

ERROR-CORRECTING CODES ON LOW RANK SURFACES

MARCOS ZARZAR

ABSTRACT. In this paper we construct some algebraic geometric error-correcting codes on surfaces whose Neron-Severi group has low rank. If the rank of the Neron-Severi group is 1, the intersection of this surface with an irreducible surface of lower degree will be an irreducible curve, and this makes possible the construction of codes with good parameters. Rank 1 surfaces are not easy to find, but we are able to find surfaces with low rank, and those will give us good codes too.

1. INTRODUCTION

In the eighties the Russian mathematician and engineer V. D. Goppa introduced the idea of constructing error-correcting codes on algebraic curves by evaluating certain spaces of functions on points of a curve. Let \mathbb{F}_q denote the finite field with q elements. Let C be an algebraic curve of genus g defined over \mathbb{F}_q , $D = P_1 + P_2 + \dots + P_n$ and G divisors on C such that $\text{supp}(D) \cap \text{supp}(G) = \emptyset$. Let

$$\mathcal{L}(G) = \{f \in \mathbb{F}_q(C) \mid (f) \geq -G\} \cup \{0\}.$$

Observe that $\mathcal{L}(G)$ is a \mathbb{F}_q -vector space. The Geometric Goppa code associated with the divisors D and G is defined as the image of the map

$$\begin{aligned} \varphi: \mathcal{L}(G) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), f(P_2), \dots, f(P_n)) \end{aligned}$$

The Riemann-Roch theorem gives us a lower bound for the minimum distance, and so the parameters for this code are $k = \dim(G) - \dim(G - D)$ and $d \geq n - \deg(G)$. On curves, points can be thought as divisors, and the Riemann-Roch theorem makes possible a good description of these codes. The construction of Goppa works for any algebraic variety, not necessarily for curves only. The construction of good codes

Keywords: error-correcting codes, algebraic geometric codes, Weil restriction of scalars, algebraic surfaces.

on higher dimensional varieties is more complicated, by the simple fact that, generally speaking, it is not easy to estimate and control the number of zeroes of algebraic functions on higher dimensional varieties. The reason for constructing codes on surfaces whose Neron-Severi group has rank 1 is the following: if we intersect it with an irreducible surface of lower degree (both surfaces in \mathbb{P}^3), we obtain an irreducible curve, and this results in good parameters for the code. Unfortunately, surfaces with rank 1 are not easy to find, but we are able to construct good codes using surfaces with low rank, not necessarily 1.

2. A FIRST CASE

In [5], Swinnerton-Dyer lists all the possibilities for the zeta function of a non-singular cubic surface over a finite field. We can check on Class 12 of Table 1, page 57 of [5], that it is possible to have a cubic surface defined over \mathbb{F}_q with $q^2 + 2q + 1$ points, and having Neron-Severi group of rank 1 (since there is no η_i of order 1). The existence of such a surface allows the construction of a good code. To estimate the minimal distance of the code, we need the following lemma.

Lemma 2.1. *Let $X \subset \mathbb{P}^3$ be a smooth surface of degree d defined over \mathbb{F}_q . Assume that the rank of the Neron-Severi group of X is 1. Let $Y \subset \mathbb{P}^3$ be an irreducible surface of degree $m < d$ defined over \mathbb{F}_q . Then $X \cap Y$ is irreducible.*

Proof:

Step 1: $Pic^o(X) = 0$ (this works for any smooth surface in \mathbb{P}^3).

Proof: Mumford (in [3], theorem on page 196) shows that

$$\dim(Pic^o(X)) \leq \dim(H^1(X, \mathcal{O}_X))$$

and since $X \subset \mathbb{P}^3$ and X is smooth, Beauville (in [1], page 99, Lemma VIII.9) shows that

$$\dim(H^1(X, \mathcal{O}_X)) = 0$$

and so $\dim(Pic^o(X)) = 0$.

Step 2: Let C_0 be a plane section of X . Then $NS(X) = C_0\mathbb{Z}$.

Proof: By hypothesis, $NS(X)$ is cyclic of rank 1 so if D is a generator, $C_0 \sim nD$ for some $n \in \mathbb{Z}$, and without loss of generality (replacing D by $-D$ if necessary) $n > 0$. By step 1 above, C_0 is already equal to

nD , i.e there exists a plane H with $nD = H \cap X$. Suppose that x, y and z are affine coordinates and H is given by $z = 0$. So $X \cap H$ is given by $h(x, y)^n$. But then

$$g(x, y, z) = h(x, y)^n + zR(x, y, z)$$

for some R (here g is such that X is given by $g = 0$). So

$$g_x = nh^{n-1}h_x + zR_x$$

$$g_y = nh^{n-1}h_y + zR_y$$

$$g_z = zR_z + R$$

and we observe that any point with $h = R = 0$ is a singularity of X , contradicting its smoothness.

Step 3: If Y is an irreducible surface in \mathbb{P}^3 of degree $m < d$ then $X \cap Y$ is irreducible.

Proof: Suppose $X \cap Y$ is reducible, so let $X \cap Y = C_1 \cup C_2$. Then, by step 2 above, $C_i \sim a_i C_0$ with $a_1 + a_2 = m$, and by step 1 this is a linear equivalence. So there exist polynomials f_1 and f_2 in $\mathbb{F}_q[z_0, z_1, z_2, z_3]$ such that

$$(f_1) = C_1 - a_1 C_0,$$

$$(f_2) = C_2 - a_2 C_0$$

and

$$(f_1 f_2) = C_1 + C_2 - m C_0.$$

On the other hand,

$$(f) = C_1 + C_2 - m C_0,$$

where $f = 0$ is the equation for Y , so

$$\left(\frac{f_1 f_2}{f} \right) = (0)$$

which implies that $\exists \lambda \in k$ such that $f_1 f_2 = \lambda f$ as functions on X , i.e, $g | (f_1 f_2 - \lambda f)$. But $\deg(g) = d$, and $\deg(f_1 f_2 - \lambda f) = m < d$, so $f_1 f_2 = \lambda f$ as polynomials, and f factors so Y is reducible. \square

Note: Observe that Lemma 2.1 does not work if we drop the condition $m < d$. To see this, consider the following example: Let X be given by $\{g = 0\}$. Start with f_1 and f_2 such that $\deg(f_1) + \deg(f_2) = d$. So $X \cap \{f_1 f_2 = 0\}$ is reducible (call Y_0 the surface given by $\{f_1 f_2 = 0\}$). Then $Y_\lambda : f_1 f_2 + \lambda g$ is a pencil of surfaces with an irreducible member $(X, \lambda = \infty)$ so a generic member is irreducible but $X \cap Y_\lambda = X \cap Y_0$ is

reducible.

Back to the code, remember that we need to find a cubic surface S defined over \mathbb{F}_q containing $q^2 + 2q + 1$ points and having Neron-Severi group of rank 1. If we can manage to find such a surface with the additional condition that there exists a plane that does not intersect it, we can build a code of length $q^2 + 2q + 1$ by making the plane that does not intersect the surface the plane at infinity. Using random searching, we were able to find surfaces in \mathbb{P}^3 over \mathbb{F}_9 satisfying these requirements. So let us estimate the parameters of such a code in \mathbb{F}_9 . First, since $q = 9$, we have a surface S with 100 points, which gives us a code of length 100. Using sections of degree at most 2, we have that the dimension of the code is at most 10 (and since S has enough points, we will see that the dimension is exactly 10). Take the linear space of sections to be generated by

$$\{x^2, xy, xz, x, y^2, yz, y, z^2, z, 1\}.$$

Taking a surface $Q \subseteq \mathbb{P}^3$ of degree 2, we see that the intersection $S \cap Q$ is either an irreducible curve or two plane cubics (note that only these are possible because of Lemma 2.1). Let us estimate the maximum number of points on the intersection:

Irreducible case: using the adjunction formula, we see that such a curve has genus $g \leq 4$. If $g = 4$, we can use the Stöhr-Voloch bound [4] for the number of points, since it admits a classical system. For a curve $C \in \mathbb{P}^n(\mathbb{F}_q)$ of degree d and genus g , we have that the number of points N is bounded by

$$N \leq \frac{1}{n}(n(n-1)(g-1) + d(q+n))$$

which in our case ($n = 3, q = 9, g = 4, d = 6$) gives us $N \leq 30$. Observe that this is better than Serre's improvement to Weil's bound $N \leq q + 1 + g[2\sqrt{q}] = 34$. If $g < 4$ we can use Weil's bound, and have $N \leq q + 1 + g[2\sqrt{q}] \leq 28$

Two plane cubics: we know that the genus of a plane cubic is 1, and we use Weil's bound to estimate the number of points, so $N \leq 2(q + 1 + g[2\sqrt{q}]) = 32$.

If $Q \subseteq \mathbb{P}^3$ has degree 1, then Q is a plane, and the intersection is a plane cubic, which has at most 16 points.

We conclude that constructing a code over \mathbb{F}_9 using S with 100 points by evaluating functions of degree at most 2, we will obtain an error-correcting code of length 100, dimension at most 10 and minimum distance at least 68. As mentioned before, we have found surfaces satisfying the conditions needed. The surface

$$v_f = [g, g, g^2, g^2, g^5, g^7, g^2, g^2, 1, 0, g, g^5, 2, g^6, g^3, g, 1, g^6, g^2, g^7]$$

and the plane

$$h(x, y, z, w) = g^6x + 2y + 2z + w - 1$$

give us a $[100, 10, 68]$ code, showing that the bounds for dimension and minimal distance are actually attained. For ease of notation, we represent the surface as a vector v_f of length 20,

$$v_f = [c_{x^3}, c_{x^2y}, c_{x^2z}, c_{x^2w}, c_{xy^2}, c_{xyz}, c_{xyw}, c_{xz^2}, \dots, c_{z^2w}, c_{zw^2}, c_{w^3}],$$

where c_m is the coefficient of the monomial m in the polynomial $f \in \mathbb{F}_9[x, y, z, w]$ that defines S . Also, we write the coefficients in terms of g , a generator of the group \mathbb{F}_9^* . The non-intersecting plane is given by the polynomial $h \in \mathbb{F}_9[x, y, z, w]$.

3. ZETA FUNCTION AND TATE'S CONJECTURE

Given a variety X of dimension n defined over \mathbb{F}_q , we denote the number of points of X whose coordinates lie in \mathbb{F}_{q^r} by N_r . The zeta function of X is defined as

$$(1) \quad Z_X(t) = \exp \left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r} \right).$$

By results of Dwork, Grothendieck and Deligne, we have that $Z_X(t)$ is a rational function that can be written as

$$(2) \quad Z_X(t) = \frac{P_1(t)P_3(t)\dots P_{2n-1}(t)}{P_0(t)P_2(t)\dots P_{2n}(t)}$$

where $P_0(t) = 1 - t$, $P_{2n}(t) = 1 - q^n t$ and for $1 \leq i \leq 2n - 1$, $P_i(t)$ is a polynomial with integer coefficients, and it can be written as

$$P_i(t) = \prod_{j=1}^{B_i} (1 - \alpha_{ij}t)$$

where the α_{ij} are algebraic integers with $|\alpha_{ij}| = q^{\frac{i}{2}}$, and B_i is the i^{th} Betti number of X . From (1) and (2) it is easy to find that

$$(3) \quad N_r = 1 + q^{nr} + \sum_{i=1}^{2n-1} \left(\sum_{j=1}^{B_i} (-1)^i \alpha_{ij}^r \right).$$

In particular, for surfaces, we have that

$$(4) \quad N_r = 1 + q^{2r} + \sum_{i=1}^3 \left(\sum_{j=1}^{B_i} (-1)^i \alpha_{ij}^r \right)$$

and this will be important to estimate the rank of the Neron-Severi group of a surface. In [6], Tate has conjectured that the rank of the Neron-Severi group of a surface S equals the number of α_{2j} in (4) with $\alpha_{2j} = q$. Although equality has not been proved yet, on the same paper he proves that $\text{rk}(NS(S)) \leq \#\{\alpha_{2j} | \alpha_{2j} = q\}$.

4. WEIL RESTRICTION OF SCALARS AND NERON-SEVERI RANK

Let C be a plane curve defined over \mathbb{F}_{q^2} by $f(x, y) = 0$, but not defined over \mathbb{F}_q . Let $g = \text{genus}(C)$. Let $\{1, \alpha\}$ be a basis for \mathbb{F}_{q^2} as a \mathbb{F}_q -vector space, with (it will become clear later why we have picked α satisfying this condition)

$$\sigma(\alpha) = \begin{cases} -\alpha & \text{if } 2 \nmid q; \\ -\alpha + 1 & \text{if } 2 \mid q. \end{cases}$$

If x and y are in \mathbb{F}_{q^2} , we can write

$$\begin{aligned} x &= x_1 + \alpha x_2 \\ y &= y_1 + \alpha y_2 \end{aligned}$$

uniquely with $x_1, x_2, y_1, y_2 \in \mathbb{F}_q$. Moreover, we have that

$$\begin{aligned} f(x, y) &= f(x_1 + \alpha x_2, y_1 + \alpha y_2) \\ &= f_1(x_1, x_2, y_1, y_2) + \alpha f_2(x_1, x_2, y_1, y_2) \end{aligned}$$

with $f_1(x_1, x_2, y_1, y_2), f_2(x_1, x_2, y_1, y_2) \in \mathbb{F}_q[x_1, x_2, y_1, y_2]$. So we can consider the surface S (in 4-dimensional space) defined over \mathbb{F}_q by $f_1(x_1, x_2, y_1, y_2) = f_2(x_1, x_2, y_1, y_2) = 0$. The surface S is denoted by $W_{\mathbb{F}_{q^2}/\mathbb{F}_q}(C)$ and it is called the Weil restriction of scalars of C over \mathbb{F}_{q^2} . This is a particular case of the general construction: let k be a finite field and K a Galois extension of k of degree n . Let C be a curve defined over K but not over k . The Weil restriction of scalars of C

over K (denoted by $W_{K/k}(C)$) is a variety of dimension n defined over k .

Proposition 4.1. *Given C and $S = W_{\mathbb{F}_{q^2}/\mathbb{F}_q}(C)$ as above, we have that*

$$\#S(\mathbb{F}_{q^k}) = \begin{cases} \#C(\mathbb{F}_{q^{2k}}) & \text{if } k \text{ is odd;} \\ (\#C(\mathbb{F}_{q^k}))^2 & \text{if } k \text{ is even.} \end{cases}$$

Proof: The odd case is straightforward. It follows directly from the construction, since we have that C is defined over $\mathbb{F}_{q^{2k}}$, but it is not defined over \mathbb{F}_{q^k} (if it were defined over \mathbb{F}_{q^k} , then it would be also on $\mathbb{F}_{q^k} \cap \mathbb{F}_{q^2} = \mathbb{F}_q$, contradicting our original assumption). So we are left to prove the case k even. For that, we are going to show that

$$S \cong C \times C^\sigma$$

over \mathbb{F}_{q^k} with k even. First, observe that k even implies that $\alpha \in \mathbb{F}_{q^k}$. Using the notation as above for f, f^σ, f_1 and f_2 (with the only difference that now we consider f^σ a polynomial on the variables z and w) we have that we need to show

$$\mathbb{F}_{q^k}[x_1, x_2, y_1, y_2]_{(f_1, f_2)} \cong \left(\mathbb{F}_{q^k}[x, y]_{(f)} \right) \otimes_{\mathbb{F}_{q^k}} \left(\mathbb{F}_{q^k}[z, w]_{(f^\sigma)} \right).$$

We have that

$$\left(\mathbb{F}_{q^k}[x, y]_{(f)} \right) \otimes_{\mathbb{F}_{q^k}} \left(\mathbb{F}_{q^k}[z, w]_{(f^\sigma)} \right) \cong \mathbb{F}_{q^k}[x, y, z, w]_{(f, f^\sigma)}$$

and so

$$\mathbb{F}_{q^k}[x_1, x_2, y_1, y_2]_{(f_1, f_2)} \cong \mathbb{F}_{q^k}[x, y, z, w]_{(f, f^\sigma)}$$

follows easily from the identifications (and now becomes clear the choice we made for α)

$$\begin{aligned} x &\longleftrightarrow x_1 + \alpha x_2 \\ y &\longleftrightarrow y_1 + \alpha y_2 \\ z &\longleftrightarrow x_1 + \sigma(\alpha)x_2 \\ w &\longleftrightarrow y_1 + \sigma(\alpha)y_2 \quad \square \end{aligned}$$

With the result of proposition 4.1 and using Tate's conjecture, we are now able to estimate the rank of the Neron-Severi group of a surface S constructed as above. In the case k odd, we have that

$$\begin{aligned} \#S(\mathbb{F}_{q^k}) &= \#C(\mathbb{F}_{q^{2k}}) \\ &= 1 + q^{2k} - \sum_{j=1}^{2g} \alpha_j^{2k} \end{aligned}$$

where the last equality follows from (3) with $n = 1$, and in this case, $B_1 = 2g$. The result above could lead us to think that $\text{rk}(NS(S)) \leq 2g$. But we have to consider that an eigenvalue and its negative might occur simultaneously, so cancellations can be happening there. So let us take a look at the case k even:

$$\begin{aligned}
\#S(\mathbb{F}_{q^k}) &= (\#C(\mathbb{F}_{q^k}))^2 \\
&= \left(1 + q^k - \sum_{j=1}^{2g} \alpha_j^k\right)^2 \\
&= 1 + 2q^k + q^{2k} - 2(1 + q^k) \left(\sum_{j=1}^{2g} \alpha_j^k\right) + \left(\sum_{j=1}^{2g} \alpha_j^k\right)^2 \\
&= 1 + 2q^k + q^{2k} - 2 \sum_{j=1}^{2g} \alpha_j^k - 2 \sum_{j=1}^{2g} (q\alpha_j)^k + \left(\sum_{j=1}^{2g} \alpha_j^k\right)^2
\end{aligned}$$

Observe that eigenvalues equal to q can only come from the terms $2q^k$ and $\left(\sum_{j=1}^{2g} \alpha_j^k\right)^2$, since $|\alpha_j| = q^{\frac{1}{2}}$. Also, note that the α_j occur in pairs, i.e, α_j and $\sigma(\alpha_j)$ are both reciprocal of roots of the polynomial $P_1(t)$ in the zeta function of C . These facts imply that $\left(\sum_{j=1}^{2g} \alpha_j^k\right)^2$ will contribute with, at least $2g$, and at most $4g^2$ eigenvalues equal to q , which gives us the estimate

$$2 + 2g \leq \text{rk}(NS(S)) \leq 2 + 4g^2,$$

where the second inequality follows from Tate's result in [6], and the first inequality follows from the fact that Tate's conjecture is true for product of curves, proved by himself in [7].

5. SOME CODES

We are able now to construct some surfaces and estimate the rank of its Neron-Severi group. We have shown how the rank depends on the genus of the curve C , so we do not want to work with curves of high genus. The first attempt was to use Weil's descent of elliptic curves. We have found reasonable codes, but nothing very impressive. One can say that this happened because the surfaces did not have many points. Roughly speaking, our codes are good if given the surface and a space of curves on this surface, we can get many points laying "outside" of each of these curves. Again, in general terms, we expect a surface to have

the square of number of points that a curve has, so it is reasonable to expect that if we do not have many points on the surface, the difference can not be big enough to give us a good code. With that in mind, we used hyperelliptic curves instead, and we have found better ones. We have constructed codes over \mathbb{F}_7 using sections of degree at most 2, more specifically, we took the 11-dimensional \mathbb{F}_7 -linear space generated by

$$\{x_1 + x_2, y_1 + y_2, gx_1 + \bar{g}x_2, gy_1 + \bar{g}y_2, x_1x_2, y_1y_2, gx_1y_2 + \bar{g}x_2y_1, x_1y_1 + x_2y_2, gx_1y_1 + \bar{g}x_2y_2, x_1y_2 + x_2y_1\}$$

(where $\bar{g} = \sigma(g)$, σ the Frobenius automorphism of \mathbb{F}_{49} , g a generator of \mathbb{F}_{49}^*), and we have found codes with the parameters displayed on Table 1 (n is the length, k is the dimension, d is the minimal distance, d_{best} is the best minimal distance found so far, considering the bounds on minimal distance on linear codes kept by Andries Brower in [8] and $f(x, y) \in \mathbb{F}_{49}[x, y]$ is the polynomial that defines a hyperelliptic curve that gave such a code).

n	k	d	d_{best}	f
50	11	27	28	$y^2 + 6x^5 + g^{27}x^3 + g^6x^2 + g^{38}x + g^{42}$
48	11	26	27	$y^2 + 6x^5 + g^{28}x^3 + g^4x^2 + g^{44}x + g^{26}$
42	11	22	23	$y^2 + 6x^5 + g^{29}x^3 + g^{29}x^2 + g^{19}x + g^{19}$
41	11	21	22	$y^2 + 6x^5 + g^{30}x^3 + g^{33}x^2 + g^7$
40	11	20	21	$y^2 + 6x^5 + g^{27}x^3 + g^{25}x^2 + g^{27}x + g^{43}$
39	11	19	20	$y^2 + 6x^5 + g^{27}x^3 + g^{27}x^2 + g^{26}x + g^{30}$
38	11	19	19	$y^2 + 6x^5 + g^{27}x^3 + g^{28}x^2 + 4x + g^{37}$
37	11	18	19	$y^2 + 6x^5 + g^{27}x^3 + g^{29}x^2 + g^{25}x + g^{26}$
36	11	17	18	$y^2 + 6x^5 + g^{27}x^3 + g^{31}x^2 + g^{25}x + g^{27}$
35	11	17	18	$y^2 + 6x^5 + g^{30}x^3 + g^5x^2 + g^{28}x + 1$
34	11	16	17	$y^2 + 6x^5 + g^{30}x^3 + g^{41}x^2 + g^2x + g^{22}$
33	11	15	16	$y^2 + 6x^5 + g^{30}x^3 + 5x^2 + g^{22}x + g^{38}$
31	11	14	15	$y^2 + 6x^5 + g^{30}x^3 + g^{10}x^2 + g^{37}x + g^{19}$
30	11	13	14	$y^2 + 6x^5 + g^{30}x^3 + g^{33}x^2 + g^{36}x + g^{23}$
29	11	12	13	$y^2 + 6x^5 + g^{30}x^3 + g^{33}x^2 + g^{26}x + g^{28}$
28	11	12	13	$y^2 + 6x^5 + g^{29}x^3 + 6x^2 + g^{14}x + g^{14}$

TABLE 1. Best codes found over \mathbb{F}_7 with $n \leq 50$

We have also found some codes of length higher than 50, but since Brower's tables do not have yet d_{best} for linear codes over \mathbb{F}_7 with

$n \geq 51$ we compare the codes we have found with the best existing ones over \mathbb{F}_5 and \mathbb{F}_8 . These are shown on Table 2.

n	k	d	d_{best}/\mathbb{F}_5	d_{best}/\mathbb{F}_8	f
71	11	42	41	47	$y^2 + 6x^5 + g^{30}x^3 + g^{28}x^2 + g^{38}x + 3$
70	11	41	40	46	$y^2 + 6x^5 + g^{27}x^3 + g^{29}x^2 + 2x + g^{47}$
69	11	41	39	45	$y^2 + 6x^5 + g^{27}x^3 + g^{31}x^2 + g^{38}x + 6$
68	11	40	39	44	$y^2 + 6x^5 + g^{27}x^3 + g^{25}x^2 + g^{17}x + g^{12}$
67	11	39	38	43	$y^2 + 6x^5 + g^{27}x^3 + 4x^2 + g^{31}x + g^{47}$
65	11	38	37	42	$y^2 + 6x^5 + g^{27}x^3 + g^{26}x^2 + g^{33}x + g^{35}$
64	11	37	36	42	$y^2 + 6x^5 + g^{27}x^3 + g^{31}x^2 + 4x + g^{38}$
62	11	36	35	40	$y^2 + 6x^5 + g^{27}x^3 + g^{26}x^2 + g^{44}x + g^{37}$
59	11	34	33	37	$y^2 + 6x^5 + g^{30}x^3 + g^{42}x^2 + g^{27}x + g^{20}$
58	11	33	32	36	$y^2 + 6x^5 + g^{27}x^3 + g^{34}x^2 + g^{33}x + g^{42}$
57	11	32	31	35	$y^2 + 6x^5 + g^{27}x^3 + g^{25}x^2 + g^{36}x + g^{34}$
56	11	31	30	34	$y^2 + 6x^5 + g^{27}x^3 + g^{25}x^2 + g^{38}x + g^{26}$
54	11	30	29	32	$y^2 + 6x^5 + g^{27}x^3 + g^{27}x^2 + g^{26}x + g^{26}$
53	11	29	28	31	$y^2 + 6x^5 + g^{27}x^3 + g^{29}x^2 + g^{29}x + g^{30}$
52	11	29	27	30	$y^2 + 6x^5 + g^{30}x^3 + g^{42}x^2 + g^{18}x + 1$
51	11	28	27	29	$y^2 + 6x^5 + g^{27}x^3 + g^{29}x^2 + g^9x + g^{44}$

TABLE 2. Best codes found over \mathbb{F}_7 with $n > 50$

Since it would not be very practical to display here all the equations for the hyperelliptic curves that gave us good codes, we have put only one of each. More curves, and the generating matrices for these codes can be found in my web page at <http://www.ma.utexas.edu/users/zarzar>.

ACKNOWLEDGMENTS

I would like to thank Prof. Felipe Voloch for the inspiring and motivating conversations. The computations in this paper were made using MAGMA Computational Algebra System.

REFERENCES

- [1] Arnaud Beauville, Complex algebraic surfaces, London Mathematical Society Lecture Note Series 68, Cambridge University Press, 1983.
- [2] V. D. Goppa, Codes on Algebraic Curves, Soviet Math. Dokl.24, No.1,170-172,1981.

- [3] David Mumford, Lectures on curves on an algebraic surface, Annals of Mathematics Studies, Number 59, Princeton University Press, 1966.
- [4] Karl-Otto Stöhr, José Felipe Voloch, Weierstrass points and curves over finite fields, Proceedings of the London Mathematical Society (3), 52, 1-19, 1986.
- [5] H. P. F. Swinnerton-Dyer, The zeta function of a cubic surface over a finite field, Proc. Camb. Phil. Soc., 63, 55-71, 1967.
- [6] John T. Tate, On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, Séminaire Bourbaki, Vol. 9, Exp. No. 306, 415-440, Soc. Math. France, Paris, 1995.
- [7] John T. Tate, Endomorphisms of abelian varieties over finite fields, Invent. Math., 2, 134-144, 1966.
- [8] A. Brower, Bounds on the minimum distance of linear codes, <http://www.win.tue.nl/~aeb/voorlincod.html>.

DEPT. OF MATHEMATICS, UNIV. OF TEXAS, AUSTIN, TX 78712-0257
E-mail address: `zarzar@math.utexas.edu`