Algebraic geometry codes and their parameters

Ruud Pellikaan
Technical University of Eindhoven

Soria Summer School
on Computational Mathematics
July 8, 2008

Content:

§4 Divisors
§5 Differentials on a curve
§6 The Riemann-Roch theorem
§7 Codes from algebraic curves

Sections 2.4, 2.5, 2.6 and 2.7 from:
Algebraic geometry codes
by T. Høholdt, J.H. van Lint and R. Pellikaan
in Handbook of Coding Theory, vol 1, pp. 871-961
V.S. Pless and W.C. Huffman eds., Elsevier, Amsterdam 1998.

http://www.win.tue.nl/ ruudp/paper/31.pdf
http://www.win.tue.nl/ ruudp/lectures/slides2-AGC-Soria.pdf

§4 Divisors

In the following, $\mathcal{X}$ is an irreducible,
nonsingular, projective plane curve.

A **divisor** is a formal sum

$$D = \sum_{P \in X} n_P P,$$

with $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but a finite number of points $P \in \mathcal{X}$.

The **support** of this divisor is the set

$$\{\, P \mid n_P \neq 0 \,\}.$$

Let $E = \sum_{P \in X} m_P P$ be another divisor. Define

$$D \leq E \Leftrightarrow n_p \leq m_P \text{ for all } P.$$

A divisor D is called **effective** if

$$0 \leq D,$$

that is if all coefficients n_P are nonnegative.

Define the **degree** of the divisor D by

$$\deg(D) = \sum n_P.$$

Let $\mathcal{X}$ and $\mathcal{Y}$ be projective plane curves defined by the equations $F = 0$ and $G = 0$ of degrees l and m.

Define the **intersection divisor** by

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

where $I(P; \mathcal{X}, \mathcal{Y})$ is the intersection multiplicity.

Bézout's theorem tells us that $\mathcal{X} \cdot \mathcal{Y}$
is indeed a divisor and

$$\deg(\mathcal{X} \cdot \mathcal{Y}) = lm.$$

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

Let v_P be the discrete valuation defined for functions on $\mathcal{X}$.

Let f be a nonzero rational function on $\mathcal{X}$.
Define the **divisor of** f by

$$(f) = \sum_{P \in X} v_P(f) P$$

The divisor of f is a bookkeeping device that tells us
where the zeros and poles of f are and what their multiplicities are.

Theorem

$$\deg(f) = 0$$

The degree of a divisor of a nonzero rational function is zero.

Proof

Let $\mathcal{X}$ be a plane curve of degree l.
Let f be a rational function on the curve $\mathcal{X}$.
Then f is represented by a quotient A/B of
two homogeneous polynomials of the same degree, say m.

Let $\mathcal{Y}$ and $\mathcal{Z}$ be the curves defined by the equations $A = 0$ and $B = 0$. Then

$$v_P(f) = I(P; \mathcal{X}, \mathcal{Y}) - I(P; \mathcal{X}, \mathcal{Z}),$$

since

$$f = a/b = (a/h^m)(b/h^m)^{-1},$$

where H is a homogeneous linear form representing h such that $H(P) \neq 0$. Hence

$$(f) = \mathcal{X} \cdot \mathcal{Y} - \mathcal{X} \cdot \mathcal{Z}.$$

So (f) is a divisor and its degree is zero, since it is the difference of two intersection divisors of the same degree lm.

Example

Consider the plane curve $\mathcal{X}$ with equation over $\mathbb{F}_4$

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

Let $Q = (0 : 1 : 1)$. Take $t = x/z$ as local parameter at Q.

We saw that

$$v_Q(x/(y+z)) = -2.$$

Let $\alpha \in \mathbb{F}_4$ with $\alpha^2 = 1 + \alpha$.

The line $\mathcal{L}$ with equation $X = 0$ intersects the curve in three points:

$$P_1 = (0 : \alpha : 1),\ P_2 = (0 : \alpha^2 : 1) \text{ and } Q.$$

So

$$\mathcal{X} \cdot \mathcal{L} = P_1 + P_2 + Q.$$

The line $\mathcal{M}$ with equation $Y = 0$ intersects the curve in three points:

$$P_3 = (1 : 0 : 1),\ P_4 = (\alpha : 0 : 1) \text{ and } P_5 = (\alpha^2 : 0 : 1).$$

So

$$\mathcal{X} \cdot \mathcal{M} = P_3 + P_4 + P_5.$$

The line $\mathcal{N}$ with equation $Y + Z = 0$ intersects the curve in Q with multiplicity 3. So

$$\mathcal{X} \cdot \mathcal{N} = 3Q.$$

Hence

$$(x/(y+z) = P_1 + P_2 - 2Q$$

and

$$(y/(y+z) = P_3 + P_4 + P_5 - 3Q.$$

Example

Let $\mathcal{X}$ be the Klein quartic with equation

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

Let

$$P_1 = (1:0:0),\ P_2 = (0:1:0) \text{ and } P_3 = (0:0:1).$$

Let $\mathcal{L}$ be the line with equation $X = 0$.
Then $\mathcal{L}$ intersects $\mathcal{X}$ in the points

$$P_2 \text{ and } P_3.$$

The line $\mathcal{L}$ is not tangent in P_2, so

$$I(P_2; \mathcal{X}, \mathcal{L}) = 1 \text{ and } I(P_3; \mathcal{X}, \mathcal{L}) = 3,$$

since the multiplicities add up to 4.
Hence

$$\mathcal{X} \cdot \mathcal{L} = P_2 + 3P_3.$$

$$\mathcal{X} \cdot \mathcal{L} = P_2 + 3P_3.$$

Similarly we get for the lines $\mathcal{M}$ and $\mathcal{N}$ with equations $Y = 0$ and $Z = 0$

$$\mathcal{X} \cdot \mathcal{M} = 3P_1 + P_3 \text{ and } \mathcal{X} \cdot \mathcal{N} = 3P_2 + P_1.$$

Therefore

$$(x/z) = 3P_3 - P_1 - 2P_2$$

and

$$(y/z) = 2P_1 + P_3 - 3P_2.$$

The divisor of a rational function is called a **principal divisor**.

Two divisors D and E are called **linearly equivalent**
if and only if $D - E$ is a principal divisor, that is

$$D - E = (f)$$

for some rational function f.

Notation

$$D \equiv E.$$

This is indeed an equivalence relation.

Let D be a divisor on a curve $\mathcal{X}$.

Define the vector space $\mathcal{L}(D)$ over $\mathbb{F}$ by

$$\mathcal{L}(D) = \{f \in \mathbb{F}(\mathcal{X})^* \mid (f) + D \geq 0\} \cup \{0\}.$$

Define

$$l(D) = \dim_{\mathbb{F}} \mathcal{L}(D).$$

If

$$D = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$$

with all $n_i, m_j > 0$, then $\mathcal{L}(D)$ consists of 0 and the rational functions that have

zeros of order at least m_j at Q_j

poles of order at most n_i at P_i

and no other poles.

If $D \equiv E$ and g is a rational function with

$(g) = D - E$, then the map

$$f \mapsto fg$$

shows that

$$\mathcal{L}(D) \cong \mathcal{L}(E)$$

as vector spaces over $\mathbb{F}$.

Theorem

(i) $l(D) = 0 \quad$ if $deg(D) < 0$,

(ii) $l(D) \leq 1 + deg(D)$.

Proof

(i) If $\deg(D) < 0$, then for any function f,
we have $\deg(f) + D) < 0$, so $f \notin \mathcal{L}(D)$.

(ii) If f is not 0 and $f \in \mathcal{L}(D)$, then

$$E := D + (f)$$

is an effective divisor for which

$$D \equiv E \text{ so } l(D) = l(E).$$

So we may assume that D is effective, say

$$D = \sum_{i=1}^{r} n_i P_i,$$

where $n_i \geq 0$ for all i.

Let $f \neq 0$ and $f \in \mathcal{L}(D)$.
Let t_i be a local parameter at P_i.
Map f onto the corresponding element in

$$(t_i^{-n_i}\mathcal{O}_{P_i})/\mathcal{O}_{P_i},$$

This space has dimension n_i.

Thus we obtain a mapping

$$\mathcal{L}(D) \to \oplus_{i=1}^{r}(t_i^{-n_i}\mathcal{O}_{P_i})/\mathcal{O}_{P_i}.$$

This is a linear mapping.

Suppose that f is in the kernel.
This means that f does not have a pole in all the points P_i, that is to say, f is a constant function. It follows that

$$l(D) \leq 1 + \sum_{i=1}^{r} n_i = 1 + \deg(D).$$

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

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

as before. We saw that

$$(x/(y+z) = P_1 + P_2 - 2Q$$

and

$$(y/(y+z) = P_3 + P_4 + P_5 - 3Q.$$

Let $f = x/(y+z)$ and $g = y/(y+z)$.

So the functions 1, f and g have
mutually distinct pole orders at Q and
are linearly independent elements of $\mathcal{L}(3Q)$.

Hence

$$3 \leq l(3Q) \leq 1 + 3.$$

We will see that $l(3Q) = 3$.

§5 Differentials on a curve

Let $\mathcal{X}$ be an irreducible smooth curve with function field $\mathbb{F}(\mathcal{X})$.

Let $\mathcal{V}$ be a vector space over $\mathbb{F}(\mathcal{X})$.
An $\mathbb{F}$-linear map

$$D : \mathbb{F}(\mathcal{X}) \to \mathcal{V}$$

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 $D(F) = \sum ia_iX^{i-1}$ for a polynomial $F = \sum a_iX^i \in \mathbb{F}[X]$

and extend this definition to quotients by

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

Then $D : \mathbb{F}(X) \to \mathbb{F}(X)$ is a derivation.

Denote the set of all derivations $D : \mathbb{F}(\mathcal{X}) \to \mathcal{V}$ by

$$Der(\mathcal{X}, \mathcal{V}).$$

Denote $Der(\mathcal{X}, \mathcal{V})$ by $Der(\mathcal{X})$ if $\mathcal{V} = \mathbb{F}(\mathcal{X})$.

Define **sum** of two derivations $D_1, D_2 \in Der(\mathcal{X}, \mathcal{V})$ by $(D_1 + D_2)(f) = D_1(f) + D_2(f)$.

Define the **product** of $f \in \mathbb{F}(\mathcal{X})$ and $D \in Der(\mathcal{X}, \mathcal{V})$ by $(fD)(g) = fD(g)$.

In this way $Der(\mathcal{X}, \mathcal{V})$ becomes a vector space over $\mathbb{F}(\mathcal{X})$.

Theorem

Let t be a local parameter at a point P.

Then there exists a unique derivation

$D_t : \mathbb{F}(\mathcal{X}) \to \mathbb{F}(\mathcal{X})$ such that $D_t(t) = 1$.

Furthermore $Der(\mathcal{X})$ is one dimensional over $\mathbb{F}(\mathcal{X})$ and

D_t is a basis element for every local parameter t.

A **rational differential form** or **differential** on $\mathcal{X}$

is an $\mathbb{F}(\mathcal{X})$-linear map from $Der(\mathcal{X})$ to $\mathbb{F}(\mathcal{X})$.

The set of all rational differential forms on $\mathcal{X}$ is denoted by

$$\Omega(\mathcal{X}).$$

Again $\Omega(\mathcal{X})$ becomes a vector space over $\mathbb{F}(\mathcal{X})$ in the obvious way.

Consider the map

$$d : \mathbb{F}(\mathcal{X}) \longrightarrow \Omega(\mathcal{X}),$$

where for $f \in \mathbb{F}(\mathcal{X})$ the differential

$$df : Der(\mathcal{X}) \to \mathbb{F}(\mathcal{X})$$

is defined by $df(D) = D(f)$ for all $D \in Der(\mathcal{X})$.

Then d is a derivation.

Theorem

The space $\Omega(\mathcal{X})$ has dimension 1 over $\mathbb{F}(\mathcal{X})$

and dt is a basis for every point P with local parameter t.

So for every point P and local parameter t_P at P,
a differential ω can be represented in a unique way as

$$\omega = f_P \, dt_P,$$

where f_P is a rational function.

The obvious definition for "the value " of ω in P by
$\omega(P) = f_P(P)$ has no meaning, since it depends on the choice of t_P.

Despite of this negative result it is possible to say whether ω
has a pole or a zero at P of a certain order.

Let ω be a differential on $\mathcal{X}$.
The **order** or **valuation** of ω in P is defined by

$$\mathrm{ord}_P(\omega) = v_P(\omega) = v_P(f_P).$$

This definition does not depend on the choices made.

The differential form ω is called **regular** if it has no poles.

The regular differentials on $\mathcal{X}$ form an $\mathbb{F}[\mathcal{X}]$-module denoted by

$$\Omega[\mathcal{X}].$$

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

Then $\Omega[\mathcal{X}]$ is generated by dx and dy as an $\mathbb{F}[\mathcal{X}]$-module

with the relation

$$f_x dx + f_y dy = 0.$$

Example

Consider the projective curve $\mathcal{X}$ given by $X^3 + Y^3 + Z^3 = 0$
in characteristic not equal to three.

Define the set U_x by $U_x = \{(x : y : z) \in \mathcal{X} \mid y \neq 0, z \neq 0\}$
and similarly U_y and U_z.

Then U_x, U_y, and U_z cover $\mathcal{X}$, since there is no point on $\mathcal{X}$
where two coordinates are zero.

The only regular functions on $\mathcal{X}$ are constants, so one cannot represent this differential as $g\,df$ with f and g regular functions on $\mathcal{X}$.

The three representations

$$\omega = \left(\frac{y}{z}\right)^2 d\left(\frac{x}{y}\right) \text{ on } U_x, \quad \eta = \left(\frac{z}{x}\right)^2 d\left(\frac{y}{z}\right) \text{ on } U_y,$$

$$\zeta = \left(\frac{x}{y}\right)^2 d\left(\frac{z}{x}\right) \text{ on } U_z$$

define the same differential on $\mathcal{X}$.

To show that η and ζ agree on $U_y \cap U_z$ consider the equation

$$(x/z)^3 + (y/z)^3 + 1 = 0,$$

differentiate, and apply the formula $d(f^{-1}) = -f^{-2}\,df$ to $f = z/x$.

The divisor of a differential is defined as for functions.

The divisor (ω) of the differential ω is defined by

$$(\omega) = \sum_{P \in \mathcal{X}} v_P(\omega) P.$$

Only finitely many coefficients in (ω) are not zero.

Let ω be a differential with divisor $W = (\omega)$.

Then W is called a **canonical divisor**.

If ω' is another nonzero differential,
then $\omega' = f\omega$ for some rational function f.

So

$$(\omega') = W' \equiv W.$$

Therefore the canonical divisors form one linear equivalence class.
This class is also denoted by W.

Consider the space $\mathcal{L}(W)$.

This space of rational functions can be mapped onto an isomorphic space of differential forms by $f \mapsto f\omega$.

By the definition of $\mathcal{L}(W)$, the image of f under this mapping
is a regular differential form,
and every regular differential form is obtained in this way.

Hence $\mathcal{L}(W)$ is isomorphic to $\Omega[X]$.

Define the **genus** g of $\mathcal{X}$ by $g = l(W)$.

Example

Consider the differential dx on the projective line.

Then dx is regular at all points $P_a = (a : 1)$,
since $x - a$ is a local parameter in P_a and $dx = d(x - a)$.

Let $Q = (1 : 0)$ be the point at infinity.
Then $t = 1/x$ is a local parameter in Q and $dx = -t^{-2}dt$.

So $v_Q(dx) = -2$. Hence

$$(dx) = -2Q$$

and $l(-2Q) = 0$.

Therefore the projective line has genus zero.

The genus of a curve plays an important role in the following.

We mention one formula without proof, the so-called **Plücker formula**.

Theorem

Let $\mathcal{X}$ be a nonsingular projective curve of degree m in $\mathbb{P}^2$.

Then

$$g = \frac{1}{2}(m-1)(m-2).$$

The genus of a line and a nonsingular conic are zero by Plücker.

In fact a curve of genus zero is isomorphic to the projective line.

For example the curve $\mathcal{X}$ with equation $XZ - Y^2 = 0$
is isomorphic to $\mathbb{P}^1$, where the isomorphism is given by

$$(x : y : z) \mapsto (x : y) = (y : z)$$

for $(x : y : z) \in \mathcal{X}$.

The inverse map is given by $(u : v) \mapsto (u^2 : uv : v^2)$.

Example

Nonsingular projective cubic plane curves have genus 1.

So $\mathcal{L}(W) = \mathbb{F}$, by the definition of genus.

Hence nonzero regular differentials on $\mathcal{X}$ are
scalar multiples of each other.

For the construction of codes over algebraic curves that generalize **Goppa codes**, we need the concept of residue of a differential at a point P.

Let P be a point on $\mathcal{X}$ and t a local parameter at P and $\omega = f\,dt$ the representation of ω.

The function f can be written as

$$f = \sum_i a_i t^i.$$

Define the **residue** of ω at the point P by

$$\mathrm{Res}_P(\omega) = a_{-1}.$$

This does not depend on the choice of the local parameter t.

One of the basic results in the theory of algebraic curves is known as the **residue theorem**. We state it without proof.

Theorem

Let ω be a differential on a nonsingular projective curve $\mathcal{X}$.

Then

$$\sum_{P \in X} \mathrm{Res}_P(\omega) = 0.$$

§6 **Theorem of Riemann-Roch**

Let$\mathcal{X}$ be a nonsingular projective curve of genus g.

Let D be a divisor on $\mathcal{X}$.

Then, for any canonical divisor W

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

We do not give a proof.

The degree of a canonical divisor W is $2g - 2$.

Corollary $\deg(W) = 2g - 2$.

The degree of a canonical divisor W is $2g - 2$.

Proof

Everywhere regular functions on a projective curve are constant, that is to say, $\mathcal{L}(0) = \mathbb{F}$, so $l(0) = 1$.

Substitute $D = W$ in the Theorem of Riemann-Roch and the result follows from the definition of genus: $g = l(W)$.

Corollary

Let $\mathcal{X}$ be an irreducible, nonsingular projective curve of genus g.

Let D be a divisor on $\mathcal{X}$.

Then

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

and equality holds if $\deg(D) > 2g - 2$.

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

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

as before.
We saw

$$3 \leq l(3Q) \leq 1 + 3.$$

It is now clear why $l(3Q) = 3$.
The curve $\mathcal{X}$ has genus $g = 1$, and

$$\deg(3Q) = 3 > 0 = 2g - 2.$$

So by the Theorem of Riemann-Roch we have

$$l(3Q) = 3 + 1 - g = 3.$$

Example

Consider the affine plane curve $\mathcal{X}_0$ of degree m defined by $G(X, Y) = 0$.

This curve intersects the line at infinity $Z = 0$, in m points.

Embed this plane curve in the projective curve $\mathcal{X}$.

Let $F(X, Y)$ be a bivariate polynomial of degree l.

Then F is regular function on $\mathcal{X}$.

Consider the rational function F^*/Z^l on the curve $\mathcal{X}$.

The possible poles of this rational functions are at infinity each with order at most l.

Let

$$D = l(\mathcal{X}^* \cdot V(Z)).$$

Then $\deg(D) = lm$

and $\mathcal{L}(D)$ consists of the rational functions of the form F^*/Z^l.

The genus of $\mathcal{X}$ is equal to $\binom{m-1}{2}$ by Plücker's formula .

Let m be a nonnegative integer.

Then

$$l((m-1)P) \;\leq\; l(mP) \;\leq\; l((m-1)P)+1.$$

And m is called a **(Weierstrass) gap** of P if

$$l(mP) = l((m-1)P).$$

The number of gaps of P is equal to the genus g of the curve,

since

$$l(iP) = i + 1 - g \text{ if } i > 2g - 2,$$

and

$$1 = l(0) \leq l(P) \leq \cdots \leq l((2g-1)P) = g.$$

A nonnegative integer that is not a gap is called a **nongap** of P.

The nonnegative integer m is a nongap of P if and only if there exists a rational function which has a pole of order m in P and no other poles.

If m_1 and m_2 are nongaps of P, then $m_1 + m_2$ is also a nongap of P.

The nongaps form the **Weierstrass semigroup** in $\mathbb{N}_0$.

Let $(\rho_i | i \in \mathbb{N})$ be an enumeration of all the nongaps of P in increasing order, so $\rho_1 = 0$.

Let $f_i \in L(\rho_i P)$ be such that $v_P(f_i) = -\rho_i$ for $i \in \mathbb{N}$.
Then $f_1, \ldots, f_i$ provide a basis for the space $\mathcal{L}(\rho_i P)$.

The term $l(W - D)$ in the Theorem of Riemann-Roch can be interpreted in terms of differentials.

Let D be a divisor on a curve $\mathcal{X}$.

Define

$$\Omega(D) = \{\omega \in \Omega(\mathcal{X}) \mid (\omega) - D \succcurlyeq 0\}$$

Denote the dimension of $\Omega(D)$ over $\mathbb{F}$ by $\delta(D)$, it is called the **index of speciality** of D.

The connection between differentials and functions is given by

Theorem $\delta(D) = l(W - D)$.

Proof

Let W be the divisor of the differential form ω.

Define the linear map

$$\phi : \mathcal{L}(W - D) \to \Omega(D)$$

by $\phi(f) = f\omega$. This is an isomorphism.

If we take $D = 0$ in

$$\dim \Omega(D) = \delta(D) = l(W - D),$$

then by the definition of the genus $g = l(D)$,

there are exactly g linearly independent regular differentials on a curve $\mathcal{X}$.

So there is a unique regular differential (up to a constant factor)
on a curve of genus 1.

§7 Codes from algebraic curves

Let $\mathcal{X}$ be an absolutely irreducible nonsingular projective curve over $\mathbb{F}_q$.
We shall define two kinds of algebraic geometry codes from $\mathcal{X}$.

The first kind generalizes Reed-Solomon codes,
the second kind generalizes Goppa codes.

In the following, $P_1, P_2, \ldots, P_n$ are rational points on $\mathcal{X}$
and D is the divisor $P_1 + P_2 + \cdots + P_n$.

Furthermore G is some other divisor that has support disjoint from D.

Although it is not necessary to do so, we assume:

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

The linear code $C(D, G)$ of length n over $\mathbb{F}_q$

is the image of the linear map

$$\alpha : \mathcal{L}(G) \to \mathbb{F}_q^n$$

defined by $\alpha(f) = (f(P_1), f(P_2), \ldots, f(P_n))$.

These codes are called **geometric Reed Solomon codes**.

Theorem Let $2g - 2 < \deg(G) < n$. Then $C(D, G)$ has

dimension $k = \deg(G) - g + 1$ and

minimum distance $d \geq n - \deg(G)$.

Proof
(i) If f belongs to the kernel of α, then $f \in \mathcal{L}(G - D)$
and this implies $f = 0$, since $\deg(G) < n$.
The result follows from the assumption $2g - 2 < \deg(G)$
and the Corollary of RR.

(ii) If $\alpha(f)$ has weight d, then there are $n - d$ points $P_{i_1}, P_{i_2}, \ldots, P_{i_{n-d}}$
for which $f(P_i) = 0$.
Therefore $f \in \mathcal{L}(G - E)$, where $E = P_{i_1} + \cdots + P_{i_{n-d}}$.
Hence $\deg(G) - (n - d) \geq 0$.

Example

Let $\mathcal{X}$ be the curve with equation $X^3 + Y^3 + Z^3 = 0$ over $\mathbb{F}_4$.
Let $G = 3Q$, where $Q = (0 : 1 : 1)$.

Take $n = 8$, so D is the sum of the remaining rational points.
The coordinates are given by

	Q	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
x	0	0	0	1	α	$\overline{\alpha}$	1	α	$\overline{\alpha}$
y	1	α	$\overline{\alpha}$	0	0	0	1	1	1
z	1	1	1	1	1	1	0	0	0

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

We saw that 1, $x/(y+z)$ and $y/(y+z)$ are a basis of $\mathcal{L}(3Q)$ over $\mathbb{F}_4$

This leads to the following generator matrix for $C(D, G)$:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & \alpha & \overline{\alpha} & 1 & \alpha & \overline{\alpha} \\ \overline{\alpha} & \alpha & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

The minimum distance is at least $8 - 3 = 5$.
One immediately sees from the generator matrix that $d = 5$.

We now come to the second class of algebraic geometry codes.

These codes are called **geometric Goppa codes**.

The linear code $C^*(D, G)$ of length n over $\mathbb{F}_q$ is the image of the linear map

$$\alpha^* : \Omega(G - D) \to \mathbb{F}_q^n$$

defined by

$$\alpha^*(\eta) = (\mathrm{Res}_{P_1}(\eta), \mathrm{Res}_{P_2}(\eta), \ldots, \mathrm{Res}_{P_n}(\eta)).$$

Theorem The code $C^*(D, G)$ has

dimension $k^* = n - \deg(G) + g - 1$

and minimum distance $d^* \geq \deg(G) - 2g + 2$.

Proof
These assertions are direct consequences of the Theorem of RR,
using the connection between the dimension of $\Omega(G)$ and $l(W - G)$)
and the Corollary stating that the degree of a canonical divisor is $2g - 2$.

Example

Let $L = \{\alpha_1, \ldots, \alpha_n\}$ be a set of n distinct elements of $\mathbb{F}_{q^m}$.

Let g be a polynomial in $\mathbb{F}_{q^m}[X]$ which is not zero at α_i for all i.

The **(classical) Goppa code** $\Gamma(L, g)$ is defined by

$$\Gamma(L, g) = \left\{ \mathbf{c} \in \mathbb{F}_q^n \mid \sum \frac{c_i}{X - \alpha_i} \equiv 0 \pmod{g} \right\}.$$

Let $P_i = (\alpha_i : 1)$, $Q = (1 : 0)$ and $D = P_1 + \cdots + P_n$.

Take for E the divisor of zeros of g on the projective line.

Then $\Gamma(L, g) = C^*(D, E - Q)$ and

$$\mathbf{c} \in \Gamma(L, g) \text{ if and only if } \sum \frac{c_i}{X - \alpha_i} dX \in \Omega(E - Q - D).$$

This is the reason that some authors extend the definition of geometric Goppa codes to subfield subcodes of codes of the form $C^*(D, G)$.

It is a well-known fact that the parity check matrix of the Goppa code $\Gamma(L, g)$ is equal to the following generator matrix of a generalized RS code

$$\begin{pmatrix} g(\alpha_1)^{-1} & \dots & g(\alpha_n)^{-1} \\ \alpha_1 g(\alpha_1)^{-1} & \dots & \alpha_n g(\alpha_n)^{-1} \\ \vdots & \dots & \vdots \\ \alpha_1^{r-1} g(\alpha_1)^{-1} & \dots & \alpha_n^{r-1} g(\alpha_n)^{-1} \end{pmatrix},$$

where r is the degree of the Goppa polynomial g.
So $\Gamma(L, g)$ is the subfield subcode of the dual of a generalized RS code.

This is a special case of the following theorem.

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

Proof We know that $k + k^* = n$.
So it suffices to take a word from each code and show that
the inner product of the two words is 0.

Let $f \in \mathcal{L}(G)$ and $\eta \in \Omega(G - D)$. The differential $f\eta$ has no poles except possibly poles of order 1 in the points $P_1, P_2, \ldots, P_n$.

The residue of $f\eta$ in P_i is equal to $f(P_i)\text{Res}_{P_i}(\eta)$.
The sum of the residues of $f\eta$ over all the poles. Hence we have

$$0 = \sum_{i=1}^{n} f(P_i)\text{Res}_{P_i}(\eta) = \langle \alpha(f), \alpha^*(\eta) \rangle.$$

Theorem Let $\mathcal{X}$ be a curve defined over $\mathbb{F}_q$.

Let $P_1, \ldots, P_n$ be n rational points on $\mathcal{X}$.

Let $D = P_1 + \cdots + P_n$.

Then there exists a differential form ω with simple poles at the P_i such that $Res_{P_i}(\omega) = 1$ for all i.

Furthermore

$$C^*(D, G) = C(D, W + D - G)$$

for all divisors G that have a support disjoint from the support of D, where W is the divisor of ω.

Several authors prefer the codes $C^*(D, G)$ over geometric RS codes, but the nonexperts in algebraic geometry probably feel more at home with polynomials than with differentials.

So one can do without differentials and the codes $C^*(D, G)$.

However, it is useful to have both classes when treating decoding methods. These use parity checks, so one needs a generator matrix for the dual code.

In the next lecture we treat several examples of algebraic geometry codes.

It is already clear that we find some **good** codes.

For example from codes over a curve of genus 0 (the projective line) are MDS codes.

In fact we have that

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

so if g is small, we are close to the Singleton bound.