

# On several new projective curves over $\text{GF}(2^m)$ with genus 3,4 et 5

Oscar Moreno, Victor Zinoviev, Dimitri Zinoviev

► **To cite this version:**

Oscar Moreno, Victor Zinoviev, Dimitri Zinoviev. On several new projective curves over  $\text{GF}(2^m)$  with genus 3,4 et 5. [Research Report] RR-2327, INRIA. 1994. <inria-00074347>

**HAL Id: inria-00074347**

**<https://hal.inria.fr/inria-00074347>**

Submitted on 24 May 2006

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

*On Several New Projective  
Curves Over  $GF(2^m)$   
with Genus 3, 4 and 5*

Oscar MORENO  
Victor ZINOVIEV - Dmitrii ZINOVIEV

N° 2327  
Août 1994

PROGRAMME 2

A large, stylized, light-colored 'R' logo is positioned to the left of the text.

*R*apport  
*de recherche*

Les rapports de recherche de l'INRIA  
sont disponibles en format postscript sous  
ftp.inria.fr (192.93.2.54)

si vous n'avez pas d'accès ftp  
la forme papier peut être commandée par mail :  
e-mail : dif.gesdif@inria.fr  
(n'oubliez pas de mentionner votre adresse postale).

par courrier :  
Centre de Diffusion  
INRIA  
BP 105 - 78153 Le Chesnay Cedex (FRANCE)

INRIA research reports  
are available in postscript format  
ftp.inria.fr (192.93.2.54)

if you haven't access by ftp  
we recommend ordering them by e-mail :  
e-mail : dif.gesdif@inria.fr  
(don't forget to mention your postal address).

by mail :  
Centre de Diffusion  
INRIA  
BP 105 - 78153 Le Chesnay Cedex (FRANCE)

On several new projective curves over  
 $GF(2^m)$  with genus 3, 4 and 5

Sur plusieurs nouvelles courbes projectives  
définies sur  $GF(2^m)$  de genres 3, 4 et 5

Oscar Moreno\*    Victor Zinoviev†    Dmitrii Zinoviev‡

**Abstract**

Using known techniques of desingularization [1] of singular projective curves over finite fields  $F_q$ ,  $q = 2^m$ , we found several new binary planar projective curves of genera 3, 4 and 5 with the maximal number of  $F_q$ -rational points. The numbers of  $F_q$ -rational points on their smooth projective models are close or meet Serre's upper bound.

**Résumé**

En utilisant des techniques bien connues de désingularisation de courbes singulières définies sur des corps finis  $F_q$ ,  $q = 2^m$  [1], nous avons trouvé plusieurs nouvelles courbes planes projectives sur un corps de caractéristique 2, de genres 3, 4 et 5 avec un nombre maximal de points rationnels sur  $F_q$ . Le nombre de points rationnels sur  $F_q$  de leurs modèles lisses atteint la borne supérieure de Serre ou en est très proche.

---

\*Department of Mathematics, University of Puerto Rico, Rio Piedras, Puerto Rico, 00931

†V. Zinoviev is also with the Institute for Problems of Information Transmission Russian Academy of Sciences, Ermolova str.19, GSP-4, Moscow, 101447, Russia. **Invité au projet CODES du 01.02.94 au 30.09.94**

‡Department of Mathematics, The Ohio State University, Columbus, OH 43210, USA

## 1. Introduction.

We denote by  $F_q = \text{GF}(q)$  a finite field of  $q = 2^m$  elements. Consider a homogeneous polynomial  $f(x, y, z) \in F_q[x, y, z]$  of degree  $d$ . Each (absolutely irreducible) polynomial  $f$  defines a plane curve. Let  $C$  be its smooth projective model and  $g$  its genus. Set  $N_q$  for the number of  $F_q$ -rational points on  $C$ . Then according to Serre's upper bound [2], [3] we have

$$|N_q - (q + 1)| \leq g[2\sqrt{q}] ,$$

where  $[\alpha]$  is the integral part of  $\alpha$ .

Fix some  $F_q$  and  $g$ . For a given smooth projective curve  $C$  defined over  $F_q$  and of a given genus  $g$ , denote by  $N_q(C, g)$  the number of its  $F_q$ -rational points. Define  $N_q(g)$  to be the maximal possible  $N_q(C, g)$ , when  $C$  runs over all projective smooth curves of genus  $g$  defined over  $F_q$ . We consider only those projective smooth curves which are the projective smooth models of plane curves given by absolutely irreducible homogeneous binary polynomials of small degrees which are either smooth or have a binary singular point. Thus, we consider all homogeneous binary polynomials  $f(x, y, z)$ ,  $f(x, y, z) \in F_2[x, y, z]$ ,  $\deg(f) = 4$  or  $5$  (with the restriction mentioned above) which define projective curves of genus 3, 4 and 5. We are also interested in the number of such curves. Note that since we restrict our search to the curves of degrees 4 and 5 with the binary singular point on them, we actually provide the lower bound for  $N_q(g)$ .

Using known techniques of desingularization (for example [1]) of singular projective curves over the finite fields (which we needed to compute the genus), we found several new binary plane curves of degrees 4 and 5 whose genus is 3, 4 or 5. Throughout all computations we considered either smooth curves of degree 4 or curves of degree 5 with one, two or three binary singular points of order two. The number of  $F_q$ -rational points on their smooth projective models meets or is close to Serre's upper bound  $q + 1 + g[2\sqrt{q}]$ . The computations were implemented on IBM R/6000-365 and DEC 3000-300L AXP workstations using the computer algebra system AXIOM (SCRATCHPAD) and C language. The most time consuming part was to select among all curves (for big  $q$ 's) those with the highest number of  $F_q$ -rational points.

## 2. Description of computation.

We follow the following idea. For small fields  $F_q$ ,  $q = 2^m$ ,  $m = 3, 4, \dots, 9$  we want to find curves of a given (small) genus  $g = 3, 4$  or  $5$  defined by irreducible binary polynomials of degrees 4 or 5. With the method we used the amount of computations will not be acceptable for polynomials of higher degrees.

Fix some  $q$  and genus  $g$ . We are interested in curves only up to the linear isomorphism (i.e.  $f_1 = f_2$  if there exists a matrix  $A \in GL_3(F_2)$ , such that  $f_1(x_1, x_2, x_3) = f_2(y_1, y_2, y_3)$ , where  $(y_1, y_2, y_3) = (x_1, x_2, x_3)A$ ). We choose the representative, whose singular points are:  $(0:0:1)$  if there is one singular point and  $(0:0:1), (0:1:0)$  if there are two of them. If for a given curve  $C$ , defined by some  $f(x, y, z)$  we know the number of  $F_q$ -rational points on it then it is easy to compute the number of  $F_q$ -rational points on its smooth projective model (see [1]). Thus, we can arrange our computations into two parts: first, we select among all curves (with the additional restriction that all singular points are binary or the curve is smooth) those with big numbers of  $F_q$ -rational points. Note that it is possible to have  $0, 1, \dots, m$   $F_q$ -rational points on a smooth model lying above the singular one of order  $m$ , which in our case is always 2. So, we will have one point on the smooth model above each cusp, and no points or two points, depending on the field  $F_q$ , above each node. This part is implemented in C. We don't check irreducibility at the first stage. In the second part of our computations (which is implemented in AXIOM) we check the irreducibility, find the curves with the given genus, select those which have the maximal number of  $F_q$ -points on their smooth models and, finally, select only those which are not linearly isomorphic to each other.

For a given plane curve  $C$ , defined by some homogeneous binary polynomial  $f = f(x, y, z) \in F_2[x, y, z]$  of degree  $d$ , it is easy to find the number of  $F_q$ -rational points and, using AXIOM, it is easy to establish the irreducibility of  $f(x, y, z)$ . So, it means that for a given plane curve we need to know how to compute its genus. We recall (see [1] f.g.) that if  $P_1, P_2, \dots, P_r$  are all the singular points and  $m_i$  is the order of  $i$ -th singular point then

$$g \leq \frac{(d-1)(d-2)}{2} - \sum_{i=1}^r \frac{m_i(m_i-1)}{2}, \quad (1)$$

which becomes an equality if all the singularities are ordinary. Recall that  $N_q$  is the number of  $F_q$ -rational points on the smooth model of  $C$ . From Serre's bound it follows that if (for some positive integer  $g_0$ ) we have

$$q + 1 + g_0[2\sqrt{q}] < N_q, \quad (2)$$

then  $g > g_0$ , where  $g$  is the genus of  $C$ . Together with the upper bound for the genus, given by (1), this allows us to determine it, provided the number of  $F_q$ -rational points of a curve is big enough. Since we are looking for curves with big numbers of  $F_q$ -points the above argument works in many cases, namely in statements 3.2 and 4.1 – 7.2.

In those cases when it does not work we wrote, following [1], an AXIOM program which computes the genus. We outline the main steps:

Suppose that we want to find the genus of some curve given by  $f(x, y, z)$ . It is known (see [1]) that to do this one can apply Cremona transformations to a curve till all of its

singular points become ordinary. Once all the singular points are ordinary, then

$$g = \frac{(d-1)(d-2)}{2} - \sum_{i=1}^r \frac{m_i(m_i-1)}{2}, \quad (3)$$

where  $d$  is the degree of the curve and  $m_i$  is the order of  $i$ -th singular point. To achieve this one follows the following steps:

1. Check if all the singularities, which might be defined over some extension of  $F_q$ , are ordinary. If yes compute the genus using formula (3) above. If not then go to step 2.
2. Shift the curve so that  $(0:0:1)$  is a singular (not ordinary and not terrible [1]) point. We did not have any terrible points in our case.
3. Make the curve into an excellent position; when we do that we may extend the field of coefficients.
4. Perform a quadratic transformation:

$$f(x, y, z) := x^{-d_x} y^{-d_y} z^{-d_z} f(yz, xz, xy),$$

where  $d_x$ ,  $d_y$ , and  $d_z$  are the highest degrees of  $x$ ,  $y$ , and  $z$  respectively which can be factored out of  $f(yz, xz, xy)$ .

5. Go to Step 1.

Another way to compute the genus is to use the AXIOM utility of [8]. We used those facilities to find the genus in Statements 1.1 – 3.1 and 3.3.

### 3. Computational results.

For  $q = 8$  and genus 4, Serres's upper bound is 29.

**Statement 1.1.** *We found that  $25 \leq N_8(4) \leq 29$ . Among all curves over  $F_2$  of degree 5 and genus 4, we found one curve up to the linear isomorphism, with 25  $F_8$ -rational points on its smooth model. This curve is given by the following polynomial:*

$$f(x, y, z) = (y^2 + xy + x^2)z^3 + (y^3 + x^3)z^2 + xy^3z + x^2y^3 + x^3y^2 + x^5.$$

It has 27  $F_8$ -rational points: 25 smooth and two singular points, which are nodes. The two singular points are  $(0:0:1)$  and  $(0:1:0)$ . The expansion around these points (after the suitable change of variables) is of the type:

$$f(u, v) = u^2 + uv + v^2 + \dots$$

Since the form  $u^2 + uv + v^2$  is irreducible over the field  $F_8$ , we obtain that on its smooth model there are no  $F_8$ -points above the singularities. This implies that we are 4 points less than Serre's upper bound.

For  $q = 8$  and genus 5, Serres's upper bound is 34.

**Statement 1.2.** *We found that  $26 \leq N_8(5) \leq 34$ . Among all curves over  $F_2$  of degree 5 and genus 5, we found three curves, with 26  $F_8$ -rational points on their smooth models. They are defined by the following polynomials:*

$$f_1(x, y, z) = (y^2 + xy + x^2)z^3 + (xy^2 + x^2y + x^3)z^2 + (y^4 + x^2y^2)z + x^5,$$

$$f_2(x, y, z) = x^2z^3 + (xy^2 + x^2y + x^3)z^2 + (y^4 + x^3y)z + x^3y^2 + x^4y + x^5,$$

$$f_3(x, y, z) = y^2z^3 + (xy^2 + x^2y + x^3)z^2 + (y^4 + x^2y^2 + x^3y + x^4)z + x^4y.$$

The first curve has 27  $F_8$ -rational points: 26 smooth and one singular point (node). Its singular point is  $(0:0:1)$ . Because of the same reason as in the previous statement, we conclude that this curve has 26 points on its smooth projective model. The other two curves have 26  $F_8$ -rational points (one of which is a cusp). Since their singular points are cusps, and there is one point above the cusp, we conclude that they have 26  $F_8$ -rational points on their smooth models.

The following two curves are the only ones with 25  $F_8$ -rational points on their smooth projective models:

$$g_1(x, y, z) = (y^2 + xy + x^2)z^3 + x^2yz^2 + (y^4 + x^2y^2 + x^3y + x^4)z + x^3y^2,$$

$$g_2(x, y, z) = (y^2 + xy + x^2)z^3 + x^3z^2 + y^4z + y^5 + x^3y^2 + x^4y + x^5.$$

They have 26  $F_8$ -points, one of which is a node.

For  $q = 16$  and genus 4, Serres's upper bound is 49.

**Statement 2.1.** *We found that  $45 \leq N_{16}(4) \leq 49$ . Among all curves over  $F_2$  of degree 5 and genus 4, we found one curve up to the linear isomorphism, with 45  $F_{16}$ -rational points on its smooth model. The following polynomial defines it:*

$$f(x, y, z) = (y^2 + xy + x^2)z^3 + y^3z^2 + (xy^3 + x^2y^2 + x^3y + x^4)z + x^3y^2 + x^4y + x^5.$$

It has 43  $F_{16}$ -rational points: 41 smooth and two singular points (nodes). The two singular points are  $(0:0:1)$  and  $(0:1:0)$ . The expansion around each point (after the suitable change of variables) is:

$$f(u, v) = u^2 + uv + v^2 + \dots$$



Since the form  $u^2 + uv + v^2$  is reducible over the field  $F_{16}$ , we have that on the smooth model there are 4 smooth  $F_{16}$ -points above the singularities. This implies that the number of  $F_{16}$ -rational points on its smooth projective model is 45, 4 points less than Serre's upper bound.

For  $q = 16$  and genus 5, Serres's upper bound is 57.

**Statement 2.2.** *We found that  $45 \leq N_{16}(5) \leq 57$ . Among all curves over  $F_2$  of degree 5 and genus 5, we found one curve up to the linear isomorphism, with 45  $F_{16}$ -rational points on its smooth model. This curve is given by the following equation:*

$$f(x, y, z) = xyz^3 + (xy^2 + x^2y + x^3)z^2 + y^4z + x^2y^3 + x^4y.$$

It has 44  $F_{16}$ -points: 43 smooth and one singular, a node with two rational points lying above it on its smooth model.

The next best curve (there is only one such curve) has 44  $F_{16}$ -rational points with one cusp. So, there are 44  $F_{16}$ -rational points on its smooth model:

$$g(x, y, z) = (y^2 + x^2)z^3 + xy^2z^2 + (y^4 + xy^3 + x^3y + x^4)z + y^5 + x^3y^2 + x^5.$$

For  $q = 32$  and genus 3, Serres's upper bound is 66.

**Statement 3.1.** *We found that  $63 \leq N_{32}(3) \leq 66$ . Among all curves over  $F_2$  of degree 5 and genus 3, we found one curve up to the linear isomorphism, with 63  $F_{32}$ -rational points on its smooth model. This curve is given by the following polynomial:*

$$f_2(x, y, z) = (y^2 + xy + x^2)z^3 + (y^3 + x^3)z^2 + (xy^3 + x^3y)z + x^2y^3 + x^3y^2.$$

It has 66  $F_{32}$ -points: 63 smooth and three singular points. The singular points are nodes:  $(0:0:1)$ ,  $(0:1:0)$  and  $(1:0:0)$ . Using the same argument as in Statement 1.1, one can see that there are no  $F_{32}$ -points above them on the smooth model of this curve. So, it has 63  $F_{32}$ -rational points.

For  $q = 32$  and genus 4, Serres's upper bound is 77.

**Statement 3.2.** *We found that  $70 \leq N_{32}(4) \leq 77$ . Among all curves over  $F_2$  of degree 5 and genus 4, we found one curve up to the linear isomorphism, with 70  $F_{32}$ -rational points on its smooth model. This curve is given by:*

$$f(x, y, z) = y^2z^3 + (y^3 + x^3)z^2 + (xy^3 + x^4)z + x^2y^3 + x^3y^2.$$

It has 71  $F_{32}$ -points: 69 smooth and two singular points, one node and one cusp. There are no  $F_{32}$ -points above this node, which is  $(0:1:0)$ , on the smooth model, but there is

one above cusp. Note that in this case it is easy to find its genus  $g$ . Indeed, applying (1), we obtain that  $g \leq 6 - 1 - 1 = 4$ , we may not have an equality because cusp is not an ordinary singular point. On the other hand its number of smooth  $F_{32}$ -points, which is 69 is greater than 66 (Serre's upper bound for genus 3).

For  $q = 32$  and genus 5, Serres's upper bound is 88.

**Statement 3.3.** *We found that  $73 \leq N_{32}(5) \leq 88$ . Among all curves over  $F_2$  of degree 5 and genus 5, we found three curves with 73  $F_{32}$ -rational points on their smooth models. The curves are defined by:*

$$f_1(x, y, z) = xyz^3 + (xy^2 + x^2y)z^2 + y^5 + x^5,$$

$$f_2(x, y, z) = xyz^3 + xy^2z^2 + (y^4 + x^3y)z + x^5,$$

$$f_3(x, y, z) = y^2z^3 + x^3z^2 + (x^2y^2 + x^3y)z + xy^4 + x^3y^2 + x^4y.$$

The first two curves have 72  $F_{32}$ -rational points, with one being a node. The third curve has 73  $F_{32}$ -rational points, but its singular point is a cusp.

We recall that from now on, to compute the genus of curves we use the same argument as in Statement 3.2.

For  $q = 64$  and genus 3, Serre's upper bound is 113.

**Statement 4.1** *We found that  $N_{64}(3) = 113$ . Among all curves over  $F_2$  of degree 4 and genus 3, we found four smooth curves, which have the maximal possible number of  $F_{64}$ -rational points (Serre's upper bound). The curves are defined by the polynomials:*

$$f_1(x, y, z) = yz^3 + y^2z^2 + (y^3 + x^3)z + x^3y,$$

$$f_2(x, y, z) = yz^3 + (y^2 + xy)z^2 + (y^3 + xy^2 + x^3)z + xy^3,$$

$$f_3(x, y, z) = z^4 + x^3z + xy^3,$$

$$f_4(x, y, z) = z^4 + x^2z^2 + x^3z + xy^3.$$

The first two are written in such a way that  $(0:0:1)$ ,  $(0:1:0)$  and  $(1:0:0)$  are lying on them.

For  $q = 64$  and genus 4, Serre's upper bound is 129.

**Statement 4.2** *We found that  $114 \leq N_{64}(4) \leq 129$ . Among all curves over  $F_2$  of degree 5 and genus 4, we found three curves with 114  $F_{64}$ -rational points on their smooth*

model. The following polynomials define them:

$$f_1(x, y, z) = (y^2 + xy + x^2)z^3 + (y^3 + xy^2)z^2 + (x^2y^2 + x^4)z + x^2y^3 + x^5,$$

$$f_2(x, y, z) = (y^2 + xy + x^2)z^3 + (x^2y + x^3)z^2 + x^2y^2z + x^2y^3 + x^5,$$

$$f_3(x, y, z) = (y^2 + xy + x^2)z^3 + (xy^2 + x^3)z^2 + (xy^3 + x^2y^2)z + x^2y^3 + x^5.$$

The first two have 113  $F_{64}$ -rational points, two of them are singular: one cusp and one node. There are two points on the smooth model lying above the node. The third one has 112  $F_{64}$ -rational points, two of them are nodes, with two points on its smooth model above each singularity.

For  $q = 64$  and genus 5, Serre's upper bound is 145.

**Statement 4.3** *We found that  $130 \leq N_{64}(5) \leq 145$ . Among all curves over  $F_2$  of degree 5 and genus 5, we found one curve with 130  $F_{64}$ -rational points on its smooth model. It is defined by:*

$$f(x, y, z) = xyz^3 + (xy^2 + x^2y)z^2 + (y^4 + x^4)z + x^3y^2.$$

It has 129  $F_{64}$ -rational points, one is a node. Hence, its genus is 5, because node is an ordinary singular point.

The following two curves are the only ones with 129  $F_{64}$ -rational points on their smooth models (both have 128  $F_{64}$ -rational points):

$$g_1(x, y, z) = (y^2 + xy + x^2)z^3 + x^3z^2 + xy^4 + x^4y,$$

$$g_2(x, y, z) = (y^2 + xy)z^3 + x^3z^2 + xy^4 + x^4y.$$

For  $q = 128$  and genus 3, Serre's upper bound is 195.

**Statement 5.1** *We found that  $184 \leq N_{128}(3) \leq 195$ . Among all curves over  $F_2$  of degree 4 and genus 3, we found two smooth curves with 184  $F_{128}$ -rational points. The curves are defined by:*

$$f_1(x, y, z) = yz^3 + (y^2 + xy + x^2)z^2 + (y^3 + x^3)z + x^4,$$

$$f_2(x, y, z) = (y + x)z^3 + (y^2 + xy + x^2)z^2 + y^3z + x^4.$$

Next best curve has one point less on its smooth model. The curve is defined by:

$$g(x, y, z) = xz^3 + xyz^2 + (x^2y + x^3)z + y^4 + x^2y^2 + x^4.$$

For  $q = 128$  and genus 4, Serre's upper bound is 217.

**Statement 5.2** *We found that  $197 \leq N_{128}(4) \leq 217$ . Among all curves over  $F_2$  of degree 5 and genus 4, we found one curve with 197  $F_{128}$ -rational points on its smooth model. The curve is defined by:*

$$f(x, y, z) = (y^2 + xy + x^2)z^3 + (y^3 + x^2y)z^2 + (xy^3 + x^2y^2 + x^4)z + x^2y^3 + x^3y^2 + x^5.$$

It has 197 smooth  $F_{128}$ -rational points and 2 nodes, with no rational points above nodes on its smooth model, because the form  $x^2 + xy + y^2$  is irreducible over the field  $F_{128}$ .

For  $q = 128$  and genus 5, Serre's upper bound is 239.

**Statement 5.3** *We found that  $227 \leq N_{128}(5) \leq 239$ . Among all curves over  $F_2$  of degree 5 and genus 5, we found one curve with 227  $F_{128}$ -rational points on its smooth model. The curve is defined by:*

$$f(x, y, z) = (y^2 + xy + x^2)z^3 + x^3z^2 + (x^2y^2 + x^3y + x^4)z + y^5.$$

It has 228  $F_{128}$ -rational points, but one of them is a node with no rational points above it in the smooth model.

The next best curve has 221 points on its smooth model. The curve is defined by:

$$g(x, y, z) = (y^2 + xy)z^3 + x^2y^2z + y^5 + x^3y^2 + x^5,$$

with 220  $F_{128}$ -rational points on it.

For  $q = 256$  and genus 3, Serres's upper bound is 353.

**Statement 6.1** *We found that  $350 \leq N_{256}(3) \leq 353$ . Among all curves over  $F_2$  of degree 4 and genus 3, we found three smooth curves with 350  $F_{256}$ -rational points. The curves are defined by:*

$$f_1(x, y, z) = xz^3 + y^2z^2 + (x^2y + x^3)z + xy^3 + x^2y^2 + x^4,$$

$$f_2(x, y, z) = xz^3 + (y^2 + x^2)z^2 + (x^2y + x^3)z + xy^3 + x^2y^2 + x^3y,$$

$$f_3(x, y, z) = z^4 + (y^2 + xy + x^2)z^2 + (xy^2 + x^2y)z + y^4 + x^2y^2 + x^4.$$

The last curve has no  $F_2$ -rational points.

For  $q = 256$  and genus 4, Serres's upper bound is 385.

**Statement 6.2.** *We found that  $381 \leq N_{256}(4) \leq 385$ . Among all curves over  $F_2$  of degree 5 and genus 4, we found three curves with 381  $F_{256}$ -rational points on their smooth models. They are defined by:*

$$f_1(x, y, z) = (y^2 + x^2)z^3 + x^3z^2 + (x^2y^2 + x^3y)z + x^2y^3 + x^4y + x^5,$$

$$f_2(x, y, z) = y^2z^3 + (x^2y + x^3)z^2 + (xy^3 + x^2y^2 + x^4)z + x^5,$$

$$f_3(x, y, z) = (y^2 + xy + x^2)z^3 + (xy^2 + x^3)z^2 + (xy^3 + x^2y^2)z + x^4y + x^5.$$

The curves have different kinds of singularities and different numbers of  $F_{256}$ -rational points. The first one has 381  $F_{256}$ -points: 379 smooth and two cusps. The second one has 380  $F_{256}$ -points: 378 smooth and two singular points, one cusp and one node. The third one has 379  $F_{256}$ -points: 377 smooth and two nodes. Again the genus of curves can be computed as in Statement 3.2.

For  $q = 256$  and genus 5, Serres's upper bound is 417.

**Statement 6.3.** *We found that  $388 \leq N_{256}(5) \leq 417$ . Among all curves over  $F_2$  of degree 5 and genus 5, we found two curves with 388  $F_{256}$ -rational points on their smooth models. The curves are defined by:*

$$f_1(x, y, z) = (xy + x^2)z^3 + x^3yz + y^5 + x^2y^3 + x^4y,$$

$$f_2(x, y, z) = (y^2 + xy + x^2)z^3 + (x^3y + x^4)z + xy^4 + x^2y^3 + x^5.$$

In both cases the singularities are nodes, so there are two rational points on their smooth models, lying above each node.

For  $q = 512$  and genus 3, Serres's upper bound is 648.

**Statement 7.1.** *We found that  $640 \leq N_{512}(3) \leq 648$ . Among all curves over  $F_2$  of degree 4 and genus 3, we found one smooth curve with 640  $F_{512}$ -rational points. The curve is defined by:*

$$f(x, y, z) = xz^3 + x^2z^2 + (x^2y + x^3)z + y^4 + xy^3.$$

The next best smooth curve has 631  $F_{512}$ -rational points and is the only one with such number of rational points:

$$g(x, y, z) = xz^3 + y^2z^2 + (y^3 + x^3)z + y^4 + x^3y + x^4.$$

For  $q = 512$  and genus 4, Serres's upper bound is 693.

**Statement 7.2.** *We found that  $661 \leq N_{512}(4) \leq 693$ . Among all curves over  $F_2$  of degree 5 and genus 4, we found 7 curves with 661  $F_{512}$ -rational points on their smooth models. The curves are defined by:*

$$f_1(x, y, z) = (y^2 + xy)z^3 + (y^3 + x^3)z^2 + x^4z + x^2y^3,$$

$$f_2(x, y, z) = (y^2 + xy)z^3 + (y^3 + xy^2 + x^2y)z^2 + x^4z + x^3y^2 + x^4y,$$

$$f_3(x, y, z) = (y^2 + xy)z^3 + x^3z^2 + x^4z + x^2y^3 + x^4y,$$

$$f_4(x, y, z) = (y^2 + xy)z^3 + y^3z^2 + xy^3z + x^3y^2 + x^5,$$

$$f_5(x, y, z) = (xy + x^2)z^3 + y^3z^2 + xy^3z + x^3y^2 + x^4y,$$

$$f_6(x, y, z) = (y^2 + xy)z^3 + x^3z^2 + (xy^3 + x^4)z + x^3y^2 + x^4y,$$

$$f_7(x, y, z) = (y^2 + xy)z^3 + (y^3 + xy^2 + x^2y + x^3)z^2 + (xy^3 + x^2y^2 + x^3y)z + x^5.$$

The first three have 660  $F_{512}$ -rational points. They have two singular points: one node, giving two rational points above it on the smooth model, and one cusp. The other four curves have 659  $F_{512}$ -rational points. Their singular points are nodes. There are two rational points on the smooth models above each node.

For  $q = 512$  and genus 5, Serres's upper bound is 738.

**Statement 7.3.** *We found that  $724 \leq N_{512}(5) \leq 738$ . Among all curves over  $F_2$  of degree 5 and genus 5, we found one curve with 724  $F_{512}$ -rational points on its smooth model. The curve is defined by:*

$$f(x, y, z) = xyz^3 + xy^2z^2 + (x^2y^2 + x^3y)z + y^5 + x^5.$$

It has 723  $F_{512}$ -rational points, one of which is a node, giving two rational points above it on the smooth model.

The next best curve has 697 rational points on its smooth model. It is the only one up to the linear isomorphism:

$$g(x, y, z) = (y^2 + xy)z^3 + x^3z^2 + (y^4 + x^2y^2)z + y^5 + x^5,$$

with 696  $F_{512}$ -rational points.

#### 4. Conclusions.

We summarize our results, adding the previously known ones (see [2]), in the following table:

$F_q$	genus 3		genus 4		genus 5	
	best known	Serre's u.b.	best known	Serre's u.b.	best known	Serre's u.b.
8	24 [2]	24	25	29	26	34
16	38 [2]	41	45	49	45	57
32	63	66	70	77	73	88
64	113	113	114	129	130	145
128	184	195	197	217	227	239
256	350	353	381	385	388	417
512	640	648	661	693	724	738

It is possible to use the desingularized curves for construction of algebraic geometric Goppa codes [5, 6, 7]. The resulting  $q$ -ary codes are interested also for construction of good binary linear codes, using the known concatenation methods. Here we should mention the paper [9], where new binary linear and nonlinear codes with the best known parameters have been obtained using algebraic geometric  $q$ -ary codes from curves of small genus.

#### Acknowledgements

Authors wish thank Paul Camion for his support of this project and Dominique Le Brigand for the useful remarks and corrections. We are indebted to Gaetan Hache for his programming package [8] and for the useful discussions.

## References

- [1] W. Fulton. *Algebraic Curves: An Introduction to Algebraic Geometry*, W. A. Benjamin Inc., New York, 1969.
- [2] J.-P. Serre, "Nombres de points des courbes algebriques sur  $F_q$ , Seminaire de Theorie des Nombres de Bordeaux, expose 22, pp. 1-8, 1983.
- [3] J.-P. Serre, "Rational points on curves over finite fields, " $q$  large", " Parts I and II, Lectures given at Harvard University, September-December, 1985, Notes by Fernando Gouvea, Serre, 1985.
- [4] D. Polemi, C. J. Moreno, O. J. Moreno. "Search and construction of good a.g. Goppa codes," submitted to *IEEE Trans. on Inform. Theory*.
- [5] V. D. Goppa. *Geometry and Codes*, Kluwer Academic Publishers, The Netherlands, 1988.
- [6] S. G. Vladut and Yu. I. Manin. "Linear codes and modular curves," *Journal of Soviet Mathematics*, 1985, v. 30, no. 6, pp. 2611-2643.
- [7] D. Le Brigand and J. J. Risler. "Algorithm de Brill-Noether et codes de Goppa," *Bull. Soc. Math. France*, 1988, v. 116, pp. 231-253.
- [8] G. Hache and D. Le Brigand. "Effective Construction of Algebraic Geometry Codes," *Rapport de Recherche INRIA N° 2267*, 1994; submitted to *IEEE*.
- [9] A. M. Barg, G. L. Katsman and M. A. Tsfasman, "Algebraic geometric codes from curves of small genus," *Problems of Information Transmission*, 1987, v. 23, no. 1, pp. 34-38.





---

Unité de recherche INRIA Rocquencourt  
Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 Le Chesnay Cedex (France)

Unité de recherche INRIA Lorraine - Technopôle de Nancy-Brabois - Campus scientifique  
615, rue du Jardin Botanique - B.P. 101 - 54602 Villers lès Nancy Cedex (France)

Unité de recherche INRIA Rennes - IRISA, Campus universitaire de Beaulieu 35042 Rennes Cedex (France)

Unité de recherche INRIA Rhône-Alpes 46, avenue Félix Viallet - 38031 Grenoble Cedex 1 (France)

Unité de recherche INRIA Sophia Antipolis - 2004, route des Lucioles - B.P. 93 - 06902 Sophia Antipolis Cedex (France)

---

Éditeur  
INRIA - Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 Le Chesnay Cedex (France)

ISSN 0249 - 6399



★ R R - 2 3 2 7 ★