 + xz^2 + z^3 + y^2z + yz^2 \in \mathbb{F}_2[x, y, z]. \]

- Intersection with \( x = 0 \): \( P_\infty + P_1 \).
- Intersection with \( x^2 = 0 \): \( 2P_\infty + 2P_1 \).
- Intersection with \( z = 0 \): \( 3P_\infty \).
- Intersection with \( z^2 = 0 \): \( 6P_\infty \).
- Intersection with \( y = 0 \): \( P_3 \).
Consider the elliptic curve defined by

\[ f(x, y, z) = x^3 + xz^2 + z^3 + y^2z + yz^2 \in \mathbb{F}_2[x, y, z]. \]

- Intersection with \( x = 0 \): \( P_\infty + P_1 \).
- Intersection with \( x^2 = 0 \): \( 2P_\infty + 2P_1 \).
- Intersection with \( z = 0 \): \( 3P_\infty \).
- Intersection with \( z^2 = 0 \): \( 6P_\infty \).
- Intersection with \( y = 0 \): \( P_3 \).
Consider the elliptic curve defined by

\[ f(x, y, z) = x^3 + xz^2 + z^3 + y^2z + yz^2 \in \mathbb{F}_2[x, y, z]. \]

- Intersection with \( x = 0 \): \( P_\infty + P_1 \).
- Intersection with \( x^2 = 0 \): \( 2P_\infty + 2P_1 \).
- Intersection with \( z = 0 \): \( 3P_\infty \).
- Intersection with \( z^2 = 0 \): \( 6P_\infty \).
- Intersection with \( y = 0 \): \( P_3 \).
When finding the minimum distance of an AG code it will be connected to the **genus of a curve**. This is related to a topological concept of the same name but quite offtopic in this course. We will just show Plücker’s formula that will serve in our case as a definition for the genus.

**Theorem (Plücker’s formula)**

The genus of a nonsingular projective plane curve determined by an homogeneous polynomial of degree \( d \geq 1 \) is

\[
g = \frac{(d - 1)(d - 2)}{2}.
\]

(20)
When finding the minimum distance of an AG code it will be connected to the genus of a curve. This is related to a topological concept of the same name but quite offtopic in this course. We will just show Plüker’s formula that will serve in our case as a definition for the genus.

**Theorem (Plüker’s formula)**

The genus of a nonsingular projective plane curve determined by an homogeneous polynomial of degree $d \geq 1$ is

$$g = \frac{(d - 1)(d - 2)}{2}.$$  \hfill (20)
Algebraic Geometry codes

Rational functions

In the classical examples we have shown all codes were function evaluation of “points” where the function runs through a certain vector space. For AG-codes we start with the definition of such functions.

Let $p(x, y, z)$ an homogeneous polynomial that defines a projective curve $X$ over $\mathbb{F}$. We define the field of rational functions on $X$ over $\mathbb{F}$ as

$$
\mathbb{F}(X) = \left\{ \frac{g}{h} \mid g, h \text{ homogeneous, same degree, } p \nmid h \right\} \cup \{0\} / \approx_X. \quad (21)
$$

where $f/g \approx_X f'/g'$ if $fg' - f'g$ is a multiple of $p(x, y, z)$. 


In the classical examples we have shown all codes were function evaluation of “points” where the function runs through a certain vector space. For AG-codes we start with the definition of such functions.

Let $p(x, y, z)$ an homogeneous polynomial that defines a projective curve $\mathcal{X}$ over $\mathbb{F}$. We define the field of rational functions on $\mathcal{X}$ over $\mathbb{F}$ as

$$\mathbb{F}(\mathcal{X}) = \left\{ \frac{g}{h} \mid g, h \text{ homogeneous, same degree, } p \nmid h \right\} \cup \{0\} \approx_{\mathcal{X}}. \quad (21)$$

where $f/g \approx_{\mathcal{X}} f'/g'$ if $fg' - f'g$ is a multiple of $p(x, y, z)$. 


Exercise

Show that $\mathbb{F}(\mathcal{X})$ is a field containing $\mathbb{F}$ as a subfield. Notice that the class of 0 is precisely when $g$ is a multiple of $p(x, y, z)$.

Let $f = \frac{g}{h} \in \mathbb{F}(\mathcal{X})$ such that $f \not\approx \mathcal{X} 0$. Then the divisor of $f$ is

$$\text{div}(f) = (\mathcal{X} \cap \mathcal{X}_g) - (\mathcal{X} \cap \mathcal{X}_h)$$

(22)

By Bézout theorem $\deg (\text{div}(f)) = d_p d_g - d_p d_h = 0$. Since $f$ is an equivalence class remains to proof that $\text{div}(f)$ is well defined. This is true but we will not prove it.
Exercise

Show that $\mathbb{F}(X)$ is a field containing $\mathbb{F}$ as a subfield. Notice that the class of 0 is precisely when $g$ is a multiple of $p(x, y, z)$.

Let $f = \frac{g}{h} \in \mathbb{F}(X)$ such that $f \not\sim 0$. Then the divisor of $f$ is

$$\text{div}(f) = (X \cap X_g) - (X \cap X_h) \quad (22)$$

By Bézout theorem $\deg(\text{div}(f)) = d_p d_g - d_p d_h = 0$. Since $f$ is an equivalence class remains to proof that $\text{div}(f)$ is well defined. This is true but we will not prove it.
Exercise

Show that $\mathbb{F}(\mathcal{X})$ is a field containing $\mathbb{F}$ as a subfield. Notice that the class of 0 is precisely when $g$ is a multiple of $p(x, y, z)$.

Let $f = \frac{g}{h} \in \mathbb{F}(\mathcal{X})$ such that $f \not\approx \mathcal{X} 0$. Then the divisor of $f$ is

$$
\text{div}(f) = (\mathcal{X} \cap X_g) - (\mathcal{X} \cap X_h)
$$

(22)

By Bézout theorem $\deg(\text{div}(f)) = d_p d_g - d_p d_h = 0$. Since $f$ is an equivalence class remains to proof that $\text{div}(f)$ is well defined. This is true but we will not prove it.
Exercise

Let $\mathcal{C}$ the elliptic curve

$$f(x, y, z) = x^3 + xz^2 + z^3 + y^2 z + yz^2 \in \mathbb{F}[x, y, z].$$

where $\text{char}(\mathbb{F}) = 2$. Let $f = \frac{g}{h}$ and $f' = \frac{g'}{h'}$ where $g = x^2 + z^2$, $h = z^2$, $g' = z^2 + y^2 + yz$ and $h' = xz$. Let $P_\infty = (0 : 1 : 0)$ and $P_2 = \{(1 : \omega : 1), (1 : \bar{\omega} : 1)\}$.

- Show that $f \cong \mathcal{C} f'$.
- Show that $\text{div}(f) = 2P_2 - P_\infty$.
- Show that $\text{div}(f') = 2P_2 - P_\infty$. 
Given two divisors on a curve we will say

\[ D = \sum n_P P \geq D' = \sum n'_P P \]

provided that \( n_P \geq n'_P \) for all the points. (I.e. \( D \) is effective if \( D \geq 0 \)).

Exercise

Prove that \( L(D) \) is a \( \mathbb{F} \)-vector space.
Given two divisors on a curve we will say

\[ D = \sum n_P P \succeq D' = \sum n'_P P \]

provided that \( n_P \geq n'_P \) for all the points. (I.e. \( D \) is effective if \( D \succeq 0 \)).

Given a divisor \( D \) on a projective curve \( \mathcal{X} \) over \( \mathbb{F} \) let

\[ L(D) = \{ f \in \mathbb{F}(\mathcal{X}) \mid f \not\equiv 0, \text{div}(f) + D \succeq 0 \} \cup \{0\}. \tag{23} \]

Exercise

Prove that \( L(D) \) is a \( \mathbb{F} \)-vector space.
Given two divisors on a curve we will say
\[ D = \sum n_P P \succeq D' = \sum n'_P P \]
provided that \( n_P \geq n'_P \) for all the points. (i.e. \( D \) is effective if \( D \succeq 0 \)).

Given a divisor \( D \) on a projective curve \( \mathcal{X} \) over \( \mathbb{F} \) let
\[
L(D) = \{ f \in \mathbb{F}(\mathcal{X}) \mid f \not\equiv 0, \text{div}(f) + D \succeq 0 \} \cup \{0\}. \tag{23}
\]

**Exercise**

Prove that \( L(D) \) is a \( \mathbb{F} \)-vector space.
Theorem

Let $D$ be a divisor on a projective curve $X$. The following statements hold:

- If $\deg(D) < 0$, then $L(D) = \{0\}$.
- The constant functions are in $L(D)$ if and only if $D \succeq 0$.
- If $P$ is a point in $X$ with $P \notin \supp(D)$, then $P$ is not a pole in any $f \in L(D)$. 
Algebraic Geometry codes
The vector space $L(D)$

Proof.

- If $f \in L(D)$ with $f \not\equiv 0$ then $\text{div}(f) + D \succeq 0$, i.e. $\deg(\text{div}(f) + D) \geq 0$, but $\deg(\text{div}(f) + D) = \deg(D)$, which is a contradiction.

- Let $f \not\equiv 0$ a constant function. If $f \in L(D)$ then $\text{div}(f) + D \succeq 0$. But $\text{div}(f) = 0$ (is constant), thus $D \succeq 0$. Conversely, if $D \succeq 0$ then $\text{div}(f) + D = D \succeq 0$.

- If $P$ is a pole in $f \in L(D)$ with $P \not\in \text{supp}(D)$ then the coefficient of $P$ in $\text{div}(f) + D$ of $X$ is negative, contradicting $f \in L(D)$.
Proof.

- If $f \in L(D)$ with $f \not\approx \chi 0$ then $\text{div}(f) + D \succeq 0$, i.e. $\deg(\text{div}(f) + D) \geq 0$, but $\deg(\text{div}(f) + D) = \deg(D)$, which is a contradiction.

- Let $f \not\approx \chi 0$ a constant function. If $f \in L(D)$ then $\text{div}(f) + D \succeq 0$. But $\text{div}(f) = 0$ (is constant), thus $D \succeq 0$. Conversely, if $D \succeq 0$ then $\text{div}(f) + D = D \succeq 0$.

- If $P$ is a pole in $f \in L(D)$ with $P \notin \text{supp}(D)$ then the coefficient of $P$ in $\text{div}(f) + D$ of $\chi$ is negative, contradicting $f \in L(D)$. \qed
Proof.

- If $f \in L(D)$ with $f \not\approx x^0$ then $\text{div}(f) + D \succeq 0$, i.e. $\deg(\text{div}(f) + D) \geq 0$, but $\deg(\text{div}(f) + D) = \deg(D)$, which is a contradiction.

- Let $f \not\approx x^0$ a constant function. If $f \in L(D)$ then $\text{div}(f) + D \succeq 0$. But $\text{div}(f) = 0$ (is constant), thus $D \succeq 0$. Conversely, if $D \succeq 0$ then $\text{div}(f) + D = D \succeq 0$.

- If $P$ is a pole in $f \in L(D)$ with $P \notin \text{supp}(D)$ then the coefficient of $P$ in $\text{div}(f) + D$ of $x$ is negative, contradicting $f \in L(D)$. 


Let $p(x, y, z)$ an homogeneous polynomial that defines a projective curve $\mathcal{X}$ over $\mathbb{F}_q$. Let $D$ be a divisor on $\mathcal{X}$ and choose a set $\mathcal{P} = \{P_1, \ldots, P_n\}$ of $n$ distinct $\mathbb{F}_q$-rational points on $\mathcal{X}$ such that $\text{supp}(D) \cap \mathcal{P} = \emptyset$. If we order the points in $\mathcal{P}$ consider the evaluation map

$$
ev_{\mathcal{P}} : L(D) \rightarrow \mathbb{F}_q^n$$

$$f \mapsto \nev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n)) \quad (24)$$

**Exercise**

Is $\nev_{\mathcal{P}}$ well defined?
Geometric Reed Solomon codes
Evaluating rational functions in $L(D)$

Let $p(x, y, z)$ an homogeneous polynomial that defines a projective curve $\mathcal{X}$ over $\mathbb{F}_q$. Let $D$ be a divisor on $\mathcal{X}$ and choose a set $\mathcal{P} = \{P_1, \ldots, P_n\}$ of $n$ distinct $\mathbb{F}_q$-rational points on $\mathcal{X}$ such that $\text{supp}(D) \cap \mathcal{P} = \emptyset$. If we order the points in $\mathcal{P}$ consider the evaluation map

$$\text{ev}_{\mathcal{P}} : L(D) \longrightarrow \mathbb{F}_q^n$$
$$f \longmapsto \text{ev}_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n)) \quad (24)$$

**Exercise**

Is $\text{ev}_{\mathcal{P}}$ well defined?
If \( f \in L(D) \) then \( P_i \) is not a pole of \( f \), however if \( f \) is represented by \( \frac{g}{h} \) then \( h \) may have \( P_i \) as a zero occurring in \( \mathcal{X} \cap \mathcal{X}_h \) and it will occur at least so many times in \( \mathcal{X} \cap \mathcal{X}_g \). If we choose \( \frac{g}{h} \) to represent \( f \) then \( f(P_i) = \frac{0}{0} \), we must avoid this situation. It can be shown that for any \( f \in L(D) \) we can choose a representative \( \frac{g}{h} \) with \( h(P_i) \neq 0 \).

Suppose now that \( f \) has two such representatives \( \frac{g}{h} \approx \frac{g'}{h'} \) where \( h(P_i) \neq 0 \neq h'(P_i) \). Then \( gh' - g'h \) is a polynomial multiple of \( p \) and \( p(P_i) = 0 \). Thus \( g(P_i)h'(P_i) = g'(P_i)h(P_i) \), i.e. \( \frac{g}{h}(P_i) = \frac{g'}{h'}(P_i) \).
If \( f \in L(D) \) then \( P_i \) is not a pole of \( f \), however if \( f \) is represented by \( \frac{g}{h} \) then \( h \) may have \( P_i \) as a zero occurring in \( \mathcal{X} \cap \mathcal{X}_h \) and it will occur at least so many times in \( \mathcal{X} \cap \mathcal{X}_g \). If we choose \( \frac{g}{h} \) to represent \( f \) then \( f(P_i) = \frac{0}{0} \), we must avoid this situation. It can be shown that for any \( f \in L(D) \) we can choose a representative \( \frac{g}{h} \) with \( h(P_i) \neq 0 \).

Suppose now that \( f \) has two such representatives \( \frac{g}{h} \approx \mathcal{X} \frac{g'}{h'} \) where \( h(P_i) \neq 0 \neq h'(P_i) \). Then \( gh' - g'h \) is a polynomial multiple of \( p \) and \( p(P_i) = 0 \). Thus \( g(P_i)h'(P_i) = g'(P_i)h(P_i) \), i.e. \( \frac{g}{h}(P_i) = \frac{g'}{h'}(P_i) \).
Exercise

Prove that $\text{ev}_P$ is a $\mathbb{F}_q$-linear mapping.

With the notation above we define the algebraic geometry code associated to $\mathcal{X}$, $\mathcal{P}$ and $D$ to be

$$ C(\mathcal{X}, \mathcal{P}, D) = \{ \text{ev}_P(f) \mid f \in L(D) \} . $$

(25)
Exercise

Prove that \( \text{ev}_P \) is a \( \mathbb{F}_q \)-linear mapping.

With the notation above we define the algebraic geometry code associated to \( \mathcal{X}, \mathcal{P} \) and \( D \) to be

\[
\mathcal{C}(\mathcal{X}, \mathcal{P}, D) = \{ \text{ev}_P(f) \mid f \in L(D) \}. \tag{25}
\]
In order to get some information on the dimension and minimum distance we will use the following version of the Riemann-Roch’s Theorem.

**Theorem (Riemann-Roch)**

Let $D$ a divisor in a nonsingular projective plane curve $\mathcal{X}$ over $\mathbb{F}_q$ of genus $g$. Then

- $\dim(L(D)) \geq \deg(D) + 1 - g$.
- *Furthermore, if* $\deg(D) > 2g - 2$ *then*

$$\dim(L(D)) = \deg(D) + 1 - g.$$
Geometric Reed Solomon codes
Riemann-Roch

**Theorem**

Let $D$ a divisor in a nonsingular projective plane curve $X$ over $\mathbb{F}_q$ of genus $g$. Let $\mathcal{P}$ a set of $n$ distinct $\mathbb{F}_q$-rational points on $X$ such that $\text{supp}(D) \cap \mathcal{P} = \emptyset$. Assume that

$$2g - 2 < \deg(D) < n.$$  

Then $C(X, \mathcal{P}, D)$ is an $[n, k, d]$ code over $\mathbb{F}_q$ where

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

In order to check $k = \deg(D) + 1 - g$ by Riemann-Roch theorem we just need to show that $ev_P$ has trivial kernel. Suppose that $ev_P(f) = 0$, then $f(P_i) = 0$ for all $i$, i.e. is a zero of $f$, since $P_i \notin \text{supp}(D)$ we have $\text{div}(f) + D - (\sum_{i=1}^{n} P_i) \geq 0$. Therefore $f \in L(D - (\sum_{i=1}^{n} P_i))$, but $\deg(D) < n$, thus $\deg(D - (\sum_{i=1}^{n} P_i)) < 0$ and we have $L(D - (\sum_{i=1}^{n} P_i)) = \{0\}$ and $f = 0$.

Suppose that $ev_P(f)$ has minimum weight $d$. Thus $f(P_i) = 0$ for $n - d$ indices $\{i_j \mid 1 \leq j \leq n - d\}$. Thus $f \in L(D - (\sum_{j=1}^{n-d} P_{i_j})$ and therefore $\deg(D - (\sum_{j=1}^{n-d} P_{i_j}) \geq 0$. Hence $\deg(D) - (n - d) \geq 0$. 


Proof.

In order to check $k = \deg(D) + 1 - g$ by Riemann-Roch theorem we just need to show that $\text{ev}_P$ has trivial kernel. Suppose that $\text{ev}_P(f) = 0$, then $f(P_i) = 0$ for all $i$, i.e. is a zero of $f$, since $P_i \notin \mathsf{supp}(D)$ we have $\text{div}(f) + D - (\sum_{i=1}^{n} P_i) \succeq 0$. Therefore $f \in L(D - (\sum_{i=1}^{n} P_i))$, but $\deg(D) < n$, thus $\deg(D - (\sum_{i=1}^{n} P_i)) < 0$ and we have $L(D - (\sum_{i=1}^{n} P_i)) = \{0\}$ and $f = 0$.

Suppose that $\text{ev}_P(f)$ has minimum weight $d$. Thus $f(P_i) = 0$ for $n - d$ indices $\{i_j \mid 1 \leq j \leq n - d\}$. Thus $f \in L(D - (\sum_{j=1}^{n-d} P_{i_j}))$ and therefore $\deg(D - (\sum_{j=1}^{n-d} P_{i_j})) \geq 0$. Hence $\deg(D - (n - d)) \geq 0$. 

{\hfill \Box}
As a corollary of previous theorem we have that if \( \{f_1, \ldots, f_k\} \) is a basis of \( L(D) \) then a generator matrix of the code \( \mathcal{C}(X, P, D) \) is

\[
\begin{pmatrix}
  f_1(P_1) & f_1(P_2) & \ldots & f_1(P_n) \\
  f_2(P_1) & f_2(P_2) & \ldots & f_2(P_n) \\
  \vdots & \vdots & \ddots & \vdots \\
  f_k(P_1) & f_k(P_2) & \ldots & f_k(P_n)
\end{pmatrix}.
\]
Consider the projective curve $\mathcal{X}$ over $\mathbb{F}_q$ given by $z = 0$. The points in the curve are $(x : y : 0)$. Let $P_\infty = (1 : 0 : 0)$, $P_0 = (0 : 1 : 0)$ and $P_1, \ldots P_{q-1}$ the remaining rational points. For narrow sense RS codes we will let $n = q - 1$ and $\mathcal{P} = \{P_1, \ldots P_{q-1}\}$ and for the extended narrow-sense RS codes $n = q$ and $\mathcal{P} = \{P_0, \ldots P_{q-1}\}$.

Fix $k$ ($1 \leq k \leq n$) and let $D = (k-1)P_\infty$ ($D = 0$ when $k = 1$). We have that $\text{supp}(D) \cap \mathcal{P} = \emptyset$ and $\mathcal{X}$ is non-singular of genus $g = 0$. Also $k - 1 = \deg(D) > 2g - 2$ thus $
 dim(L(D)) = \deg(D) + 1 - g = k$. 


Consider the projective curve $\mathcal{X}$ over $\mathbb{F}_q$ given by $z = 0$. The points in the curve are $(x : y : 0)$. Let $P_\infty = (1 : 0 : 0)$, $P_0 = (0 : 1 : 0)$ and $P_1, \ldots P_{q-1}$ the remaining rational points. For narrow sense RS codes we will let $n = q - 1$ and $\mathcal{P} = \{P_1, \ldots P_{q-1}\}$ and for the extended narrow-sense RS codes $n = q$ and $\mathcal{P} = \{P_0, \ldots P_{q-1}\}$.

Fix $k$ ($1 \leq k \leq n$) and let $D = (k - 1)P_\infty$ ($D = 0$ when $k = 1$). We have that $\text{supp}(D) \cap \mathcal{P} = \emptyset$ and $\mathcal{X}$ is non singular of genus $g = 0$. Also $k - 1 = \deg(D) > 2g - 2$ thus $\dim(L(D)) = \deg(D) + 1 - g = k$. 

Geometric Reed Solomon codes
Reed-Solomon codes are AG codes

Consider the projective curve $\mathcal{X}$ over $\mathbb{F}_q$ given by $z = 0$. The points in the curve are $(x : y : 0)$. Let $P_\infty = (1 : 0 : 0)$, $P_0 = (0 : 1 : 0)$ and $P_1, \ldots P_{q-1}$ the remaining rational points. For narrow sense RS codes we will let $n = q - 1$ and $\mathcal{P} = \{P_1, \ldots P_{q-1}\}$ and for the extended narrow-sense RS codes $n = q$ and $\mathcal{P} = \{P_0, \ldots P_{q-1}\}$.

Fix $k$ ($1 \leq k \leq n$) and let $D = (k - 1)P_\infty$ ($D = 0$ when $k = 1$). We have that $\text{supp}(D) \cap \mathcal{P} = \emptyset$ and $\mathcal{X}$ is non singular of genus $g = 0$. Also $k - 1 = \deg(D) > 2g - 2$ thus $\dim(L(D)) = \deg(D) + 1 - g = k$. 

Geometric Reed Solomon codes
Reed-Solomon codes are AG codes
Geometric Reed Solomon codes
Reed-Solomon codes are AG codes

$$\mathcal{B} = \left\{ 1, \frac{x}{y}, \frac{x^2}{y^2}, \ldots, \frac{x^{k-1}}{y^{k-1}} \right\}$$

is a basis of $L(D)$.
First \( \text{div}(x^j/y^j) = jP_0 - jP_\infty \), thus \( \text{div}(x^j/y^j) + D = jP_0 - (k-1-j)P_\infty \) which is effective since \( 0 \leq j \leq k-1 \).

Consider a linear combination of elements of \( \mathcal{B} \)

$$f = \sum_{j=0}^{k-1} a_j \frac{x^j}{y^j} \approx \chi 0.$$

\( f = g/h \) and by definition of \( \approx \), \( g \) must be a multiple of \( z \), clearly this multiple should be \( 0 \) since \( z \) does not appear on \( f \), therefore \( a_i = 0 \) for all \( i \).
Geometric Reed Solomon codes
Reed-Solomon codes are AG codes

\[ \mathcal{B} = \left\{ 1, \frac{x}{y}, \frac{x^2}{y^2}, \ldots \frac{x^{k-1}}{y^{k-1}} \right\} \]

is a basis of \( L(D) \).
First \( \text{div}(x^j/y^j) = jP_0 - jP_\infty \), thus \( \text{div}(x^j/y^j) + D = jP_0 - (k - 1 - j)P_\infty \) which is effective since \( 0 \leq j \leq k - 1 \).

Consider a linear combination of elements of \( \mathcal{B} \)

\[ f = \sum_{j=0}^{k-1} a_j \frac{x^j}{y^j} \approx \lambda \ 0. \]

\( f = g/h \) and by definition of \( \approx \), \( g \) must be a multiple of \( z \), clearly this multiple should be 0 since \( z \) does not appear on \( f \), therefore \( a_i = 0 \) for all \( i \).
Geometric Reed Solomon codes
Reed-Solomon codes are AG codes

Using $B$, any nonzero element $f \in L(D)$ can be written as

$$f(x, y, z) = \frac{g(x, y, z)}{y^d}, \quad g(x, y, z) = \sum_{j=0}^{d} g_j x^j y^{d-j}$$

with $g_d \neq 0$ and $d \leq k - 1$.

Notice that $g(x, y, z)$ is the homogenization in $\mathbb{F}_q[x, y]$ of $m(x) = \sum_{j=0}^{d} g_j x^j$ thus there is a 1-1 relation between the elements of $L(D)$ and those of $\mathcal{P}_k \subseteq \mathbb{F}_q[x]$. 
Using \( B \), any nonzero element \( f \in L(D) \) can be written as

\[
f(x, y, z) = \frac{g(x, y, z)}{y^d}, \quad g(x, y, z) = \sum_{j=0}^{d} g_j x^j y^{d-j}
\]

with \( g_d \neq 0 \) and \( d \leq k - 1 \).

Notice that \( g(x, y, z) \) is the homogenization in \( \mathbb{F}_q[x, y] \) of \( m(x) = \sum_{j=0}^{d} g_j x^j \) thus there is a 1-1 relation between the elements of \( L(D) \) and those of \( \mathcal{P}_k \subseteq \mathbb{F}_q[x] \).
Moreover, if $\beta \in \mathbb{F}_q$ then $m(\beta) = f(\beta, 1, 0)$ and additionally $f(\beta, 1, 0) = f(x_0, y_0, z_0)$ where $(\beta : 1 : 0) = (x_0 : y_0 : z_0)$.

Let $\alpha$ a primitive element of $\mathbb{F}_q$ and order the points $P_i = (\alpha^i : 1 : 0)$ for $1 \leq i \leq n$. The discussion shows that the following sets are the same

\[
\{(m(1), m(\alpha), \ldots, m(\alpha^{n-1})) \mid m(x) \in \mathcal{P}_k\}
\]

\[
\{(f(P_1), f(P_2), \ldots, f(P_n)) \mid f \in L(D)\}
\]

and by R-R theorem $\deg(D) + 1 - g = k - 1 + 1 + 0 = k$, $d \geq n - \deg(G) = n - k + 1$, hence by Singleton Bound $d = n - k + 1$ and they are MDS.
Geometric Reed Solomon codes
Reed-Solomon codes are AG codes

Moreover, if $\beta \in \mathbb{F}_q$ then $m(\beta) = f(\beta, 1, 0)$ and additionally $f(\beta, 1, 0) = f(x_0, y_0, z_0)$ where $(\beta : 1 : 0) = (x_0 : y_0 : z_0)$.

Let $\alpha$ a primitive element of $\mathbb{F}_q$ and order the points $P_i = (\alpha^i : 1 : 0)$ for $1 \leq i \leq n$. The discussion shows that the following sets are the same

$\{ (m(1), m(\alpha), \ldots, m(\alpha^{n-1})) \mid m(x) \in \mathcal{P}_k \}$

$\{ (f(P_1), f(P_2), \ldots, f(P_n)) \mid f \in L(D) \}$

and by R-R theorem $\deg(D) + 1 - g = k - 1 + 1 + 0 = k$, $d \geq n - \deg(G) = n - k + 1$, hence by Singleton Bound $d = n - k + 1$ and they are MDS.
Geometric Reed Solomon codes
Generalized Reed-Solomon codes are AG codes

As an exercise show that Generalized Reed-Solomon codes are AG codes using the discussion above and using the following steps:

1. Let \( \gamma = (\gamma_0, \ldots, \gamma_{n-1}) \) a \( n \)-tuple of distinct elements of \( \mathbb{F}_q \), and \( v = (v_0, \ldots, v_{n-1}) \in \mathbb{F}_q^n \). Compute the polynomial given by the Lagrange Interpolation Formula

\[
p(x) = \sum_{i=0}^{n-1} v_i \prod_{j \neq i} \frac{x - \gamma_j}{\gamma_i - \gamma_j}.
\]

2. Let \( \mathcal{X} \) be the curve defined by \( z = 0 \) and \( h(x, y) \) the homogenization of polynomial \( p(x) \) of degree \( d \leq n - 1 \). We will assume that the \( v_i \)'s are noncero, thus \( h \neq 0 \).
Geometric Reed Solomon codes
Generalized Reed-Solomon codes are AG codes

As an exercise show that Generalized Reed-Solomon codes are AG codes using the discussion above and using the following steps:

- Let \( \gamma = (\gamma_0, \ldots, \gamma_{n-1}) \) a \( n \)-tuple of distinct elements of \( \mathbb{F}_q \), and \( \mathbf{v} = (v_0, \ldots, v_{n-1}) \in \mathbb{F}_q^n \). Compute the polynomial given by the Lagrange Interpolation Formula

\[
p(x) = \sum_{i=0}^{n-1} v_i \prod_{j \neq i} \frac{x - \gamma_j}{\gamma_i - \gamma_j}.
\]

- Let \( \mathcal{X} \) be the curve defined by \( z = 0 \) and \( h(x, y) \) the homogenization of polynomial \( p(x) \) of degree \( d \leq n - 1 \). We will assume that the \( v_i \)'s are noncero, thus \( h \neq 0 \).
Geometric Reed Solomon codes
Generalized Reed-Solomon codes are AG codes

- Let \( u(x, y, z) = \frac{h(x, y)}{y^d} \in \mathbb{F}_q(\mathcal{X}) \) and 
  \( \mathcal{P} = \{ P_1, P_2, \ldots, P_n \} \) such that 
  \( P_i = (\gamma_{i-1} : 1 : 0) \), 
  \( P_\infty = (1 : 0 : 0) \) and 
  \( D = (k - 1)P_\infty - \text{div}(u) \).

- Prove that \( u(P_i) = \nu_{i-1} \).

- Prove that \( \text{supp}(D) \cap \mathcal{P} = \emptyset \).

- Since the divisor of any element in \( \mathbb{F}_q(\mathcal{X}) \) is cero then 
  \( \deg(D) = k - 1 \).

- Prove that a basis of \( L(D) \) is 
  \[ \mathcal{B} = \left\{ u, u \frac{x}{y}, u \frac{x^2}{y^2}, \ldots u \frac{x^{k-1}}{y^{k-1}} \right\} \]

- Prove that \( \mathcal{GRS}_k(\gamma, \nu) = \mathcal{C}(\mathcal{X}, \mathcal{P}, D) \).
Let $\mathcal{X} = \mathcal{F}_3(\mathbb{F}_4)$ the Fermat curve over $\mathbb{F}_4$ given by the eqn.

$$x^3 + y^3 + z^3 = 0$$

It has nine projective points given by

<table>
<thead>
<tr>
<th>$Q$</th>
<th>$P_1$</th>
<th>$P_2$</th>
<th>$P_3$</th>
<th>$P_4$</th>
<th>$P_5$</th>
<th>$P_6$</th>
<th>$P_7$</th>
<th>$P_8$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>$\alpha$</td>
<td>$\bar{\alpha}$</td>
<td>1</td>
<td>$\alpha$</td>
</tr>
<tr>
<td>1</td>
<td>$\alpha$</td>
<td>$\bar{\alpha}$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

where $\bar{\alpha} = \alpha^2 = 1 + \alpha$. 

AG codes : E. Martínez-Moro (SINGACOM-UVa)
Let $\mathcal{X} = \mathcal{F}_3(\mathbb{F}_4)$ the Fermat curve over $\mathbb{F}_4$ given by the eqn.

$$x^3 + y^3 + z^3 = 0$$

It has nine projective points given by

<table>
<thead>
<tr>
<th>$Q$</th>
<th>$P_1$</th>
<th>$P_2$</th>
<th>$P_3$</th>
<th>$P_4$</th>
<th>$P_5$</th>
<th>$P_6$</th>
<th>$P_7$</th>
<th>$P_8$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>$\alpha$</td>
<td>$\bar{\alpha}$</td>
<td>1</td>
<td>$\alpha$</td>
<td>$\bar{\alpha}$</td>
</tr>
<tr>
<td>1</td>
<td>$\alpha$</td>
<td>$\bar{\alpha}$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

where $\bar{\alpha} = \alpha^2 = 1 + \alpha$. 
Geometric Reed Solomon codes
A worked example

By R-R’s theorem $\dim(L(3Q)) = 3$. The functions

$$1, \frac{x}{x+y}, \frac{y}{y+z}$$

are regular outside $Q$ and have a pole of order 2 and 3 respectively. They are a basis of $L(D)$.

A generator matrix of $C(\mathcal{X}, \mathcal{P}, D)$ is

$$G = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & \tilde{\alpha} & 1 & \alpha & \tilde{\alpha} & \alpha & \tilde{\alpha} \\
\tilde{\alpha} & \alpha & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{pmatrix}$$

and by R-R $d \geq 5$ but having a look to $G$ clearly $d = 5$. 
Geometric Reed Solomon codes
A worked example

By R-R’s theorem $\dim(L(3Q)) = 3$. The functions

$$1, \frac{x}{x+y}, \frac{y}{y+z}$$

are regular outside $Q$ and have a pole of order 2 and 3 respectively. They are a basis of $L(D)$.

A generator matrix of $C(\mathcal{X}, \mathcal{P}, D)$ is

$$G = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & \alpha & \alpha & 1 & \alpha & \bar{\alpha} \\
\alpha & \bar{\alpha} & 0 & 0 & 0 & 1 & 1 & 1
\end{pmatrix}$$

and by R-R $d \geq 5$ but having a look to $G$ clearly $d = 5$. 
Geometric Goppa Codes
Differentials

Let $V$ be a vector space over $\mathbb{F}(\mathcal{X})$. An $\mathbb{F}$-linear map $D : \mathbb{F}(\mathcal{X}) \to V$ is called a derivation if it satisfies the product rule

$$D(fg) = fD(g) + gD(f).$$

**Example**

Let $\mathcal{X}$ be the projective line with function field $\mathbb{F}(x)$. Define $D(F) = \sum ia_i x^{i-1}$ for a polynomial $F = \sum a_i x^i \in \mathbb{F}[x]$ and extend this to quotients by

$$D \left( \frac{F}{G} \right) = \frac{GD(F) - FD(G)}{G^2}.$$

Then $D : \mathbb{F}(x) \to \mathbb{F}(x)$ is a derivation.
Let $\mathcal{V}$ be a vector space over $\mathbb{F}(x)$. An $\mathbb{F}$-linear map $D : \mathbb{F}(x) \to \mathcal{V}$ is called a derivation if it satisfies the product rule:

$$D(fg) = fD(g) + gD(f).$$

**Example**

Let $\mathcal{X}$ be the projective line with function field $\mathbb{F}(x)$. Define $D(F) = \sum ia_i x^{i-1}$ for a polynomial $F = \sum a_i x^i \in \mathbb{F}[x]$ and extend this to quotients by

$$D\left(\frac{F}{G}\right) = \frac{GD(F) - FD(G)}{G^2}$$

Then $D : \mathbb{F}(x) \to \mathbb{F}(x)$ is a derivation.
Geometric Goppa Codes

Local ring at a point

The set of all derivations $D : \mathbb{F}(\mathcal{X}) \to \mathcal{V}$ will be denoted by $\text{Der}(\mathcal{X}, \mathcal{V})$ (or $\text{Der}(\mathcal{X})$ if $\mathcal{V} = \mathbb{F}(\mathcal{X})$). Notice that $\text{Der}(\mathcal{X}, \mathcal{V})$ is a $\mathbb{F}(\mathcal{X})$-vector space.

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

The set of all the regular rational functions at $P$ will be denoted by $\mathcal{O}_P(\mathcal{X})$, the local ring at $P$ and indeed it is a local ring, i.e. it has a unique maximal ideal, given by

$$\mathcal{M}_P = \{ f \in \mathcal{O}_P(\mathcal{X}) \mid f(P) = 0 \} \quad (27)$$
The set of all derivations $D : \mathbb{F}(\mathcal{X}) \rightarrow \mathcal{V}$ will be denoted by $\text{Der}(\mathcal{X}, \mathcal{V})$ (or $\text{Der}(\mathcal{X})$ if $\mathcal{V} = \mathbb{F}(\mathcal{X})$). Notice that $\text{Der}(\mathcal{X}, \mathcal{V})$ is a $\mathbb{F}(\mathcal{X})$-vector space.

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

The set of all the regular rational functions at $P$ will be denoted by $\mathcal{O}_P(\mathcal{X})$, the local ring at $P$ and indeed it is a local ring, i.e. it has a unique maximal ideal, given by

$$\mathcal{M}_P = \{ f \in \mathcal{O}_P(\mathcal{X}) \mid f(P) = 0 \} \quad (27)$$
Example

In \( \mathbb{P}^2(\mathbb{F}) \) consider the parabola \( \mathcal{X} \) defined by \( XZ - Y^2 = 0 \). It has one point at infinity \( P_\infty = (1 : 0 : 0) \). The function \( x/y \) is equal to \( y/z \) on the curve, hence it is regular in the point \( P = (0 : 0 : 1) \).

\[
\frac{(2xz+z^2)}{(y^2+z^2)} \quad \text{is regular in } P \quad \text{and this function is equal to} \quad \frac{(2x+z)}{(x+z)}
\]

and therefore also regular in \( P_\infty \).
Example

In \( \mathbb{P}^2(\mathbb{F}) \) consider the parabola \( \mathcal{C} \) defined by \( XZ - Y^2 = 0 \). Now with it has one point at infinity \( P_\infty = (1 : 0 : 0) \). The function \( x/y \) is equal to \( y/z \) on the curve, hence it is regular in the point \( P = (0 : 0 : 1) \).

\[
\frac{(2xz + z^2)}{(y^2 + z^2)}
\]
is regular in \( P \) and this function is equal to \( \frac{(2x + z)}{(x + z)} \) and therefore also regular in \( P_\infty \).
Let see that $\mathcal{M}_P$ is generated by a single element (i.e. is a principal ideal). Let $\mathcal{X}$ be a smooth curve in $\mathbb{A}^2(F)$ defined by the equation $f = 0$, and let $P = (a, b)$ be a point on it.

$$\mathcal{M}_P = \langle x - a, y - b \rangle \text{ and } f_x(P)(x - a) + f_y(P)(y - b) \equiv 0 \mod \mathcal{M}^2_P$$

The $F$-vector space $\mathcal{M}_P/\mathcal{M}^2_P$ has dimension 1 and therefore $\mathcal{M}_P$ has one generator. Let $g \in F[x]$ 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 $d_P f$, where

$$d_P f = f_x(a, b)(x - a) + F_y(a, b)(y - b).$$
Geometric Goppa Codes
Local parameters

Let see that $\mathcal{M}_P$ is generated by a single element (i.e. is a principal ideal). Let $\mathcal{X}$ be a smooth curve in $\mathbb{A}^2(\mathbb{F})$ defined by the equation $f = 0$, and let $P = (a, b)$ be a point on it.

$$\mathcal{M}_P = \langle x - a, y - b \rangle \text{ and } f_x(P)(x - a) + f_y(P)(y - b) \equiv 0 \mod \mathcal{M}_P^2$$

The $\mathbb{F}$-vector space $\mathcal{M}_P/\mathcal{M}_P^2$ has dimension 1 and therefore $\mathcal{M}_P$ has one generator. Let $g \in \mathbb{F}[x]$ 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 $d_P f$, where

$$d_P f = f_x(a, b)(x - a) + F_y(a, b)(y - b).$$
Let $< t > = M_P$, and $z \in \mathcal{O}_P(\mathcal{X})$, then it can be written in a unique way as

$$z = ut^m,$$

where $u$ is a unit and $m \in \mathbb{N}_0$. The function $t$ is called a local parameter or uniformizing parameter in $P$.

If $m > 0$, then $P$ is a zero of multiplicity $m$ of $z$. We write $m = \text{ord}_P(z) = \nu_P(z)$. ($\nu_P(0) = \infty$).
Theorem

Let $< t > = M_P$ a local parameter for $t$, then there exists a unique derivation

$$D_t : \mathbb{F}(\mathcal{X}) \to \mathbb{F}(\mathcal{X}) \text{ s.t. } D_t(t) = 1,$$

(28)

Moreover, $\text{Der}(\mathcal{X})$ is one dimensional over $\mathbb{F}(\mathcal{X})$ and $D_t$ is a basis element.

A rational differential form or differential on $\mathcal{X}$ is an $\mathbb{F}(\mathcal{X})$ linear map from $\text{Der}(\mathcal{X})$ to $\mathbb{F}(\mathcal{X})$. The set of all rational differential forms on $\mathcal{X}$ is denoted by $\Omega(\mathcal{X})$. 
Theorem

Let \( \langle t \rangle = \mathcal{M}_P \) a local parameter for \( t \), then there exist a unique derivation

\[
D_t : \mathbb{F}(\mathcal{X}) \rightarrow \mathbb{F}(\mathcal{X}) \text{ s.t. } D_t(t) = 1, \tag{28}
\]

Moreover, \( \text{Der}(\mathcal{X}) \) is one dimensional over \( \mathbb{F}(\mathcal{X}) \) and \( D_t \) is a basis element.

A rational differential form or differential on \( \mathcal{X} \) is an \( \mathbb{F}(\mathcal{X}) \) linear map from \( \text{Der}(\mathcal{X}) \) to \( \mathbb{F}(\mathcal{X}) \). The set of all rational differential forms on \( \mathcal{X} \) is denoted by \( \Omega(\mathcal{X}) \).
Consider the map \( d : \mathbb{F}(\mathcal{X}) \to \Omega(\mathcal{X}) \) given by for each \( f \in \mathbb{F}(\mathcal{X}) \) the image \( df : \text{Der}(\mathcal{X}) \to \mathbb{F}(\mathcal{X}) \) is defined by \( df(D) = D(f) \) for all \( D \in \text{Der}(\mathcal{X}) \). Then \( d \) is a derivation. and provides to \( \Omega(\mathcal{X}) \) a vector space structure over \( \mathbb{F}(\mathcal{X}) \).

**Theorem**

The space \( \Omega(\mathcal{X}) \) has dimension 1 over \( \mathbb{F}(\mathcal{X}) \) and \( dt \) is a basis for every point \( P \in \mathcal{X} \) with local parameter \( t \).
Consider the map $d : \mathbb{F}(\mathcal{X}) \to \Omega(\mathcal{X})$ given by for each $f \in \mathbb{F}(\mathcal{X})$ the image $df : \text{Der}(\mathcal{X}) \to \mathbb{F}(\mathcal{X})$ is defined by $df(D) = D(f)$ for all $D \in \text{Der}(\mathcal{X})$. Then $d$ is a derivation. and provides to $\Omega(\mathcal{X})$ a vector space structure over $\mathbb{F}(\mathcal{X})$.

**Theorem**

The space $\Omega(\mathcal{X})$ has dimension 1 over $\mathbb{F}(\mathcal{X})$ and $dt$ is a basis for every point $P \in \mathcal{X}$ with local parameter $t$. 
That is, for each differential we have a unique representation \( \omega = f_P dt_P \), where \( f_P \) is a rational function at point \( P \). We can not evaluate \( P \) at \( \omega \) as by \( \omega(P) = f_P(P) \) since it depends on the choice of \( t_P \).

Let \( \omega \in \Omega(X) \). The order or valuation of \( \omega \) in \( P \) is defined by \( \text{ord}_P(\omega) = v_P(\omega) := v_P(f_P) \). It is called regular if it has no poles. This definition does not depend on the choices made.

The canonical divisor \( (\omega) \) of the differential \( \omega \) is defined by

\[
W = (\omega) = \sum_{P \in X} v_P(\omega) P. \tag{29}
\]

If \( D \) is a divisor, \( \Omega(D) = \{ \omega \in \Omega(X) \mid (\omega) - D \succeq 0 \} \).
That is, for each differential we have a unique representation \( \omega = f_P dt_P \), where \( f_P \) is a rational function at point \( P \). We can not evaluate \( P \) at \( \omega \) as by \( \omega(P) = f_P(P) \) since it depends on the choice of \( t_P \).

Let \( \omega \in \Omega(X) \). The order or valuation of \( \omega \) in \( P \) is defined by \( \text{ord}_P(\omega) = \nu_P(\omega) := \nu_P(f_P) \). It is called regular if it has no poles. This definition does not depend on the choices made.

The canonical divisor \( (\omega) \) of the differential \( \omega \) is defined by

\[
W = (\omega) = \sum_{P \in X} \nu_P(\omega)P.
\]

If \( D \) is a divisor, \( \Omega(D) = \{ \omega \in \Omega(X) \mid (\omega) - D \geq 0 \} \).
That is, for each differential we have a unique representation $\omega = f_P dt_P$, where $f_P$ is a rational function at point $P$. We can not evaluate $P$ at $\omega$ as by $\omega(P) = f_P(P)$ since it depends on the choice of $t_P$.

Let $\omega \in \Omega(\mathcal{X})$. The order or valuation of $\omega$ in $P$ is defined by $\operatorname{ord}_P(\omega) = \nu_P(\omega) := \nu_P(f_P)$. It is called regular if it has no poles. This definition does not depend on the choices made.

The canonical divisor $(\omega)$ of the differential $\omega$ is defined by

$$W = (\omega) = \sum_{P \in \mathcal{X}} \nu_P(\omega) P. \quad (29)$$

If $D$ is a divisor, $\Omega(D) = \{\omega \in \Omega(\mathcal{X}) \mid (\omega) - D \geq 0\}$. 
Let \( P \in \mathcal{X} \) and \( t \) is a local parameter, let \( \omega = fd_t \) a differential form, \( f = \sum a_i t^i \), then the residue at point \( P \) is defined as

\[
\text{Res}_P(\omega) = a_{-1}.
\]

As usual, let \( D \) be a divisor on \( \mathcal{X} \) and choose a set \( \mathcal{P} = \{P_1, \ldots, P_n\} \) of \( n \) distinct \( \mathbb{F}_q \)-rational points on \( \mathcal{X} \) such that \( \text{supp}(D) \cap \mathcal{P} = \emptyset \).

The linear code \( \mathcal{C}^*(\mathcal{P}, D) \) of length \( n \) over \( \mathbb{F}_q \) is the image of the linear map \( \alpha^* : \omega(\sum P_i - D) \to \mathbb{F}_q^n \) defined by

\[
\alpha^*(\eta) = (\text{Res}_{P_1}(\eta), \text{Res}_{P_2}(\eta), \ldots, \text{Res}_{P_n}(\eta)).
\]
Let \( P \in \mathcal{X} \) and \( t \) is a local parameter, let \( \omega = f dt \) a differential form , \( f = \sum a_i t^i \), then the residue at point \( P \) is defined as

\[
\text{Res}_P(\omega) = a_{-1}.
\]

As usual, Let \( D \) be a divisor on \( \mathcal{X} \) and choose a set \( \mathcal{P} = \{P_1, \ldots, P_n\} \) of \( n \) distinct \( \mathbb{F}_q \)-rational points on \( \mathcal{X} \) such that \( \text{supp}(D) \cap \mathcal{P} = \emptyset \).

The linear code \( \mathcal{C}^*(\mathcal{P}, D) \) of length \( n \) over \( \mathbb{F}_q \) is the image of the linear map \( \alpha^* : \omega(\sum P_i - D) \to \mathbb{F}_q^n \) defined by

\[
\alpha^*(\eta) = (\text{Res}_{P_1}(\eta), \text{Res}_{P_2}(\eta), \ldots, \text{Res}_{P_n}(\eta)).
\]
Theorem

The code $C^*(\mathcal{P}, D)$ has dimension $k^* = n - \deg(D) + g - 1$ and minimum distance $d^* \geq \deg(D) - 2g + 2$.

The proof follows from Riemann-Roch’s theorem and the isomorphisms between $L(W - D)$ and $\Omega(D)$.

Theorem

The codes $C^*(\mathcal{P}, D)$ and $C(\mathcal{P}, D)$ are dual codes.

The proof follows from the residue theorem that states $\sum_{P \in \mathcal{X}} \text{Res}_P(\omega) = 0$. 

AG codes : E. Martínez-Moro (SINGACOM-UVa)
The code $C^*(P, D)$ has dimension $k^* = n - \deg(D) + g - 1$ and minimum distance $d^* \geq \deg(D) - 2g + 2$.

The proof follows from Riemann-Roch's theorem and the isomorphisms between $L(W - D)$ and $\Omega(D)$.

Theorem

The codes $C^*(P, D)$ and $C(P, D)$ are dual codes.

The proof follows from the residue theorem that states

$$\sum_{P \in \mathcal{X}} \text{Res}_P(\omega) = 0.$$
Geometric Goppa Codes
Geometric Goppa Codes are evaluation codes

Theorem

Let $\mathcal{X}$ be a curve defined over $\mathbb{F}_q$. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ rational points on $\mathcal{X}$. Then there exists a differential form $\omega$ with simple poles at the $P_i$ such that $\text{Res}_{P_i}(\omega) = 1$ for all $i$. Furthermore

$$C^*(\mathcal{P}, D) = C(\mathcal{P}, W + \sum P_i - D)$$

for all divisors $D$ that have a support disjoint from $\mathcal{P}$, where $W$ is the divisor of $\omega$. 
AG codes

E. Martínez-Moro

History

$\mathbb{A}^n(F), \mathbb{P}^n(F)$

Classical codes

Generalized RS
Goppa
Reed-Muller

Curves

Examples
Degree & multiplicity
Bézout and Plücker

AG codes

Rational functions
$L(D)$
Evaluation
GRS are AG
Differentials and dual

GV bound

Goppa meet
AG exceed
AG codes

E. Martínez-Moro

History

$\mathbb{A}^n(F), \mathbb{P}^n(F)$

Classical codes

Generalized RS
Goppa
Reed-Muller

Curves

Examples
Degree & multiplicity
Bézout and Plücker

AG codes

Rational functions
$L(D)$
Evaluation
GRS are AG
Differentials and dual

GV bound

Goppa meet
AG exceed
Further topics and reading