Algebraic geometry codes and their parameters

Ruud Pellikaan
Technical University of Eindhoven

Mastermath Coding Theory
November 4, 2008

Content:
§5 Differentials on a curve
§6 The Riemann-Roch theorem
§7 Codes from algebraic curves
§8 Some algebraic geometry codes
§9 Asymptotically good sequences of codes and curves

Sections 2.5, 2.6, 2.7, 2.8 and 2.9 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/masterm-AGC2.pdf`

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

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

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

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.

§8 Some algebraic geometry codes

We know that to find good codes, we must find long codes. To use the methods from algebraic geometry, it is necessary to find rational points on a given curve. The number of these is a bound on the length of the code.

A central problem in algebraic geometry is finding bounds for the number of rational points on a variety. We mention without proof the improvement by **Serre** of the **Hasse-Weil bound**.

Theorem Let $\mathcal{X}$ be a curve of genus g over $\mathbb{F}_q$. If $N_q(\mathcal{X})$ denotes the number of rational points on $\mathcal{X}$, then

$$|N_q(\mathcal{X}) - (q+1)| \leq g\lfloor 2\sqrt{q} \rfloor.$$

Example In this example we consider codes from **Hermitian** curves.

Let $q = r^2$. Consider the affine equation

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

of the Hermitian curve $\mathcal{H}_r$ in $\mathbb{A}^2$ over $\mathbb{F}_q$.

The genus g of $\mathcal{H}_r$ is

$$\frac{1}{2}r(r-1) = \frac{1}{2}(q - \sqrt{q}).$$

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

The right side of the equation $X^{r+1} = Y^r + Y$ is the trace from $\mathbb{F}_q$ to $\mathbb{F}_r$.
There are r elements in $\mathbb{F}_q$ with zero trace.

The remaining elements in $\mathbb{F}_q$ have a nonzero trace.
$X^{r+1} = \beta$ has exactly $r+1$ solutions in $\mathbb{F}_q$, for every $\beta \in \mathbb{F}_r^*$.

Hence the number of $\mathbb{F}_q$-rational points of $\mathcal{H}_r$ is

$$1 + r + (r^2 - r)(r+1) = 1 + r^3.$$

$\mathcal{H}_r$ is a maximal curve, since

$$q + 1 + 2g\sqrt{q} = r^2 + 1 + r(r-1)r = 1 + r^3.$$

Let $q = r^2$ and $n = r^3$.

Let $P_1, \ldots, P_n$ be the n affine rational points and $Q = (0 : 1 : 0)$.

Take $D = P_1 + \cdots + P_n$ and $G = mQ$, where $q - \sqrt{q} < m < q\sqrt{q}$.

The code $C(D, G)$ over $\mathbb{F}_q$ has length n,
dimension $k = m - g + 1$, and distance $d \geq n - m$.

A basis for $L(G)$ is given by the functions

$$f_{i,j} = x^i y^j,\ 0 \leq i \leq r,\ ri + (r+1)j \leq m$$

To see how good these codes are, we take as example $r = 4$, $q = 16$.

A basis for $\mathcal{L}(G)$ consists of

$$f_{i,j} = x^i y^j / z^{i+j},\ 0 \leq i \leq 4,\ 4i + 5j \leq m$$

Observe that there are $m - 5 = m - g + 1$ of such pairs (i, j).

The functions x/z and y/z can be treated in exactly the same way as before, showing that $f_{i,j}$ has a pole of order $4i + 5j$ in Q.

Hence, these functions are independent.

Therefore, the code is easily constructed.

What is the quality of this code?

Suppose a long message of 10^9 bits is send over a channel with an error probability $p_e = 0.01$ (quite a bad channel).

Compare coding using a rate $\frac{1}{2}$ Reed-Solomon code over $\mathbb{F}_{16}$ with using $C(D, G)$, where we take $m = 37$ to also have rate $\frac{1}{2}$.

In this case, $C(D, G)$ has distance 27.
The RS code has word length 16 (so 64 bits) and distance 9.

If a word is received incorrectly, we assume that all the bits are wrong when we count the number of errors.

For the RS code, the error probability after decoding is roughly $3 \cdot 10^{-4}$.
However, for the code $C(D, G)$ this is less than $2 \cdot 10^{-7}$.

Keep in mind that we are fixing the alphabet $\mathbb{F}_{16}$.

If we compare the code $C(D, G)$, for which the words are strings of 256 bits,

with a rate $\frac{1}{2}$ RS code over $\mathbb{F}_{2^5}$, words are 160 bits long.

The latter will come close in performance with error probability $2 \cdot 10^{-6}$

and a rate $\frac{1}{2}$ RS code over $\mathbb{F}_{2^6}$, words are 384 bits long,

performs better: roughly 10^{-7}.

Compare our code with a binary BCH code of length 255 and rate about $\frac{1}{2}$.

The BCH code wins when we are concerned with random errors.

On a bursty channel the code $C(D, G)$ handles bursts of 46 bits length

which influence at most 13 letters of a codeword,

while the BCH code would fail completely.

The **Klein quartic** over $\mathbb{F}_8$

has affine equation

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

The genus is 3.

So it can have at most 24 rational points by the Serre bound.
It has in fact 24 rational points.

Let $Q = (0 : 0 : 1)$ and let D be the sum of the other 23 rational points, $G = 10Q$.
We find that $C(D, G)$ has dimension $10 - g + 1 = 8$ and minimum distance $d \geq 23 - 10 = 13$.

We now concatenate this code [23,8,13] code over $\mathbb{F}_8$
with the binary [4,3,2] single parity check code.

The symbols in codewords of $C(D, G)$ are elements of $\mathbb{F}_8$
which we interpret as column vectors of length 3 over $\mathbb{F}_2$

Adjoin the parity check. The resulting code C is a binary $[92, 24, 26]$ code.
This is world record.

Example We construct a generator matrix for this code.

Consider the functions x/z and y/z.

The divisors $(x/z) = 3P_1 - P_2 - 2Q$ and $(y/z) = P_1 + 2P_2 - 3Q$ were computed.

From these divisors, we deduce that the functions

$$(x/z)^i(y/z)^j,\ 0 \leq 2i + 3j \leq 10,\ 0 \leq i \leq 2j$$

are in $\mathcal{L}(10Q)$.

Thus we have eight functions in $\mathcal{L}(10Q)$ with poles in Q of order

$0, 3, 5, 6, 7, 8, 9$ and 10, respectively.

Hence they are independent and since $l(10Q) = 8$.

They are a basis of $\mathcal{L}(10Q)$.

By substituting the coordinates of the rational points of $\mathcal{X}$

in these functions, we find the 8 by 23 generator matrix of the code.

Example Let $\mathbb{F}_4 = \{0, 1, \alpha, \overline{\alpha}\}$,
where $\alpha^2 = \alpha + 1 = \overline{\alpha}$.

Consider the curve $\mathcal{X}$ over $\mathbb{F}_4$ given by the equation $x^2y + \alpha y^2 z + \overline{\alpha} z^2 x = 0$.

This is a nonsingular curve with genus 1. Its nine rational points are given by

	P_1	P_2	P_3	P_4	P_5	P_6	Q_1	Q_2	Q_3
x	1	0	0	1	1	1	α	1	1
y	0	1	0	α	$\overline{\alpha}$	1	1	α	1
z	0	0	1	$\overline{\alpha}$	α	1	1	1	α

Let $D = P_1 + P_2 + \cdots + P_6$, $G = 2Q_1 + Q_2$.

The functions $x/(x+y+\overline{\alpha}z)$, $y/(x+y+\overline{\alpha}z)$, $\overline{\alpha}z/(x+y+\overline{\alpha}z)$ are a basis of $\mathcal{L}(G)$.

To see this, note that the numerators in these fractions are not 0 in Q_1 and Q_2 and that the line with equation $x + y + \overline{\alpha}z = 0$ meets $\mathcal{X}$ in Q_2 and is tangent to $\mathcal{X}$ in Q_1.

The code $C(D, G)$ of length 6 has minimum distance at least 3.

However, the code is in fact an MDS code, namely the **hexacode**.

§9 Asymptotically good sequences of codes and curves

The **parameters** of a linear block code over the finite field $\mathbb{F}_q$ of

length n, **dimension** k and **minimum distance** d

will be denoted by

$$[n, k, d]_q \text{ or } [n, k, d].$$

The quotient $R = k/n$ is called the **information rate**

and $\delta = d/n$ is the **relative minimum distance**.

The parameters of an **algebraic geometry code**

on a curve of genus g with n points that are defined over $\mathbb{F}_q$ satisfy

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

Hence

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

A sequence of codes

$$(C_m | m \in \mathbb{N})$$

with parameters $[n_m, k_m, d_m]$ over a fixed finite field $\mathbb{F}_q$ is called

asymptotically good if n_m tends to infinity and

$$\lim_{m \to \infty} d_m/n_m = \delta > 0,$$

and

$$\lim_{m \to \infty} k_m/n_m = R > 0.$$

Define the q-ary **entropy function** by $H_q(0) = 0$ and

$$H_q(x) = x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x)$$

for $0 < x \leq (q-1)/q$.

For every R and δ such that

$$R \geq 1 - H_q(\delta).$$

there exist asymptotically good sequences of codes attaining

the **Gilbert-Varshamov** bound

In order to construct asymptotically good codes

we therefore need curves with

low genus and many $\mathbb{F}_q$-rational points.

Let $N_q(g)$ be the maximal number of $\mathbb{F}_q$-rational points on
an absolutely irreducible nonsingular projective curve over $\mathbb{F}_q$ of genus g.

Let

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g}.$$

The Hasse-Weil bound implies

$$A(q) \leq 2\sqrt{q}.$$

This has been improved to the **Drinfeld-Vldut** bound.

Theorem

$$A(q) \leq \sqrt{q} - 1.$$

Ihara and Tsfasman-Vladut-Zink have shown that

Theorem

$$A(q) = \sqrt{q} - 1 \quad \text{if } q \text{ is a square.}$$

This equality is proved by studying

the number of rational points of **modular curves** over finite fields.

The theory of modular curves is a central and
very important part of mathematics,

but it is very involved and deep, much more so than the theory
concerning the Riemann-Roch theorem.

Applying this to algebraic geometry codes one derives
the **Tsfasman-Vludut-Zink** (TVZ) bound.

Theorem Let q be a square.

Then for every R there exists an asymptotically good sequence of codes

such that the limit value of the information rate is R and

the relative minimum distance is δ and

$$R + \delta \geq 1 - \frac{1}{\sqrt{q} - 1}.$$

This in turn means that the TVZ bound is better than the

Gilbert-Varshamov bound when q is a square and $q \geq 49$

in a certain range of δ.

This fact was the starting point of the

current interest in algebraic geometry codes.

An alternative method instigated by **Feng-Rao** to derive these results.

Let F be a polynomial in the variables X and Y with coefficients in $\mathbb{F}_q$.

Let $a = \deg_Y(F)$.

Suppose that there exists a subset S of $\mathbb{F}_q$ such that

for any given $x \in S$ there exist exactly a distinct $y_1, \ldots, y_a \in S$

such that $F(x, y_i) = 0$ for all $i = 1, \ldots, a$.

Consider the algebraic set $\mathcal{X}_m$ in $\mathbb{A}^m$ defined by the equations

$$F(X_i, X_{i+1}) = 0 \text{ for } i = 1, \ldots, m-1.$$

A lower bound on the number of rational points of $\mathcal{X}_m$ is

easily seen to be

$$|S| \cdot a^{m-1}.$$

If $\mathcal{X}_m$ is absolutely irreducible, then it is a curve.

Example

Let $F = (X^q - X) - (Y^q - Y)$.

Then F is an example with $a = q$ and $S = \mathbb{F}_q$.

Then $\mathcal{X}_m$ has q^m rational points.

This is the maximal possible number of rational points for an algebraic set $\mathcal{X}_m$ in $\mathbb{A}^m$.

But $\mathcal{X}_m$ is reducible, since F is divisible by $X - Y$.

Example

Let $F = X(X^q - X) - (Y^q - Y)$.

Then F is an example with $a = q$ and $S = \mathbb{F}_q$.

One can show that $\mathcal{X}_m$ is a curve.

The number of rational points of $\mathcal{X}_m$ is again q^m.

But the genus of these curves grows

much faster than the number of rational points.

A sequence of curves $(\mathcal{X}_m | m \in \mathbb{N})$ is called **asymptotically good**

if $g(\mathcal{X}_m)$ tends to infinity and the following limit exists and

$$\lim_{m \to \infty} \frac{N_q(\mathcal{X}_m)}{g(\mathcal{X}_m)} > 0,$$

where $g(\mathcal{X})$ is the genus of $\mathcal{X}$ and

$N_q(\mathcal{X})$ is the number of $\mathbb{F}_q$-rational points of $\mathcal{X}$.

Example

Let $q = 8$. Let $F = XY^3 + Y + X^3$.

Then F is an example with $a = 3$ and $S = \mathbb{F}_8^*$.

Therefore this gives a curve with $7 \cdot 3^{m-1}$ points

with nonzero coordinates in $\mathbb{F}_8$.

But this sequence of curves is not asymptotically good.

Example

Let $q = 4$. Let $F = XY^2 + Y + X^2$.

Then F is an example with $a = 2$ and $S = \mathbb{F}_4^*$.

Therefore this gives a curve with $3 \cdot 2^{m-1}$ points

with nonzero coordinates in $\mathbb{F}_4$,

and in fact it gives a sequence of curves that is asymptotically good.

More generally, let $q = r^2$ and consider

$$F = X^{r-1}Y^r + Y - X^r.$$

Then we get an example with $a = r$ and $S = \mathbb{F}_q^*$,

the equation $F = 0$ has the property that
for every nonzero $x \in \mathbb{F}_q$ there are exactly

r nonzero solutions in $\mathbb{F}_q$ of the equation $F(x, Y) = 0$ in Y.

This is seen by multiplying the equation by X and

replacing XY by Z.

Then the equation $Z^r + Z = X^{r+1}$ is obtained,

which is the Hermitian curve over $\mathbb{F}_q$.

Therefore

$$N_q(\mathcal{X}_m) \geq (q-1)r^{m-1}.$$

The genus of the curve $\mathcal{X}_m$ is computed

by induction and applying the formula of **Hurwitz-Zeuthen**

to the covering

$$\pi_m : \mathcal{X}_m \to \mathcal{X}_{m-1},$$

where π_m is defined as $\pi_m(x_1, \ldots, x_m) = (x_1, \ldots, x_{m-1})$.

In this case it turns out to be an **Artin-Schreier covering**.

It is easier to view this in terms of function fields.

Let $\mathcal{F}_m$ be the function field of $\mathcal{X}_m$.

Then $\mathcal{F}_1 = \mathbb{F}_q(z_1)$ and $\mathcal{F}_m$ is obtained from

$\mathcal{F}_{m-1}$ by adjoining a new element z_m

that satisfies the equation

$$z_m^r + z_m = x_{m-1}^{r+1},$$

where $x_{m-1} = z_{m-1}/x_{m-2} \in \mathcal{F}_{m-1}$ for

$m \geq 2$, and $x_1 = z_1$, $x_0 = 1$.

Theorem (Garcia-Stichtenoth)

The genus g_m of the curve $\mathcal{X}_m$,

or equivalently of the function field $\mathcal{F}_m$ is equal to

$$g_m = \begin{cases} r^m + r^{m-1} - r^{\frac{m+1}{2}} - 2r^{\frac{m-1}{2}} + 1 & \text{if } m \text{ is odd}, \\ r^m + r^{m-1} - \frac{1}{2}r^{\frac{m+2}{2}} - \frac{3}{2}r^{\frac{m}{2}} - r^{\frac{m-2}{2}} + 1 & \text{if } m \text{ is even}. \end{cases}$$

Thus the Drinfeld-Vladut bound is attained.

A second tower of curves $\mathcal{Y}_m$

with function field $\mathcal{T}_m$ over $\mathbb{F}_q$ with $q = r^2$.

Let $\mathcal{T}_1 = \mathbb{F}_q(X_1)$.

Let $\mathcal{T}_m$ be obtained from $\mathcal{T}_{m-1}$

by adjoining a new element x_m that satisfies the equation:

$$x_m^r + x_m = \frac{x_{m-1}^r}{x_{m-1}^{r-1} + 1}.$$

By induction it is shown that

$$N_q(\mathcal{Y}_m) \geq (r^2 - r)r^{m-1}.$$

Theorem (Garcia-Stichtenoth)

The genus g_m of the curve $\mathcal{Y}_m$ is equal to

$$g_m = \begin{cases} (r^{\frac{m+1}{2}} - 1)(r^{\frac{m-1}{2}} - 1) & \text{if } m \text{ is odd ,} \\ (r^{\frac{m}{2}} - 1)^2 & \text{if } m \text{ is even .} \end{cases}$$

Hence this sequence of function fields

attains the Drinfeld-Vladut bound too.