Asymptotically good sequences of codes and curves

Ruud Pellikaan
Technical University of Eindhoven

Soria Summer School
on Computational Mathematics
July 9, 2008

Content:
§8 Some algebraic geometry codes
§9 Asymptotically good sequences of codes and curves

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.

http://www.win.tue.nl/ ruudp/paper/31.pdf
http://www.win.tue.nl/ ruudp/lectures/slides3-AGC-Soria.pdf

§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. In order to appreciate some of the examples in this paragraph, 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 second affine equation $X^{r+1} = Y^r + Y$ of the Hermitian curve $\mathcal{X}$ in $\mathbb{A}^2$ over $\mathbb{F}_q$. The genus g of $\mathcal{X}$ equals $\frac{1}{2}r(r-1) = \frac{1}{2}(q - \sqrt{q})$. We shall first show that $\mathcal{X}$ has the maximal number of rational points, that is to say, exactly $1 + q\sqrt{q}$. The last equation has $(0 : 1 : 0)$ as the only point at infinity. To see that the number of affine $\mathbb{F}_q$-rational points is $r+(r+1)(r^2-r) = r^3$ one argues as follows. The right side of the equation $X^{r+1} = Y^r + Y$ is the trace from $\mathbb{F}_q$ to $\mathbb{F}_r$. The first r in the formula on the number of points corresponds to the elements of $\mathbb{F}_r$. These are exactly the elements of $\mathbb{F}_q$ with zero trace. The remaining term corresponds to the elements in $\mathbb{F}_q$ with a nonzero trace, since the equation $X^{r+1} = \beta$, $\beta \in \mathbb{F}_r^*$, has exactly $r + 1$ solutions in $\mathbb{F}_q$.

We take $G = mQ$, where $Q = (0 : 1 : 0)$ and $q - \sqrt{q} < m < q\sqrt{q}$.

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

To see how good these codes are, we take as example $q = 16$.
A basis for $\mathcal{L}(G)$ is easily found. The functions

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

will do the job.

First, observe that there are $m - 5 = m - g + 1$ pairs (i, j) satisfying these conditions. 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.

Let us try to get some idea of the quality of this code. Suppose that we intend to send a long message (say 10^9 bits) over a channel with an error probability $p_e = 0.01$ (quite a bad channel). We 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 $C(D, G)$, the error probability after decoding is less than $2 \cdot 10^{-7}$.

In this example, it is important to keep in mind that we are fixing the alphabet (in this case $\mathbb{F}_{16}$). 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 (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}).

One could also 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. If we are using a bursty channel, then the code $C(D, G)$ can handle bursts of length up to 46 bits (which influence at most 13 letters of a codeword) while the BCH code would fail completely.

Example Let $\mathcal{X}$ be the Klein quartic over $\mathbb{F}_8$.

The genus is 3, so $\mathcal{X}$ can have at most 24 rational points by the Serre bound, and we saw that it has 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 with the [4,3,2] single parity check code as follows. The symbols in codewords of $C(D, G)$ are elements of $\mathbb{F}_8$ which we interpret as column vectors of length 3 over $\mathbb{F}_2$ and then we adjoin the parity check. The resulting code C is a binary $[92, 24, 26]$ code is a world record.

Example We show how to construct a generator matrix for the code of the previous example. We 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 as before.

From these divisors, we can deduce that the functions

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

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

We thus 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 $D = P_1 + P_2 + \cdots + P_6$, $G = 2Q_1 + Q_2$. We claim that 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 $[n, k, d]_q$ or $[n, k, d]$.

The quotient k/n is called the **information rate** and denoted by $R = k/n$ and the **relative minimum distance** d/n is denoted by δ.

The dimension k and the minimum distance d 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 d_m/n_m tends to a nonzero constant δ, and k_m/n_m tends to a nonzero constant R for $m \to \infty$.

Let $H_q(0) = 0$ and

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

for $0 < x \leq (q-1)/q$ be the entropy function.

Then there exist asymptotically good sequences of codes attaining the the **Gilbert-Varshamov** bound

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

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 and we will not touch it.

Applying this to algebraic geometry codes one derives the following **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 GV 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.

In the following we discuss an alternative method due to 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 $\#S \cdot a^{m-1}$ by induction. 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 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 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 $S = \mathbb{F}_q^*$, that is to say, the equation $F = 0$ has the property that for every given nonzero element $x \in \mathbb{F}_q$ 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 defines the Hermitian curve over $\mathbb{F}_q$. Therefore the corresponding sequence of curves $\mathcal{X}_m$ satisfies

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

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

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.

A new sequence of curves $\mathcal{Y}_m$ with function field $\mathcal{T}_m$ over $\mathbb{F}_q$ with $q = r^2$ is given as follows. 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.

Let Q_m be the rational point on the curve $\mathcal{Y}_m$ that is the unique pole of x_1.

Theorem (Pellikaan-Stichtenoth-Torres)

Let Λ_m be the Weierstrass semigroup of Q_m. Then $\Lambda_1 = \mathbb{N}_0$ and

$$\Lambda_{m+1} = r \cdot \Lambda_m \cup \{n \in \mathbb{N}_0 \mid n \geq c_m\},$$

where

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

This means that the sequence of nongaps of Q_m is known, but an explicit description of a basis for the spaces $\mathcal{L}(iQ_m)$ is not known in general.