Efficient construction of algebraic geometry codes; the q-th power algorithm

Ruud Pellikaan
Technical University of Eindhoven

RISC seminar:
"Algebraic Function Fields and Their Cryptographic Applications"
at CWI Amsterdam, October 21, 2008

Literature:

Sections 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.

§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

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

The code is easily constructed.

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.

§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.

It turns out that finding bases for the vector spaces involved

in the construction of AG codes is difficult.

This last part remains to be done in order

to make the codes really constructive.

One method is given by the q-th power algorithm:

D.A. Leonard and R. Pellikaan,
Integral closures and weight functions over finite fields,
Finite Fields and their Applications, vol. 9 (4), pp. 479-504, 2003.