

**SOME APPLICATIONS OF
THE SET OF CURVES ON FIBRED SURFACES TO
CODING THEORY**

G. FAILLA

*Department of Mathematics, University of Messina,
Messina, 98166/Sicily, Italy
E-mail: gfailla@dipmat.unime.it*

M. LAHYANE*

*Centro de Investigación en Matemáticas (CIMAT)
Callejón Jalisco s/n, Mineral de Valenciana, Apdo. Postal 402
Guanajuato, C.P. 36240/ Guanajuato, México
*E-mail: lahyane@cimat.mx
<http://www.cimat.mx>*

G. MOLICA BISCI

*DIMET, University of Reggio Calabria,
Reggio Calabria, 89100/Reggio Calabria, Italy
E-mail: giovanni.molica@ing.unirc.it*

Abstract.

We construct some linear error-correcting codes on fibred surfaces. Estimations of their parameters are also given.

Keywords: Linear error-correcting codes; Parameters of a code, Good codes; Fibred surfaces; Effective divisors; Absolutely irreducible curves; finite fields.

1. Introduction

In¹ (see also² and³), Goppa constructed a subclass of linear error-correcting codes, known nowadays as *Algebraic-Geometric codes*, by using the geometry of a given smooth projective curve which is defined over a finite base field k . His geometric construction enabled generalizations of the Reed-Solomon codes for which the parameters satisfy the Singleton Bound (see Lemma 1.1 and Remark 1.1). A spectacular use of the construction is the one given by Tsfasman, Vladut and Zink in⁴ to provide codes with parameters which are above the Gilbert-Varshamov bound.

In this work we construct Algebraic-Geometric codes by using the geometry of fibred surfaces. Here a surface X is said to be *fibred* if there exists a morphism from X to the projective line such that a fiber is absolutely irreducible and smooth of genus g . For the convenience of the reader, we will recall some facts about codes, see for instance⁵ and⁶.

Throughout, k is a fixed finite field having q elements, a linear error-correcting code is any subvector space \mathcal{C} of k^n for some positive integer n . The dimension of \mathcal{C} as a vector

space over k is called its *dimension* and n is referred to as its *length*.

On the other hand, k^n is naturally endowed with a norm, called its *weight function* leading to the so called Hamming distance on k^n :

a weight of a vector v in k^n is nothing than the number of nonzero coordinates of v . The *minimum distance* of a linear error-correcting \mathcal{C} is by definition the minimum of weights of nonzero vectors in \mathcal{C} . For simplicity, we refer to a linear error-correcting codes of length n , dimension k and minimum distance d as an $[n, k, d]$ -code. The length, the dimension and the minimum distance of a linear error-correcting code are its *parameters*.

Recall that the parameters of a given $[n, k, d]$ -code could not take any values, they satisfy the Singleton Bound:

Lemma 1.1. *For any $[n, k, d]$ -code, the following inequality holds:*

$$d \leq n - k + 1.$$

Remark 1.1. A Reed-Solomon code is a $[q - 1, q - d, d]$ -code, hence its parameters are optimal for the Singleton Bound.

The following is a simple illustration of how to use the geometry of a surface to obtain codes, it follows the idea of Goppa construction:

Theorem 1.1.

Let X be a fibred surface defined over a finite field k of cardinality q . Then there exists an Algebraic-Geometric code \mathcal{C} intrinsically associated to X of length n , minimum distance $d = n - N$ and of dimension 2, where $n = N(q + 1)$ and N is the number of k -rational points on a fibre.

Proof. Consider the complete linear system $|D|$ giving rise to the natural morphism from X to the projective line (see⁷), we have $h^0(X, \mathcal{O}_X(D)) = 2$. Let P_1, \dots, P_n be the number of k -rational points on X , it follows by evaluating the global sections of $\mathcal{O}_X(D)$ on the points P_1, \dots, P_n , that there exists a linear map $\varphi : H^0(X, \mathcal{O}_X(D)) \rightarrow k^n$.

Since a global section of \mathcal{O}_X vanishes only on N points, we deduce that the weight of an element of the image is equal to $n - N$, hence the minimum distance of \mathcal{C} is equal to $n - N$. On the other hand, since the number of the k -rational points of the projective line is equal to $q + 1$, it follows that the number of k -rational points of X is $N(q + 1)$. \square

Here using the morphism associated naturally to a fibred surface X , we construct codes with good parameters.

Theorem 1.2.

Let X be a fibred surface defined over a finite field k of cardinality q . Let D a divisor whose complete linear system gives to X the structure of a fibred surface. Then for a fixed positive integer $a < N$, where N is the number of k -rational points on a fibre, there exists an $[n, k, d]$ -code whose parameters satisfy the followings:

1. n is equal to $N(q + 1)$,
2. k is the dimension over k of the vector space of global sections of the invertible sheaf $\mathcal{O}_X(aD)$,
3. the minimum distance d is larger than or equal to $n - a(q + 1)$.

Proof. Use the same strategy as in the proof of Theorem 1.1 by considering the evaluation map associated to the divisor aD and to the $n = N(q + 1)$ k -rational points of X . \square

Remark 1.2. The idea of constructing codes as it is shown in the proof of Theorem 1.1 will be explored to construct other codes on some projective surfaces with concrete applications in a forthcoming paper.

Acknowledgements

This work was supported by G.N.S.A.G.A at the Mathematics Department of Messina University (Messina, Italy) and by the Centro de Investigación en Matemáticas (CIMAT) in Guanajuato, Mexico.

REFERENCES

1. V. D. Goppa, *Geometry and Codes*, Mathematics and its Applications (Soviet Series), volume 24 (Kluwer Academic Publishers Group, 1988).
2. V. D. Goppa, *Codes and information*, *Russian Math. Surveys* **39** (1984), no. 1, 87–141.
3. V. D. Goppa, *Codes that are associated with divisors*, *Problems of Information Transmission* **13** (1977), no. 1, 22–27.
4. M. A. Tsfasman, S. G. Vladut, T. Zink, *Modular curves, Shimura curves, and Goppa codes better than Varshamov-Gilbert bound*, *Math. Nachr.* **109** (1982), 21–28.
5. J. H. Van Lint, *Introduction to Coding Theory*, (Graduate Texts in Mathematics, Springer Verlag, 1982).
6. S. Roman, *Coding Theory and Information Theory*, (Graduate Texts in Mathematics, Springer Verlag, 1982).
7. R. Hartshorne, *Algebraic Geometry*, (Graduate Texts in Mathematics, Springer Verlag, 1977).